SHA-3 submission

SIMD Is a Message Digest

Principal submitter:

Gaëtan Leurent

École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

Gaetan.Leurent@ens.fr
Tel: +33.1.44.32.20.47
Fax: +33.1.44.32.21.51

Auxiliary submitters:

Charles Bouillaguet, Pierre-Alain Fouque

Algorithm inventors/developers:

Gaëtan Leurent, Charles Bouillaguet, Pierre-Alain Fouque

Backup contact:

Pierre-Alain Fouque
École Normale Supérieure
Département d'Informatique
45, rue d'Ulm
75005 Paris
France

Pierre-Alain.Fouque@ens.fr
Tel: +33.1.44.32.20.48
Fax: +33.1.44.32.21.51

Signature:

Introduction

The SIMD hash function is quite similar to members of the MD/SHA family. It is based on a familiar Merkle-Damgård design, where the compression function is built from a Feistel-like cipher in Davies-Meyer mode. However there are some innovations in this design: the internal state is twice as big as the output size, we use a strong message expansion, and we use a modified feed-forward in the compression function. The main design criteria was to follow the MD/SHA designs principle which are quite well understood, and to add some elements to avoid all known attacks.

SIMD is particularly efficient on platforms with vector instructions (SIMD) which are available on many processors. Such instructions have been proposed since 1997 and are now widely deployed. Moreover, it is also possible to use two cores on multicore processors to boost the performance with a factor 1.8 by splitting the message expansion function and the hashing process.

Contents

Chapter 1

Algorithm Specification and Rationale

This document defines the SIMD family of hash functions. This family is based on two functions SIMD-256 and SIMD-512; we define SIMD-n with $n \leq 256$ as a truncation of SIMD-256, and SIMD-n with $256 < n \leq 512$ as a truncation of SIMD-512.

Each function SIMD-n takes as input a message of arbitrary size, and outputs a digest of n bits.

1.1 Mathematical Preliminaries and Notations

The design of SIMD uses a number of different operations with useful mathematical properties. In this section, we introduce the operations that will be used through this document, and detail their properties.

1.1.1 The Field $\mathbb{F}_{257}$

Since 257 is a prime, the field $\mathbb{F}_{257}$ is only the ring $\mathbb{Z}_{257}$ of the integers modulo 257. The operations in this field are indicated with $\pmod{257}$. This field is interesting because we can map a byte to an element of the field, and the operations in $\mathbb{F}_{257}$ can be computed efficiently in software and in hardware.

1.1.2 The Number-Theoretic Transform

The Number-theoretic transform of size n in $\mathbb{F}_{257}$ is defined as:

$$\begin{aligned} \mathsf{NTT}_n : \mathbb{F}_{257}^n &\mapsto \mathbb{F}_{257}^n \\ (x_i)_{i=0}^{n-1} \to (y_i)_{i=0}^{n-1} : &\quad y_i = \sum_{j=0}^{n-1} x_j \omega^{ij} \pmod{257}. \end{aligned}$$

where $n \leq 256$, and ω is a n-th root of unity in $\mathbb{F}_{257}$. We can see it as a polynomial evaluation: if the sequence $(x_i)_{i=0}^{n-1}$ is interpreted as a polynomial $P = \sum_{j=0}^{n-1} x_j X^j$, then we have $y_i = P(\omega^i)$.

This transformation is similar to the Discrete Fourier Transform but it operates on a finite field instead of the field of complex numbers. It can be computed efficiently by the same algorithm as the Fast Fourier Transform, which has a complexity of $\mathcal{O}(n \log n)$ field operations.

1.1.3 The Ring $\mathbb{Z}_{2^{16}}$ and $\mathbb{Z}_{2^{32}}$

$\mathbb{Z}_{2^{16}}$ denotes the ring of integers modulo 2^{16}, and $\mathbb{Z}_{2^{32}}$ denotes the ring of the integers modulo 2^{32}. We use $\boxplus$ and $\boxtimes$ to represent the modular addition and multiplication in these rings. (Actually, we only use $\boxplus$ in $\mathbb{Z}_{2^{32}}$ and $\boxtimes$ in $\mathbb{Z}_{2^{16}}$).

Since an element of $\mathbb{Z}_{2^{16}}$ can be seen as a 16-bit word, and an element of $\mathbb{Z}_{2^{32}}$ can be seen as a 32-bit word, we can apply bit-wise boolean functions to them. We will use the following functions:

$$\mathsf{IF}(A,B,C) = (A \wedge B) \ \vee (\neg A \wedge C)$$
$$\mathsf{MAJ}(A,B,C) = (A \wedge B) \ \vee (A \wedge C) \vee (B \wedge C)$$

where $\vee$ denotes the boolean OR, $\wedge$ denotes AND, and $\neg$ denotes NOT. We also use $\oplus$ for the exclusive or. IF acts as a conditional, and MAJ is the majority function. These function are already used in some hash functions because they have good properties: the output is unbiased, and no input bit has a linear effect on the output.

1.2 Description of the Algorithm

The SIMD hash is an iterative hash function that follows the Merkle-Damgård design. The main component of a Merkle-Damgård hash function h is a compression function $C : \{0,1\}^p \times \{0,1\}^m \mapsto \{0,1\}^p$. To compute $h(M)$, the message M is first divided into k chunks M_i's of m bits. Then the compression function is used to compress the message chunks and the internal state: $H_{i+1} = C(H_i, M_i)$. There is a padding rule to fill the last m-bit blocks, and the padding usually includes the message size (this is known as the Merkle-Damgård strengthening). The initial value of the internal state is called IV and is fixed in the description of the hash function. The output of the hash function is given by computing a finalization function $D : \{0,1\}^p \mapsto \{0,1\}^n$ on the last internal state H_{k-1}.

The Davies-Meyer mode is a common way to build a compression function C from a block cipher E: it is defined as $C(h,m) = E_m(h) \oplus h$. Many hash functions use a custom block cypher, designed with a message expansion step, and Feistel ladder.

The SIMD family uses a similar design, and the size parameters are as follows:

	Output size n	Message block size m	Internal state size p
SIMD-256	256	512	512
SIMD-512	512	1024	1024

The inner state is represented as a matrix of 32-bit words. For SIMD-256, it is a 4×4 matrix, while SIMD-512 has a 8×4 inner state:

$$\mathcal{S}_{256} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix} \qquad \mathcal{S}_{512} = \begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}$$

In this section, we will describe more precisely the operating mode of SIMD, and the inside of the compression function: the message expansion and the Feistel ladder.

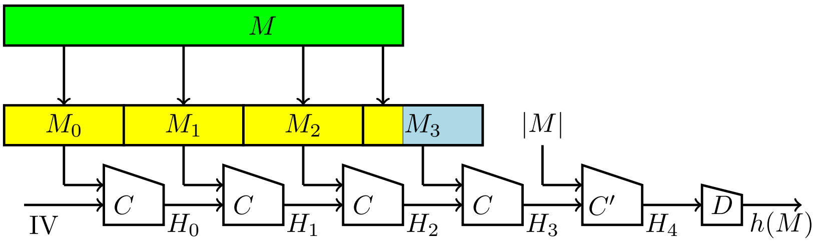

Figure 1.1: The iteration used in SIMD

1.2.1 Mode of operation

Iteration

Our mode of operation is similar to the wide-pipe construction of Lucks [15] and to Chop-MD [5]: the internal state is twice as large as the output. The padding rule is quite simple: the last message block is filled with zeros if it is smaller than m bits, and an extra block containing the size of the message in bits is added. This extra block is compressed with a slightly modified compression function C', and the output is truncated. This is described by Figure 1.1.

The size of the message input to SIMD is not limited, and the number of bits of the message included in the last block is taken modulo 2^{2^m}. We believe that it is not necessary to limit the message size in the description of the algorithm, but for all practical purpose it can be considered to be below 2^{64}. Therefore, the message input in the last message block is quite constrained. The last compression function C' acts as kind of blank round, and makes it harder to use the truncation to find a collision.

Modified Davies-Meyer

To build our compression from a Feistel-like block cipher, we will use a technique similar to the well known Davies-Meyer construction, but with a few variations.

First, we have a message block size that is equal to the internal state size, so we can use $C(h, m) = E_m(h \oplus m) \oplus h$ instead of $C(h, m) = E_m(h) \oplus h$. This is construction 8 from [3] (and construction 41 from [19]). It enjoys the same provable security guarantees than the original Davies-Meyer construction. Note that this is natural, because the former can be seen as a special case of the later, with a block cipher E' defined as $E'_k(x) = E_k(x \oplus k)$. The fact that $h \oplus m$ goes into the block cipher means that the adversary has to "commit" to a given value of m before starting to evaluate $E_m(h \oplus m)$. This prevents, for example, to construct the message m "on the fly", and complicates message modification techniques.

Second, instead of using a simple XOR to combine $E_m(h \oplus m)$ and h, we will use a few extra Feistel rounds, with h entering as the key. This makes a function $P : \{0,1\}^p \times \{0,1\}^p \mapsto \{0,1\}^p$, and the compression function is defined as $P(h, E_m(h \oplus m))$. The good property of P is that the partial functions $x \mapsto P(x, y)$ that for all y's, and the partial functions $y \mapsto P(x, y)$ that for all x's are bijective. This is sufficient to prove the same security results as the original Davies-Meyer mode. Moreover, this modified mode prevents some kind of multi-block attacks, and does not allow to find trivial fixed points useful in many second preimage attacks [14]. Our modified Davies-Meyer mode is described in Figure 1.2.

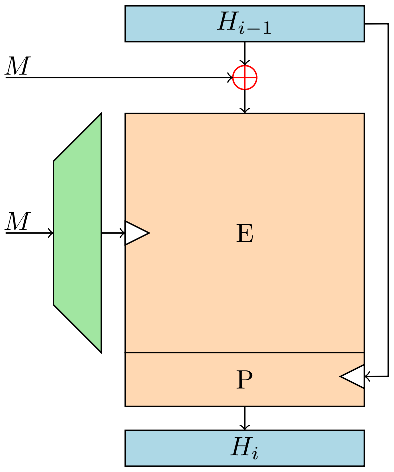

Figure 1.2: Modified Davies-Meyer

1.2.2 The Message Expansion

The message expansion is a very important part of our design. It seems that all the attacks against member of the MD/SHA family use the fact that in order to modify a small part of the expanded message, one can modify the original message block without too much effect on other parts of the full expanded message. Therefore, we choose to view the message expansion as an error correcting code, and we try to build a code with a high minimal distance. This is similar to the approach of [13], but our message expansion is very different from the MD/SHA one.

The message expansion is composed of three layers, which can each be considered as a code in some vector space. For SIMD-256 (resp. SIMD-512), it expands a 512-bit (resp. 1024-bit) message block into a 4096-bit (resp. 8192) expanded message, with a minimal distance of 520 (resp. 1032).

First Layer: Number-Theoretic Transform

The first layer of the message expansion is computationally expansive, but it a very important part of our design. The basic idea is to consider the message as a polynomial P of degree 63 (resp. 127) in $\mathbb{F}_{257}[X]$, and to evaluate this polynomial over 128 (resp. 256) points of the field $\mathbb{F}_{257}[X]$ using a Number-Theoretic Transform. This is essentially a truncated Reed-Solomon code, and it has optimal minimal distance: two different polynomials will match on at most 63 (resp. 127) points (it reaches the Singleton bound, and therefore is a linear MDS code).

However, this code has some unwanted properties, that would allow to build very specific expanded messages:

- The Reed-Solomon code is cyclic: for any polynomial P, if $(y_i) = \mathsf{NTT}(P(X))$ and $(z_i) = \mathsf{NTT}(P(\omega X))$ with ω a n-th root of the unity, then $z_i = y_{i+1 \pmod n}$.
- The NTT of a constant polynomial k is uniform $(\forall i,\ y_i = k)$. In particular, $\mathsf{NTT}(0) = 0$.

To avoid those properties, we will actually compute the NTT of the polynomial $P + X^{127}$ (resp. $P + X^{255}$). This is equivalent to adding some constants (actually the NTT of X^{127} or X^{255}) to the NTT of P. This makes the code affine, instead of just linear.

More precisely, the first message expansion step of SIMD-256 is defined as:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{64} &\to (\mathbb{F}_{257})^{128} \\ (x_i)_{i=0}^{63} &\mapsto (y_i)_{i=0}^{127} : \quad y_i = \sum_{j=0}^{127} x_j \alpha^{ij} + \alpha^{127i} \pmod{257}. \end{aligned}$$

where $\alpha = 139$ is a 128th root of unity in $\mathbb{F}_{257}$.

For SIMD-512, the first message expansion step is defined as:

$$\begin{aligned} O : (\mathbb{Z}_{2^8})^{128} &\to (\mathbb{F}_{257})^{256} \\ (x_i)_{i=0}^{127} &\mapsto (y_i)_{i=0}^{255} : \quad y_i = \sum_{j=0}^{255} x_j \beta^{ij} + \beta^{256i} \pmod{257}. \end{aligned}$$

where $\beta = 41$ is a 256th root of unity in $\mathbb{F}_{257}$, and a square root of α.

To map the x_i's from $\mathbb{Z}_{2^8}$ to $\mathbb{F}_{257}$, we take them as integers between 0 and 255.

Second Layer: Concatenated Code

In order to output a sequence of bytes (rather than elements of $\mathbb{F}_{257}$) and to increase the minimal distance of our message expansion, each symbol of $O(M)$ will be encoded through an inner code $I : \mathbb{F}_{257} \to \mathbb{Z}_{2^{16}}$. We choose to use a class of very efficient codes, implemented with only a single multiplication modulo 2^{16}: $I(x) = C \boxtimes x$ for some constant C. We ran an exhaustive search over the constant C, and we found two values that give a minimal Hamming distance of 4 bits: $C = 185$ and $C = 233$ (and their opposites). Thus, we will use the two following inner codes:

$$\begin{aligned} I_{185} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\ x &\mapsto 185 \boxtimes \widetilde{x} \qquad \text{where } -128 \le \widetilde{x} \le 128 \text{ and } \widetilde{x} = x \pmod{257} \\ I_{233} : \mathbb{F}_{257} &\to \mathbb{Z}_{2^{16}} \\ x &\mapsto 233 \boxtimes \widetilde{x} \qquad \text{where } -128 \le \widetilde{x} \le 128 \text{ and } \widetilde{x} = x \pmod{257} \end{aligned}$$

where $\widetilde{x}$ is x lifted to the integers, with $-128 \le \widetilde{x} \le 128$ (lifting to $\{-128, ...128\}$ is easier than to $\{0, ...257\}$). We will use both $I_{185}(O(M))$ and $I_{233}(O(M))$ in the expanded message (*i.e.*, we will have two copies of $O(M)$ coded differently).

Third Layer : Permutation

The expanded message will be used as a sequence of 32-bit words, so we have to pack two 16-bit words together. The 32-bit word with $I_C(x)$ in his lower 16 bits and $I_C(y)$ in its higher 16 bits is denoted by $I_C(x, y)$. If $I_C(x)$ and $I_C(y)$ are seen as integers between 0 and $2^{16} - 1$, we have $I_C(x, y) = I_C(x) + 2^{16} I_C(y)$.

To make the message expansion stronger we permute the message words so that if an attacker wants to cancel some expanded message words, he will have to choose them quite far away. We first define an intermediate 32×4 (resp. 32×8) matrix of 32-bit words. For SIMD-256, we have (with $0 \le j \le 3$):

$$Z_i^{(j)} = \begin{cases} I_{185}\big(y[8i+2j], & y[8i+2j+1]\big) \quad \text{when } 0 \le i \le 15 \\ I_{223}\big(y[8i+2j-128], & y[8i+2j-64]\big) \quad \text{when } 16 \le i \le 23 \\ I_{223}\big(y[8i+2j-191], & y[8i+2j-127]\big) \quad \text{when } 24 \le i \le 31 \end{cases}$$

For SIMD-512, we have (with $0 \le j \le 7$):

$$Z_i^{(j)} = \begin{cases} I_{185}\big(y[16i+2j], & y[16i+2j+1]\big) & \text{when } 0 \le i \le 15 \\ I_{223}\big(y[16i+2j-256], & y[16i+2j-128]\big) & \text{when } 16 \le i \le 23 \\ I_{223}\big(y[16i+2j-383], & y[16i+2j-255]\big) & \text{when } 24 \le i \le 31 \end{cases}$$

Lastly, we permute the lines of the matrix Z. Let $W_i^{(j)} = Z_{P(i)}^{(j)}$ with the following permutation:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	4	6	0	2	7	5	3	1	15	11	12	8	9	13	10	14

i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	17	18	23	20	22	21	16	19	30	24	25	31	27	29	28	26

The full message expansion for SIMD-256 is given in Table 1.1.

1.2.3 The Feistel Ladder

The compression function is based on a Feistel structure, with a step function similar to the step functions of the MD/SHA family:

$$\begin{aligned} A_j^{(i)} &= \Big(D_j^{(i-1)} \boxplus W_j^{(i)} \boxplus \phi_i(A_j^{(i-1)}, B_j^{(i-1)}, C_j^{(i-1)})\Big)^{\lll s_i} \boxplus A_{p_i(j)}^{(i-1)^{\lll r_i}} \\ B_j^{(i)} &= A_j^{(i-1)^{\lll r_i}} \\ C_j^{(i)} &= B_j^{(i-1)} \\ D_j^{(i)} &= C_j^{(i-1)} \end{aligned}$$

where ϕ_i is a boolean function, $\boxplus$ is the addition modulo 2^{32} and $\lll s_i$ denotes rotation to the left by an amount of s_i bits. This step function is shown in Figure 1.3. Note that all the values used to compute the new $A_j^{(i+1)}$'s go through a rotation. That should prevent the possibility of a weak bit, as was found in MD5 [8].

Alternatively, we can write an equivalent description of the step update involving only the A_j registers:

$$\begin{aligned} B_j^{(i)} &= A_j^{(i-1)^{\lll r_{i-1}}} \\ C_j^{(i)} &= A_j^{(i-2)^{\lll r_{i-2}}} \\ D_j^{(i)} &= A_j^{(i-3)^{\lll r_{i-3}}} \\ A_j^{(i)} &= \Big(A_j^{(i-4)^{\lll r_{i-4}}} \boxplus W_j^{(i)} \boxplus \phi_i(A_j^{(i-1)}, A_j^{(i-2)^{\lll r_{i-2}}}, A_j^{(i-3)^{\lll r_{i-3}}})\Big)^{\lll s_i} \boxplus A_{p_i(j)}^{(i-1)^{\lll r_i}} \end{aligned}$$

We basically have 4 parallel Feistel ladders for SIMD-256 (resp. 8 for SIMD-512), and they interact together because of the permutations p_i's. At each round, a new value is computed in each Feistel, and this new value is sent to another Feistel at the following round. The p_i's are chosen to ensure a good diffusion. For SIMD-256, we define

$$p_i(x) = \begin{cases} x+1 \pmod 4 & \text{if } i \text{ is even} \\ x+2 \pmod 4 & \text{if } i \text{ is odd} \end{cases}$$

i	$W_i^{(0)}$	$W_i^{(1)}$	$W_i^{(2)}$	$W_i^{(3)}$
0	$I_{185}(y_{32}, y_{33})$	$I_{185}(y_{34}, y_{35})$	$I_{185}(y_{36}, y_{37})$	$I_{185}(y_{38}, y_{39})$
1	$I_{185}(y_{48}, y_{49})$	$I_{185}(y_{50}, y_{51})$	$I_{185}(y_{52}, y_{53})$	$I_{185}(y_{54}, y_{55})$
2	$I_{185}(y_0, y_1)$	$I_{185}(y_2, y_3)$	$I_{185}(y_4, y_5)$	$I_{185}(y_6, y_7)$
3	$I_{185}(y_{16}, y_{17})$	$I_{185}(y_{18}, y_{19})$	$I_{185}(y_{20}, y_{21})$	$I_{185}(y_{22}, y_{23})$
4	$I_{185}(y_{56}, y_{57})$	$I_{185}(y_{58}, y_{59})$	$I_{185}(y_{60}, y_{61})$	$I_{185}(y_{62}, y_{63})$
5	$I_{185}(y_{40}, y_{41})$	$I_{185}(y_{42}, y_{43})$	$I_{185}(y_{44}, y_{45})$	$I_{185}(y_{46}, y_{47})$
6	$I_{185}(y_{24}, y_{25})$	$I_{185}(y_{26}, y_{27})$	$I_{185}(y_{28}, y_{29})$	$I_{185}(y_{30}, y_{31})$
7	$I_{185}(y_8, y_9)$	$I_{185}(y_{10}, y_{11})$	$I_{185}(y_{12}, y_{13})$	$I_{185}(y_{14}, y_{15})$
8	$I_{185}(y_{120}, y_{121})$	$I_{185}(y_{122}, y_{123})$	$I_{185}(y_{124}, y_{125})$	$I_{185}(y_{126}, y_{127})$
9	$I_{185}(y_{88}, y_{89})$	$I_{185}(y_{90}, y_{91})$	$I_{185}(y_{92}, y_{93})$	$I_{185}(y_{94}, y_{95})$
10	$I_{185}(y_{96}, y_{97})$	$I_{185}(y_{98}, y_{99})$	$I_{185}(y_{100}, y_{101})$	$I_{185}(y_{102}, y_{103})$
11	$I_{185}(y_{64}, y_{65})$	$I_{185}(y_{66}, y_{67})$	$I_{185}(y_{68}, y_{69})$	$I_{185}(y_{70}, y_{71})$
12	$I_{185}(y_{72}, y_{73})$	$I_{185}(y_{74}, y_{75})$	$I_{185}(y_{76}, y_{77})$	$I_{185}(y_{78}, y_{79})$
13	$I_{185}(y_{104}, y_{105})$	$I_{185}(y_{106}, y_{107})$	$I_{185}(y_{108}, y_{109})$	$I_{185}(y_{110}, y_{111})$
14	$I_{185}(y_{80}, y_{81})$	$I_{185}(y_{82}, y_{83})$	$I_{185}(y_{84}, y_{85})$	$I_{185}(y_{86}, y_{87})$
15	$I_{185}(y_{112}, y_{113})$	$I_{185}(y_{114}, y_{115})$	$I_{185}(y_{116}, y_{117})$	$I_{185}(y_{118}, y_{119})$
16	$I_{223}(y_8, y_{72})$	$I_{223}(y_{10}, y_{74})$	$I_{223}(y_{12}, y_{76})$	$I_{223}(y_{14}, y_{78})$
17	$I_{223}(y_{16}, y_{80})$	$I_{223}(y_{18}, y_{82})$	$I_{223}(y_{20}, y_{84})$	$I_{223}(y_{22}, y_{86})$
18	$I_{223}(y_{56}, y_{120})$	$I_{223}(y_{58}, y_{122})$	$I_{223}(y_{60}, y_{124})$	$I_{223}(y_{62}, y_{126})$
19	$I_{223}(y_{32}, y_{96})$	$I_{223}(y_{34}, y_{98})$	$I_{223}(y_{36}, y_{100})$	$I_{223}(y_{38}, y_{102})$
20	$I_{223}(y_{48}, y_{112})$	$I_{223}(y_{50}, y_{114})$	$I_{223}(y_{52}, y_{116})$	$I_{223}(y_{54}, y_{118})$
21	$I_{223}(y_{40}, y_{104})$	$I_{223}(y_{42}, y_{106})$	$I_{223}(y_{44}, y_{108})$	$I_{223}(y_{46}, y_{110})$
22	$I_{223}(y_0, y_{64})$	$I_{223}(y_2, y_{66})$	$I_{223}(y_4, y_{68})$	$I_{223}(y_6, y_{70})$
23	$I_{223}(y_{24}, y_{88})$	$I_{223}(y_{26}, y_{90})$	$I_{223}(y_{28}, y_{92})$	$I_{223}(y_{30}, y_{94})$
24	$I_{223}(y_{49}, y_{113})$	$I_{223}(y_{51}, y_{115})$	$I_{223}(y_{53}, y_{117})$	$I_{223}(y_{55}, y_{119})$
25	$I_{223}(y_1, y_{65})$	$I_{223}(y_3, y_{67})$	$I_{223}(y_5, y_{69})$	$I_{223}(y_7, y_{71})$
26	$I_{223}(y_9, y_{73})$	$I_{223}(y_{11}, y_{75})$	$I_{223}(y_{13}, y_{77})$	$I_{223}(y_{15}, y_{79})$
27	$I_{223}(y_{57}, y_{121})$	$I_{223}(y_{59}, y_{123})$	$I_{223}(y_{61}, y_{125})$	$I_{223}(y_{63}, y_{127})$
28	$I_{223}(y_{25}, y_{89})$	$I_{223}(y_{27}, y_{91})$	$I_{223}(y_{29}, y_{93})$	$I_{223}(y_{31}, y_{95})$
29	$I_{223}(y_{41}, y_{105})$	$I_{223}(y_{43}, y_{107})$	$I_{223}(y_{45}, y_{109})$	$I_{223}(y_{47}, y_{111})$
30	$I_{223}(y_{33}, y_{97})$	$I_{223}(y_{35}, y_{99})$	$I_{223}(y_{37}, y_{101})$	$I_{223}(y_{39}, y_{103})$
31	$I_{223}(y_{17}, y_{81})$	$I_{223}(y_{19}, y_{83})$	$I_{223}(y_{21}, y_{85})$	$I_{223}(y_{23}, y_{87})$

Table 1.1: Full Message Expansion for SIMD-256

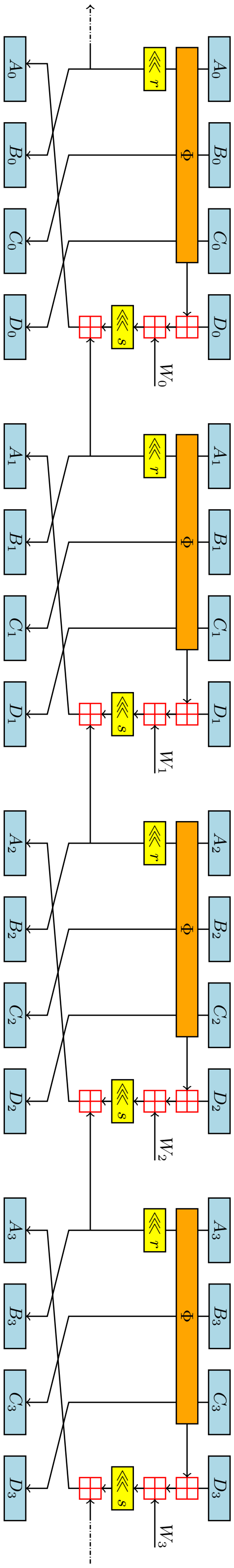

Figure 1.3: Step update of SIMD-256, with $p_i(x) = x + 1$

If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+2$. For SIMD-512, we define four permutations:

$$\begin{aligned}
p_0(x) &= x+4 \pmod 8 \\
p_1(x) &= \begin{cases} x+1 \pmod 8 & \text{if } x = 0 \pmod 2 \\ x-1 \pmod 8 & \text{otherwise} \end{cases} \\
p_2(x) &= \begin{cases} x+2 \pmod 8 & \text{if } x = 0 \pmod 4 \text{ or } x = 1 \pmod 4 \\ x-2 \pmod 8 & \text{otherwise} \end{cases} \\
p_3(x) &= 7-x \pmod 8
\end{aligned}$$

The permutation used at step i is $p_{i \bmod 4}$. If a difference is introduced in one Feistel at round i, it will have propagated to all the Feistels at round $i+3$.

More precisely, the step update function of SIMD-256 is:

$$\mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \end{bmatrix}, \phi, r, s, p\right)$$
$$= \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0,B_0,C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1,B_1,C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2,B_2,C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3,B_3,C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \end{bmatrix} \tag{1.1}$$

and the step update function of SIMD-512 is:

$$\mathsf{Step}\left(\begin{bmatrix} A_0 & B_0 & C_0 & D_0 \\ A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \\ A_5 & B_5 & C_5 & D_5 \\ A_6 & B_6 & C_6 & D_6 \\ A_7 & B_7 & C_7 & D_7 \end{bmatrix}, \begin{bmatrix} W_0 \\ W_1 \\ W_2 \\ W_3 \\ W_4 \\ W_5 \\ W_6 \\ W_7 \end{bmatrix}, \phi, r, s, p\right)$$
$$= \begin{bmatrix} (D_0 \boxplus W_0 \boxplus \phi(A_0,B_0,C_0))^{\lll s} \boxplus A_{p(0)}^{\lll r} & A_0^{\lll r} & B_0 & C_0 \\ (D_1 \boxplus W_1 \boxplus \phi(A_1,B_1,C_1))^{\lll s} \boxplus A_{p(1)}^{\lll r} & A_1^{\lll r} & B_1 & C_1 \\ (D_2 \boxplus W_2 \boxplus \phi(A_2,B_2,C_2))^{\lll s} \boxplus A_{p(2)}^{\lll r} & A_2^{\lll r} & B_2 & C_2 \\ (D_3 \boxplus W_3 \boxplus \phi(A_3,B_3,C_3))^{\lll s} \boxplus A_{p(3)}^{\lll r} & A_3^{\lll r} & B_3 & C_3 \\ (D_4 \boxplus W_4 \boxplus \phi(A_4,B_4,C_4))^{\lll s} \boxplus A_{p(4)}^{\lll r} & A_4^{\lll r} & B_4 & C_4 \\ (D_5 \boxplus W_5 \boxplus \phi(A_5,B_5,C_5))^{\lll s} \boxplus A_{p(5)}^{\lll r} & A_5^{\lll r} & B_5 & C_5 \\ (D_6 \boxplus W_6 \boxplus \phi(A_6,B_6,C_6))^{\lll s} \boxplus A_{p(6)}^{\lll r} & A_6^{\lll r} & B_6 & C_6 \\ (D_7 \boxplus W_7 \boxplus \phi(A_7,B_7,C_7))^{\lll s} \boxplus A_{p(7)}^{\lll r} & A_7^{\lll r} & B_7 & C_7 \end{bmatrix} \tag{1.2}$$

We now define one round as eight steps, with given rotation constants and boolean functions. The whole compression function is made of 4 rounds, plus one final round to mix the initial

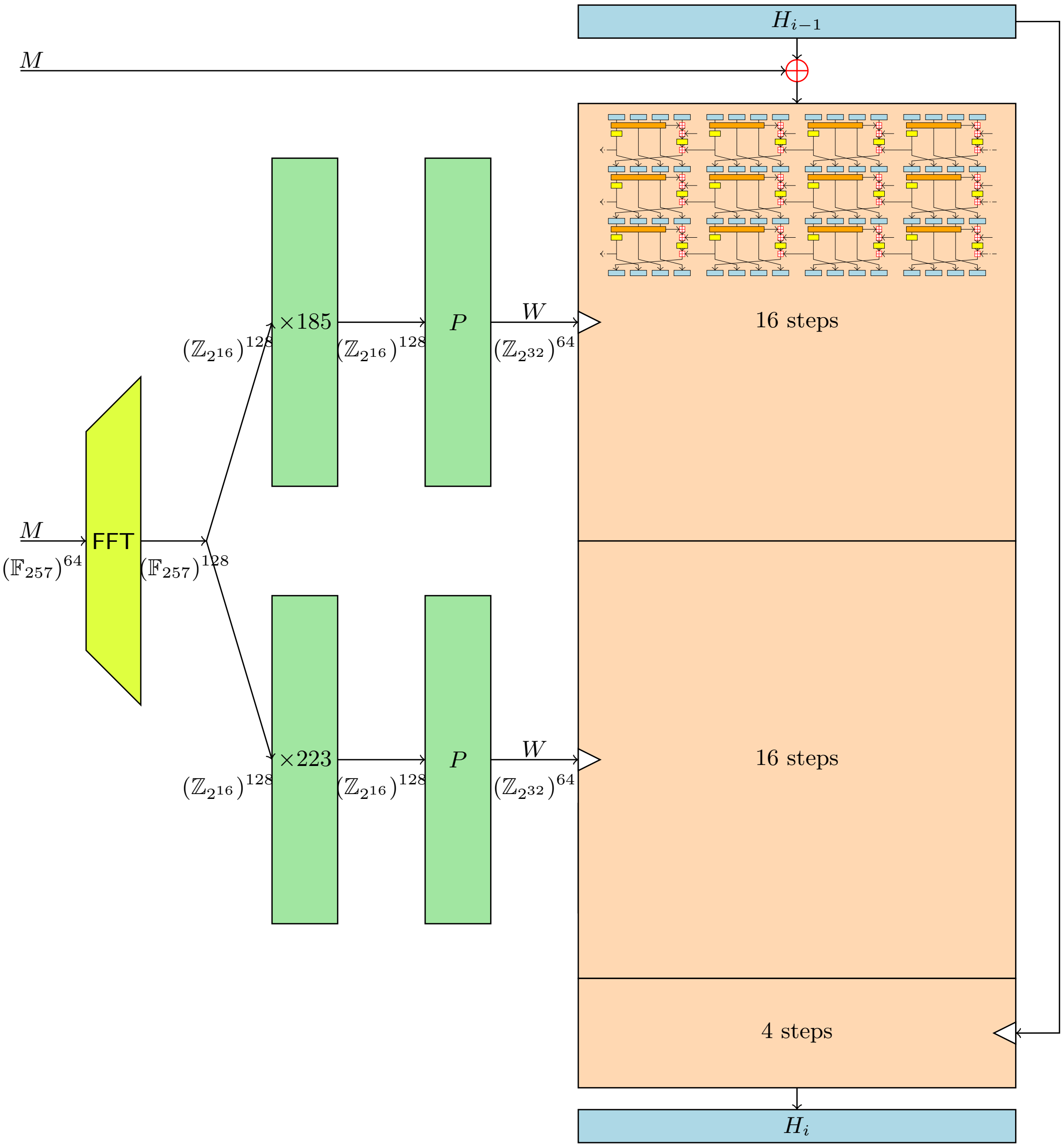
H_{i-1}
M
M
$(\mathbb{F}_{257})^{64}$
FFT
$(\mathbb{F}_{257})^{128}$
$(\mathbb{Z}_{2^{16}})^{128}$
×185
$(\mathbb{Z}_{2^{16}})^{128}$
P
W
$(\mathbb{Z}_{2^{32}})^{64}$
16 steps
$(\mathbb{Z}_{2^{16}})^{128}$
×223
$(\mathbb{Z}_{2^{16}})^{128}$
P
W
$(\mathbb{Z}_{2^{32}})^{64}$
16 steps
4 steps
H_i

Figure 1.4: Compression function of SIMD-256

chaining value to the initial state (this is our feed-forward). A graphical representation of the compression function is given in Figure 1.4, and Algorithm 1 gives a pseudo-code description of the full SIMD hash function, with the choice of constants and boolean functions.

1.2.4 The Final Compression Function

After all the message blocks have been compressed, there is an extra call to the compression function, with the message length as input. The message length is counted in bits, modulo 2^{2^m} is needed. It is written as a sequence of bytes using the little endian convention, *i.e.* the first message word will be the low order byte of the counter.

For this final compression function, we use a slightly different message expansion, with a tweaked outer code. In SIMD-256, instead of using $O(M) = \mathsf{NTT}_{128}(M+X^{127})$, we use $O'(M) = \mathsf{NTT}_{128}(M + X^{127} + X^{125})$. In SIMD-512, instead of using $O(M) = \mathsf{NTT}_{256}(M + X^{255})$, we use $O'(M) = \mathsf{NTT}_{256}(M + X^{255} + X^{253})$. The range of this modified message expansion is distinct from the range of the main message expansion, so that the expanded message is prefix-free.

After that step, the output is defined as follows:

- For SIMD-256, output the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3.

- For SIMD-n with $n \leq 256$, output the n-bit prefix of the SIMD256 output. For instance, SIMD-224's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, B_0, B_1, B_2.

- For SIMD-512, output the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7.

- For SIMD-n with $256 < n \leq 512$, output the n-bit prefix of the SIMD512 output. For instance, SIMD-384's output is the bit-string representation of:
  A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7, B_0, B_1, B_2, B_3.

1.2.5 Initialization Vector

Each SIMD-n function will use a distinct Initialization Vector, so as to avoid relations between the outputs of different members of the family. The IV of SIMD-n is defined as

$$\mathrm{IV}_n = \mathsf{SIMD\text{-}Compress}(0, \texttt{"SIMD-}\langle i\rangle\texttt{ v1.0"}, 0)$$

Where the string is written in ASCII and padded with zeros, and $\langle i\rangle$ is the decimal representation of n in ASCII, without any trailing zero or space. The values for SIMD-224, SIMD-256, SIMD-384 and SIMD-512 are given in Table 1.2.

1.2.6 Input and Output

To defines the set of function SIMD-$n : \{0,1\}^* \mapsto \{0,1\}^n$, we still have to define how to map a bit-string to the input of SIMD, and how to map the output of SIMD to a bit string. We will use a little-endian mapping, following the convention of MD4.

Algorithm 1 Pseudo-code description of SIMD.

```
function MessageExpansion($M$, $f$)        ▷ $f$ marks the final compression function
    if $f = 0$ then
        $(y_i) \leftarrow \mathsf{NTT}(M + X^{127})$        ▷ resp. $X^{255}$ for SIMD-512
    else
        $(y_i) \leftarrow \mathsf{NTT}(M + X^{127} + X^{125})$        ▷ resp. $X^{255} + X^{253}$ for SIMD-512
    end if
    Compute the $Z_i^{(j)}$'s by applying the inner codes $I_{185}$ and $I_{233}$ to the $y_i$'s.
    Compute the $W_i^{(j)}$'s by permuting the $Z_i^{(j)}$'s.
    return the $W_i^{(j)}$'s.
end function

function Round($\mathcal{S}$, $i$, $r$)
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+0}, \mathsf{IF}, r_0, r_1)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+1}, \mathsf{IF}, r_1, r_2)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+2}, \mathsf{IF}, r_2, r_3)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+3}, \mathsf{IF}, r_3, r_0)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+4}, \mathsf{MAJ}, r_0, r_1)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+5}, \mathsf{MAJ}, r_1, r_2)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+6}, \mathsf{MAJ}, r_2, r_3)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, W_{8i+7}, \mathsf{MAJ}, r_3, r_0)$
    return $\mathcal{S}$
end function

function SIMD-Compress(IV, $M$, $f$)
    $W \leftarrow \mathsf{MessageExpansion}(M, f)$
    $\mathcal{S} \leftarrow \mathrm{IV} \oplus M$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 0, [3, 20, 14, 27])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 1, [26, 4, 23, 11])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 2, [19, 28, 7, 22])$
    $\mathcal{S} \leftarrow \mathsf{Round}(\mathcal{S}, 3, [15, 5, 29, 9])$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_0, \mathsf{IF}, 15, 5)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_1, \mathsf{IF}, 5, 29)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_2, \mathsf{IF}, 29, 9)$
    $\mathcal{S} \leftarrow \mathsf{Step}(\mathcal{S}, \mathrm{IV}_3, \mathsf{IF}, 9, 15)$
    return $\mathcal{S}$
end function

function SIMD($M$)
    Split the message $M$ into chunks $M_i, 0 \leq i < k$.
    $M_{k-1}$ is padded with zeros.
    $\mathcal{S} \leftarrow \mathrm{IV}$
    for $0 \leq i < k$ do
        $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, M_i, 0)$
    end for
    $\mathcal{S} \leftarrow \mathsf{SIMD\text{-}Compress}(\mathcal{S}, \|M\|, 1)$
    return Truncate($\mathcal{S}$)
end function
```

SIMD-224 IV				
$A_{0..3}$	0xeebfea74	0x70c30346	0x4b538718	0x4f06a655
$B_{0..3}$	0xa22aad99	0x434a528c	0x355e2a29	0x8523b76e
$C_{0..3}$	0x20bcf05e	0x9eb5b91a	0x4ddc22e8	0xce0ae099
$D_{0..3}$	0x9d4dda03	0xae00fc41	0x40279fc8	0x9f0ec1f5

SIMD-256 IV				
$A_{0..3}$	0x99dae06a	0xc3d43239	0x4979de73	0x3ee5d052
$B_{0..3}$	0xda4d98d0	0xcf5c52be	0x655cbaf9	0x2a9d238e
$C_{0..3}$	0xfd892a60	0x8a471f8c	0x86ce033f	0x0ff768d3
$D_{0..3}$	0xfad01f14	0x9eeef3b3	0x68aec37a	0x6b209d72

SIMD-384 IV				
$A_{0..3}$	0x3a8f3d6f	0x756a1087	0x5d5318aa	0xbbca76f7
$A_{4..7}$	0x26a3a959	0xaca1e37e	0xb40c4642	0x904085d9
$B_{0..3}$	0xf46f6c9b	0x9ab248ef	0xdbbfc9cc	0xcc8821fa
$B_{4..7}$	0x354d3c2e	0xda334fb1	0x68ed79ce	0xa5bc107d
$C_{0..3}$	0x2da6fdc3	0xfbafce00	0x4c9a6954	0xb61f0faf
$C_{4..7}$	0xf56099b5	0xa3a5bdfb	0xf83e0977	0x7eb15372
$D_{0..3}$	0x91195b41	0xfcb9404e	0x214e6c84	0x88740b3a
$D_{4..7}$	0xba03a4b1	0xa82202fc	0x994fddfb	0xb2e1a1de

SIMD-512 IV				
$A_{0..3}$	0xb314b806	0x676cf96e	0xed91a471	0x5f306791
$A_{4..7}$	0x4ea515ee	0xde2a06cf	0xc9c96851	0x4f49a403
$B_{0..3}$	0xf778d95b	0x6e5e21da	0xad570671	0x4584c064
$B_{4..7}$	0xac201a0f	0xd4ce2a86	0xc6d663f4	0x8ec5d766
$C_{0..3}$	0x14c1303a	0xb5b890d5	0x82e61e95	0x94f47683
$C_{4..7}$	0x6ebc9ce7	0xf9af5b29	0xf4177798	0xf6cec3ee
$D_{0..3}$	0xd10eca9e	0xea3c1b82	0x5061c319	0x0c2a9f5c
$D_{4..7}$	0xfcfc980e	0xbab373c6	0x1699d7c9	0x0822d6af

Table 1.2: Initialization Vector for common versions of SIMD.

Input mapping

The input sequence of bits is interpreted in a natural manner as a sequence of bytes, where each consecutive group of eight bits is interpreted as a byte with the high-order (most significant) bit of each byte listed first.

Each byte represents an integer between 0 and 255, and we use the canonical mapping from $\mathbb{Z}$ to $\mathbb{Z}_{257} = \mathbb{F}_{257}$ to construct the inputs of the NTT step of the message expansion. Note that the NTT will never receive the input value 256.

The message also needs to be interpreted as a sequence of 32-bit words to compute $\mathrm{IV} \oplus M$. Each consecutive group of four bytes is interpreted as a word with the low-order (least significant) byte given first.

In the final compression function, we use a counter as the message input. The counter is taken modulo 2^{2^m}, so that it fits in one message block. The counter is converted to a sequence of bit using the same little endian convention: the first byte is the low-order byte. Note that the reference implementation only keep a counter modulo 2^{64}, and is therefore unable to compute the hash of a message of more than 2^{64} bits, but this not a limitation of the algorithm.

Output Mapping

The output of SIMD is made of 32-bit words, which will be converted to bytes in a little-endian fashion: the first output byte is the low-order byte.

1.3 Rationale

The SIMD hash function follows the spirit of the MD/SHA family, but it should be protected against known attacks on members of this family.

1.3.1 Iteration Mode

We believe that Merkle-Damgård construction is now well understood, thanks to all previous attacks which have shown where weaknesses can be found. In particular the Merkle-Damgård iteration without a finalization function D is sensible to some generic attacks:

- the extension attack;
- the second preimage attack on long messages [14];
- the multi-collision attack [12];
- various meet-in-the-middle attacks: building expandable messages from fixed point[7], preimages.

Those weakness can be tolerated, but we believe it is better to avoid them. This is why we use an internal state larger than the output size, and a modified compression function for the last block.

1.3.2 Davies-Meyer

The Davies-Meyer mode is also well studied, and suffers the following problems:

- It is easy to find fixed-points, which can be used to build expandable messages. If we choose a message M, then $E_M^{-1}(0)$ is a fixed point as seen in Figure 1.5.

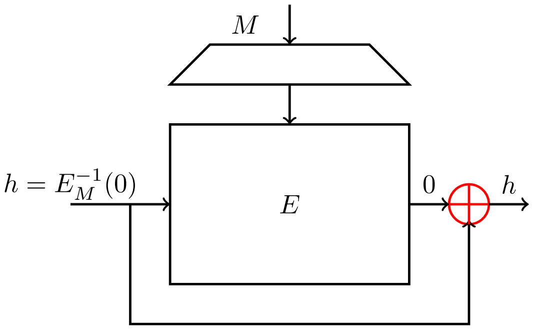

Figure 1.5: Finding fixed points in a Devies-Meyer compression function

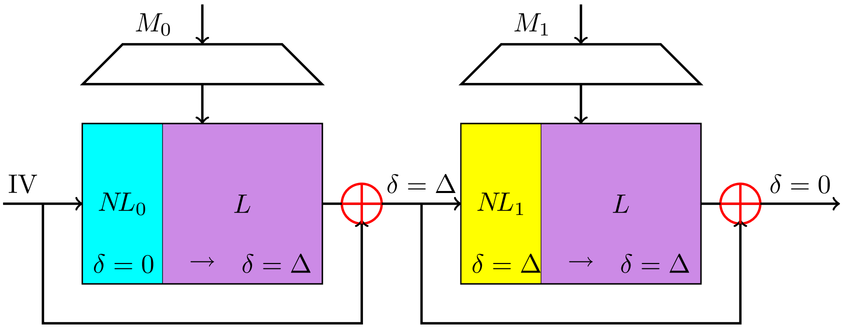

Figure 1.6: Multi-block attack using the Davies-Meyer feed-forward.

- In collision attacks, the feed-forward make it quite easy to transform pseudo-collision into collisions. If we have a linear characteristic that gives a message difference Δ, we can use two non-linear characteristic to build a differential path $0 \rightarrow \Delta$ and $\Delta \rightarrow \Delta$ in the Feistel part. Figure 1.6 shows that this allows to find a collision when the input difference Δ cancels the output difference Δ in the feed-forward. This property was used to break MD5 [22] and SHA-1 [21].

Our non-linear feedback should avoid these attacks.

1.3.3 The Message Expansion

When a block cipher is used to build hash function in Davies-Meyer mode, the key of the block cipher is under control of the attacker. This setting is quite different from the regular use of a block cipher, and an attack against the hash function usually translates to a related-key attack on the block cipher. Therefore, the block cipher should be designed with a strong key expansion (the key expansion of the block cipher become the message expansion of the hash function).

Indeed, most attacks against Davies-Meyer based hash functions use the fact that the message expansion is weak. For the members of the MD/SHA family, the message expansion can be seen as a linear code and the minimal distance of this code seems to play a very important role. This minimal distance is only 3 and 4 for MD4 and MD5, so the attacker has a lot of control. In SHA-1, the minimal distance is no more than 44, and is exactly 25 in the last 60 words [13]. Additionally, it is easy to shift a differential pattern one round down. This allows to build local collisions.

In our design, we follow the approach of Jutla and Patthak [13], who designed an better message expansion for SHA-1 with a minimal distance of 82, and 75 on the last 60 words. In [13], the authors used a code with a structure similar to the code of SHA-1 for efficiency reasons, and ruled out various algebraic codes. They consider Reed-Solomon codes over $\mathbb{F}_{2^8}$ which have a very good minimal distance, but they conclude they are unsuitable for a software implementation. In SIMD, we do use a Reed-Solomon code, but we use the field $\mathbb{F}_{257}$ which allows a quite efficient software implementation. This field was already used in the design of SWIFFT [16] for the same reason. Finally using concatenated code, we can increase the minimal distance without adding much computations.

Our message expansion is designed to avoid related key attacks on the block cipher. It has a provable minimal distance of 520 for SIMD-256, and 1032 for SIMD-512. After the NTT layer of SIMD-256, any pair of distinct message are mapped to a sequence of 128 elements in $\mathbb{F}_{257}$, with at least 65 distinct components (resp. 256 elements with 129 distinct elements). The concatenated code maps the elements of $\mathbb{F}_{257}$ to 16-bit words, so that two distinct elements are mapped to words with a Hamming distance of at least 4. We have two copies of the concatenated code (with a different inner code), so this makes a minimal hamming distance of $2 \times 4 \times 65 = 520$ for the message expansion of SIMD-256 (resp. $2 \times 4 \times 129 = 1032$ for SIMD-512).

Chapter 2

Implementation Aspect and Performances

The design of SIMD is highly parallellisable due to the choice of the components: the NTT and the parallel Feistel ladders. This should allow efficient hardware implementations. As far as software is concerned, we can use SIMD instructions (Single Instructions, Multiple Data) to compute some operations in parallel.

2.1 Software Implementation

2.1.1 SIMD instructions

SIMD instructions allow to compute a given operation on multiple data in parallel. Processors that supports SIMD instructions usually come with a set of dedicated registers, which can contain a vector of integers or floating point data. For instance the SSE registers in x86 processors are 128-bit wide ans be used to store 16 8-bit values, 8 16-bit values, 4 32-bit values, or 2 64-bit values. The SIMD instruction set allows to compute in parallel some arithmetic operations on those vectors: addition, multiplication, bit-wise operations, ...

SIMD instructions were introduced in personal computers to improve the efficiency of multimedia computations, and are now very widely available. The x86 family offers MMX since 1997 and SSE since 1999 and the PPC family has AltiVec since 1998. For embedded systems, Intel has introduced IwMMXt to it's PXA family of ARM processors, and is now promoting the Atom, an x86 processor which supports SSE. We believe that SIMD support will become even more widespread in the future. We also note that the efficiency of SIMD implementations is constantly improving: the SSE units of Intel Core micro-architecture based processors is much faster than in the older NetBurst micro-architecture. Similarly, the new AMD K10 processors feature a much better SSE units than AMD K8 ones.

Another advantage of SIMD instructions is that they usually come with a relatively large set of registers, even on CISC processors. The x86 architecture has only 8 general purpose 32-bit registers but SSE instructions comes with 8 extra 128-bit registers (on x86-64 we have 16 general purpose 64-bit registers, and 16 128-bit SSE registers). In most cases, the full state of the Feistel ladder can be kept inside those registers, which is good for performances.

Architecture		SHA-1	SHA-256	SHA-512	Scalar		Vector
					SIMD-256	SIMD-512	SIMD-256
Core2	32 bits	261	140	45	31	24	245
	64 bits	323	176	223	45	33	270
K10	32 bits	207	135	39	30	20	145
	64 bits	301	147	193	38	29	160
P4	32 bits	147	89	19	16	13	85
K8	32 bits	174	107	31	23	15	80
	64 bits	238	111	148	30	22	78
Atom	32 bits	66	35	12	7.2	5.7	64
G4		102	55	16	10	7.5	78
ARM		19	11	3.0	2.1	1.6	13

Table 2.1: Performances of SIMD compared to the SHA family. The figures are in megabyte per second (MB/s).

2.1.2 Multi-core

Our design can also exploit multi-core processors: the most expensive part of the algorithm is the message expansion, and it can be done in parallel for different message blocks. For instance, one can use o cores for the message expansion, and one core for the Feistel part. In this case, we gain a factor 1.8 on the performance.

2.1.3 Performance

SIMD-512 and SIMD-256 offer comparable performances: one SIMD-512 compression function need roughly twice the number of operations of one SIMD-256 compression function, but it also take a message block twice as big. SIMD-512 is still somewhat slower because of the higher memory requirement, and the slightly more expensive NTT (because of the $\log n$ factor). As a general rule, the message expansion of SIMD takes half of the computing time.

The memory requirement of SIMD is essentially the internal state (64 bytes for SIMD-256 and 128 bytes for SIMD-512) and the output of the NTT ($4 \times 64 = 256$ bytes for SIMD-256 and $4 \times 128 = 256$ bytes for SIMD-512).

The performance for SHA-1, SHA-256 and SHA-512 have been obtained using the implementation from sphlib [20]. We used the same compiler for SHA and SIMD.

We stress that the *optimized* versions are not really optimized since they are written in pure C, and only use scalar instructions. The natural way to write an optimized version of SIMD is to write a vectorized implementation using SIMD instructions, which are available on many platforms.

Performances on a range of computers are given in Table 2.1 and Table 2.2. We compare two implementations of SIMD, a scalar one written in pure C and a vectorized one written in C using compiler extensions to access the SIMD instructions. Our vector implementation runs on x86 with SSE2, on PowerPC with Altivec, and on ARM with IwMMXT.

Software platforms

Here is a brief description of the test platforms:
Core2: Intel Xeon E5440 running at 2.83 GHz; compiled with gcc 4.1.2.

					Scalar		Vector
Architecture		SHA-1	SHA-256	SHA-512	SIMD-256	SIMD-512	SIMD-256
Core2	32 bits	11	21	63	90	118	12
	64 bits	9	16	13	63	85	11
K10	32 bits	12	18	64	80	125	17
	64 bits	9	17	13	65	85	16
P4	32 bits	19	89	147	170	210	32
K8	32 bits	12	19	65	90	135	25
	64 bits	9	18	14	66	88	26
Atom	32 bits	24	46	133	220	280	25
G4		12	23	78	125	166	16
ARM		22	38	138	200	260	32

Table 2.2: Performances of SIMD compared to the SHA family. The figures are in cycles per byte (c/B).

K10:	AMD Phenom 9850 running at 2.5 GHz; compiled with gcc 4.2.4.
P4:	Intel Pentium 4 running at 2.8 GHz; compiled with gcc 4.1.2.
K8:	AMD Athlon64 X2 3800+ running at 2 GHz; compiled with gcc 4.2.3.
Atom:	Intel Atom N270 running at 1.6 GHz; compiled with gcc 4.1.3.
G4:	PowerPC 7447 running at 1.25 GHz; compiled with gcc 4.1.2.
ARM:	Intel XScale PXA270 running at 416 MHz; compiled with gcc 4.3.0.

2.2 8-bit Implementation

We also tested SIMD on a 8-bit platform. We used gcc to compile the optimized code to an Atmel AVR AtMega8, and we ran it in the simularv simulator. We optimized some part of the code with inline assembly to handle the 8-bit architecture. Our code ran at 1300 cycles/byte.

2.3 Hardware implementation

We did a preliminary study to implement SIMD on a FPGA. The Feistel part of SIMD can be implemented in the same way as the Feistel part of other hash functions of the MD/SHA family, and we would include the hardware to compute the four Feistels in parallel. Since SIMD has less steps than SHA-1 and SHA-2, this part will run faster, but requires more gates to computes the four Feistels. To compute the NTT, we propose to include the hardware to compute a size 8 NTT, which will be called 32 times to compute the size 128 NTT of SIMD-256. It should run at about the same speed as the Feistel part.

Chapter 3

Expected strength

We conjecture that no non-random properties of an instance of SIMD-224 or SIMD-256 (indexed by the IV) can be identified with less than 2^{256} calls to the compression function.

Similarly we conjecture that no non-random properties of an instance of SIMD-384 or SIMD-512 can be identified with less than 2^{512} calls to the compression function.

In particular this means that we believe that a collision attack on SIMD-n has a complexity of $2^{n/2}$, and preimage or second preimage attack has a complexity of 2^n. There should be neither shortcut multi-collision attack nor shortcut second preimage against long messages.

Chapter 4

Security Analysis

4.1 Mode of Operation

4.1.1 Mode of Operation for the Hash Function

Since we use a modified message expansion for the final compression function, the expanded message will be prefix free. This allow better security proofs of the iteration mode. Alternatively, we can model the compression function C and the final compression C' as two independent random oracles and see our construction as an instance of the wide-pipe design of Lucks [15].

Thus, following proofs from [4, 17, 15], our iteration mode is indifferentiable from a random oracle if the compression function is a random oracle. These proofs show that there is no generic attack against the mode of operation. Moreover, the security proved is up to 2^n queries, where n is the length of the hash function. Consequently, we can hope there is no generic attack against collision, second-preimage attack or preimage attack as long as the compression function is good.

4.1.2 Security Results for Some Hash Based Constructions

The security proof for ChopMD has been provided in [4] by Chang and Nandi at FSE 2008 and the security proof for ChopMD with prefix-free message by Maurer and Tessaro at Crypto 2007 in [17] in the indifferentiablity framework. Such results show that there is no generic attack against the mode of operation. Moreover, since the security is above the birthday barrier and in 2^n if n is the hash length, then there is no better collision, second or preimage attack.

Moreover, the fact that messages are *prefix-free* allows to prove that the cascade construction of a PRF function is also a PRF [2]. This can also be used to prove the security of MAC function.

MAC function

We propose two distinct ways to build a Message Authentication Code from the SIMD hash function.

First, as any Merkle-Damgård based hash function, SIMD can be used with the HMAC construction. The security proof of Bellare in [1] can be used to prove the security of HMAC-SIMD.

Second, we can simply compute $MAC_k(M) = \mathsf{SIMD}(k\|M)$ where $\|$ denotes the concatenation. Thanks to the security proof in the indifferentiability framework, there are not generic shortcut attack on this construction. This means that one has to find a weakness in the compression in order to break this MAC.

Key Derivation

If SIMD is a PRF assuming that the compression function is a good PRF, then it is easy to prove that SIMD is a good randomness extractor that can be plugged in a key derivation function. Such results have been provided in [10]. The important point to construct a good randomness extractor already pointed out in [9] is the fact that we need to truncate the output of the function.

4.1.3 Mode of Operation for the Compression Function

The mode of operation for the compression function does not follow directly from the Davies-Meyer mode of operation. This mode presents some weaknesses we want to avoid : fix points can be easily found for example. The mode we used can be seen as a variant of the construction 8 of paper [3] (and construction 41 from [19]). Finally, the proofs provided in [3] can be extended to our construction in the ideal cipher model.

4.2 Security of the Compression Function

4.2.1 Resistance to Differential Cryptanalysis

The SIMD-family is provably secure against a class of differential attacks. The proof is very simple:

1. Any pair of distinct messages gives expanded messages with a least 520 bit differences for SIMD-256, resp. 1032 for SIMD-512.

2. When a difference is introduced by the message, an attacker will have to control its non-linear propagation. The attacker must at least control the effect of the carry, which will be good with a probability of 2^{-1}. As a comparison, in SHA-1, it is quite easy to control the error propagation because the perturbation vector can shifted to correct the errors, but the success probability is only $2^{-2.5}$. We expect that it will actually be more difficult to control the propagation of differences in SIMD.

3. Even if the adversary can use message-modification techniques to control the non-linearity in one half of the hash function for free, he still has to deal with 260 differences, resp. 516 for SIMD-512. Note that our compression function construction forces the adversary to choose the message from the beginning, so we do not expect message modification techniques to work.

Thus, even an extremely optimistic and lucky attacker using techniques similar to the attacks of Wang *et al.* against the MD/SHA family will not break SIMD, and there is still a big security margin.

4.2.2 The Step Update Function

The step update function of SIMD is defined as:

$$A_j^{(i)} = \left(A_j^{(i-4)^{\lll r_{i-4}}} \boxplus W_j^{(i)} \boxplus \phi_i(A_j^{(i-1)}, A_j^{(i-2)^{\lll r_{i-2}}}, A_j^{(i-3)^{\lll r_{i-3}}})\right)^{\lll s_i} \boxplus A_{p_i(j)}^{(i-1)^{\lll r_i}}$$

It is quite similar to the step update functions of members of the MD/SHA family, and has been built with previous attacks on these functions in mind.

Our function is of form $A^{(i)} = F(A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}) \boxplus A^{(i-1)}$, like in MD5. This gives a good avalanche effect, since a difference in $A^{(i-1)}$ will most likely be propagated to $A^{(i)}$ and can not be easily absorbed. Most attacks on MD4 are based on the fact that the step update allows to easily absorb a difference in the internal state.

Den Boer and Bosselaers discovered an other kind of weakness in the step update function of MD5 [8]. If there is some differential pattern in $A^{(i-4)}, A^{(i-3)}, A^{(i-2)}, A^{(i-1)}$, than can be cancelled through F, then the addition of $A^{(i-1)}$ will reintroduce this pattern and it will propagate in the compression function. To avoid this kind of attack, we added a rotation on $A^{(i-1)}$ in the design of SIMD.

4.3 Reduced Versions

We define two sets of reduced version of SIMD for security analysis, with a reduced number of steps, and a weaker message expansion. We encourage cryptographers to try and break them.

4.3.1 SIMD-$n/2.k$

We let SIMD-$n/2.k$ be a reduced version of SIMD-n with $2k$ steps in the main part of the Feistel instead of 2×16. The steps of SIMD-$n/2.k$ are the steps 0, 1, ... $k-1$, and 16, 17, ... $15+k$ of SIMD-n, plus the feed-forward steps. For SIMD-256/$2.k$, the reduced message expansion is defined as:

$$W_i^{(j)} = \begin{cases} I_{185}\big(y[8i+2j], & y[8i+2j+1]\big) \quad \text{when } 0 \leq i < k \\ I_{223}\big(y[8i+2j-128], & y[8i+2j-127]\big) \quad \text{when } 16 \leq i < 16+k \end{cases}$$

and for SIMD-512/k:

$$W_i^{(j)} = \begin{cases} I_{185}\big(y[16i+2j], & y[16i+2j+1]\big) \quad \text{when } 0 \leq i < k \\ I_{223}\big(y[16i+2j-256], & y[16i+2j-255]\big) \quad \text{when } 16 \leq i < 16+k \end{cases}$$

SIMD-$n/2.k$ is defined for k between 8 and 16.

4.3.2 SIMD-n/k

We let SIMD-n/k be a reduced version of SIMD-n with only k steps in the main part of the Feistel. The steps of SIMD-n/k are the steps 0, 1, ... $k-1$ of SIMD-n. For SIMD-256/k, the reduced message expansion is defined as:

$$W_i^{(j)} = I_{185}\big(y[8i+2j], y[8i+2j+1]\big)$$

and for SIMD-512/k:

$$W_i^{(j)} = I_{185}\big(y[16i+2j], y[16i+2j+1]\big)$$

SIMD-n/k is defined for k between 8 and 16.

There are no permutations is these reduced versions, and the message expansion of SIMD-256/$2.k$ and SIMD-256/k only uses $8k$ outputs of the NTT ($16k$ for SIMD-512/k). SIMD-$n/2.16$ and SIMD-$n/16$ uses the full NTT, while in SIMD-$n/8$ SIMD-$n/2.8$, the NTT does not expand the message at all, which should greatly reduce the security.

Note that SIMD-$n/2.8$ and SIMD-$n/16$ both have 16 steps, but the message expansion of SIMD-$n/2.8$ is much weaker than the message expansion of SIMD-$n/16$.

Chapter 5

Advantages and limitations

5.1 Parallelism

SIMD features a small scale parallelism. The compression function itself can be parallelized to some extend. This can be used to improve hardware efficiency, and allows an efficient software implementation using SIMD instructions. The fact that about half the time required to compute the hash function is spent in the message expansion also allows a second level of parallelism: the message expansion of the message block $i + 1$ can be computed while the Feistel part is compressing the message block i.

We believe that this level of parallelism is sufficient for a general purpose hash function. If a specific application require an extremely fast hash function, it can use SIMD in a custom parallel mode. For instance, given a parallelization parameter k, one can split the message into k independent parts, hash the k parts with SIMD, and use an extra call to SIMD to rehash the concatenation of the k hash values.

5.2 Strong Message Expansion

We believe that the internal block cipher in a hash function does not have the same security requirement than a block cipher to encrypt a message. In particular, the block cipher inside a Davies-Meyer hash function should be secure under related key attacks. This is why the message expansion of SIMD is very strong. The security of the hash function is mainly based on its very high minimal distance. Of course, this also means that the message expansion is quite expansive: it accounts for about half the time spent in the hash function. However, there are some cases where we can reduce this cost and improve the efficiency of SIMD. If there is only a small of the message block that is variable, we can precompute the NTT of the fixed part, and add the variable part when it is known. This trick can be used to speed up the hashing of small messages (the counter in the final compression function has at most two active byte), or when SIMD is used in counter mode.

5.3 Performance

The performances of SIMD are very good on high-end desktop computers. SIMD-256 only needs 11 cycles per byte on one core of a Core2 processor, and we can go down to 6 cycles per byte if we use two cores. More generally, SIMD is efficient on architectures which include a set of SIMD instructions.

On the other hand, it should also be noted than a fast implementation of the SIMD hash function has to use SIMD instructions, and can not be written in pure C. Similarly, the performances are not very good if there is no SIMD support on the target platform.

Chapter 6

Test Vectors

In this section we give test vectors and intermediate value during the computations. This should help implementors to make a correct implementation.

6.1 SIMD-224

6.1.1 Empty message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
y[ 24.. 31] =   96  176  161   47  189   61  248  107
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
```

```
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe4201be  993666ca  d8cd2733  9f4f60b1
Z[17] = ab81547f  2812d7ee  d5512aaf  5c56a3aa
Z[18] = 3b3cc4c4  037cfc84  bdcc4234  15c7ea39
Z[19] = ac6053a0  53a0ac60  3b3cc4c4  07d7f829
Z[20] = 00000000  6c0493fc  f1310ecf  f58c0a74
Z[21] = 053afac6  ce5931a7  d70f28f1  06f8f908
Z[22] = 3b3cc4c4  2e2bd1d5  2d4cd2b4  3cfac306
Z[23] = 08b6f74a  65eb9a15  bced4313  edb5124b
Z[24] = 57fba805  a2cb5d35  2733d8cd  52c1ad3f
Z[25] = 06f8f908  fd63029d  a80557fb  1d9ee262
Z[26] = 44d1bb2f  2e2bd1d5  b892476e  c761389f
Z[27] = 468fb971  d70f28f1  cadd3523  a2cb5d35
Z[28] = 6dc2923e  9d91626f  e3411cbf  9f4f60b1
Z[29] = a64759b9  5ef3a10d  c761389f  634e9cb2
Z[30] = f90806f8  1785e87b  5c56a3aa  1a22e5de
Z[31] = 9f4f60b1  fac6053a  f74a08b6  5e14a1ec
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
```

```
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = ab81547f  2812d7ee  d5512aaf  5c56a3aa
W[17] = 3b3cc4c4  037cfc84  bdcc4234  15c7ea39
W[18] = 08b6f74a  65eb9a15  bced4313  edb5124b
W[19] = 00000000  6c0493fc  f1310ecf  f58c0a74
W[20] = 3b3cc4c4  2e2bd1d5  2d4cd2b4  3cfac306
W[21] = 053afac6  ce5931a7  d70f28f1  06f8f908
W[22] = fe4201be  993666ca  d8cd2733  9f4f60b1
W[23] = ac6053a0  53a0ac60  3b3cc4c4  07d7f829
W[24] = f90806f8  1785e87b  5c56a3aa  1a22e5de
W[25] = 57fba805  a2cb5d35  2733d8cd  52c1ad3f
W[26] = 06f8f908  fd63029d  a80557fb  1d9ee262
W[27] = 9f4f60b1  fac6053a  f74a08b6  5e14a1ec
W[28] = 468fb971  d70f28f1  cadd3523  a2cb5d35
W[29] = a64759b9  5ef3a10d  c761389f  634e9cb2
W[30] = 6dc2923e  9d91626f  e3411cbf  9f4f60b1
W[31] = 44d1bb2f  2e2bd1d5  b892476e  c761389f
```

Feistel Steps

```
IV :
A[0]=eebfea74  B[0]=a22aad99  C[0]=20bcf05e  D[0]=9d4dda03
A[1]=70c30346  B[1]=434a528c  C[1]=9eb5b91a  D[1]=ae00fc41
A[2]=4b538718  B[2]=355e2a29  C[2]=4ddc22e8  D[2]=40279fc8
A[3]=4f06a655  B[3]=8523b76e  C[3]=ce0ae099  D[3]=9f0ec1f5

IV XOR M :
A[0]=eebfea74  B[0]=a22aad99  C[0]=20bcf05e  D[0]=9d4dda03
A[1]=70c30346  B[1]=434a528c  C[1]=9eb5b91a  D[1]=ae00fc41
A[2]=4b538718  B[2]=355e2a29  C[2]=4ddc22e8  D[2]=40279fc8
A[3]=4f06a655  B[3]=8523b76e  C[3]=ce0ae099  D[3]=9f0ec1f5

Step  0: (r= 3, s=20)
A[0]=a7f660dc  B[0]=75ff53a7  C[0]=a22aad99  D[0]=20bcf05e
A[1]=26b91ad7  B[1]=86181a33  C[1]=434a528c  D[1]=9eb5b91a
A[2]=67cb1096  B[2]=5a9c38c2  C[2]=355e2a29  D[2]=4ddc22e8
A[3]=8cd698b2  B[3]=783532aa  C[3]=8523b76e  D[3]=ce0ae099

Step  1: (r=20, s=14)
A[0]=2c964fd2  B[0]=0dca7f66  C[0]=75ff53a7  D[0]=a22aad99
A[1]=0663020c  B[1]=ad726b91  C[1]=86181a33  D[1]=434a528c
A[2]=dbca545d  B[2]=09667cb1  C[2]=5a9c38c2  D[2]=355e2a29
```

```
A[3]=66eedbf5  B[3]=8b28cd69  C[3]=783532aa  D[3]=8523b76e

Step  2: (r=14, s=27)
A[0]=563bca0b  B[0]=93f48b25  C[0]=0dca7f66  D[0]=75ff53a7
A[1]=bdc03502  B[1]=c0830198  C[1]=ad726b91  D[1]=86181a33
A[2]=bfeed7f5  B[2]=951776f2  C[2]=09667cb1  D[2]=5a9c38c2
A[3]=16ca42ad  B[3]=b6fd59bb  C[3]=8b28cd69  D[3]=783532aa

Step  3: (r=27, s= 3)
A[0]=74ce8601  B[0]=5ab1de50  C[0]=93f48b25  D[0]=0dca7f66
A[1]=6ca9691c  B[1]=15ee01a8  C[1]=c0830198  D[1]=ad726b91
A[2]=b1d95341  B[2]=adff76bf  C[2]=951776f2  D[2]=09667cb1
A[3]=4ead75ba  B[3]=68b65215  C[3]=b6fd59bb  D[3]=8b28cd69

Step  4: (r= 3, s=20)
A[0]=c8265853  B[0]=a674300b  C[0]=5ab1de50  D[0]=93f48b25
A[1]=189a014e  B[1]=654b48e3  C[1]=15ee01a8  D[1]=c0830198
A[2]=2a0815d4  B[2]=8eca9a0d  C[2]=adff76bf  D[2]=951776f2
A[3]=8b8eedad  B[3]=756badd2  C[3]=68b65215  D[3]=b6fd59bb

Step  5: (r=20, s=14)
A[0]=950b4aa7  B[0]=853c8265  C[0]=a674300b  D[0]=5ab1de50
A[1]=e6059ad0  B[1]=14e189a0  C[1]=654b48e3  D[1]=15ee01a8
A[2]=311e1f1b  B[2]=5d42a081  C[2]=8eca9a0d  D[2]=adff76bf
A[3]=e543bd32  B[3]=dad8b8ee  C[3]=756badd2  D[3]=68b65215

Step  6: (r=14, s=27)
A[0]=23df62af  B[0]=d2a9e542  C[0]=853c8265  D[0]=a674300b
A[1]=cca80670  B[1]=66b43981  C[1]=14e189a0  D[1]=654b48e3
A[2]=1707b84d  B[2]=87c6cc47  C[2]=5d42a081  D[2]=8eca9a0d
A[3]=0804958e  B[3]=ef4cb950  C[3]=dad8b8ee  D[3]=756badd2

Step  7: (r=27, s= 3)
A[0]=8c0b021b  B[0]=791efb15  C[0]=d2a9e542  D[0]=853c8265
A[1]=d0f9aed9  B[1]=86654033  C[1]=66b43981  D[1]=14e189a0
A[2]=f19228f4  B[2]=68b83dc2  C[2]=87c6cc47  D[2]=5d42a081
A[3]=bf9e1864  B[3]=704024ac  C[3]=ef4cb950  D[3]=dad8b8ee

Step  8: (r=26, s= 4)
A[0]=624af5c3  B[0]=6e302c08  C[0]=791efb15  D[0]=d2a9e542
A[1]=42d53c8e  B[1]=6743e6bb  C[1]=86654033  D[1]=66b43981
A[2]=60e3d25c  B[2]=d3c648a3  C[2]=68b83dc2  D[2]=87c6cc47
A[3]=0094db61  B[3]=92fe7861  C[3]=704024ac  D[3]=ef4cb950

Step  9: (r= 4, s=23)
A[0]=098149ac  B[0]=24af5c36  C[0]=6e302c08  D[0]=791efb15
A[1]=d7534581  B[1]=2d53c8e4  C[1]=6743e6bb  D[1]=86654033
A[2]=9b81a26b  B[2]=0e3d25c6  C[2]=d3c648a3  D[2]=68b83dc2
A[3]=8c5d3002  B[3]=094db610  C[3]=92fe7861  D[3]=704024ac
```

```
Step 10: (r=23, s=11)
A[0]=b4257378  B[0]=d604c0a4  C[0]=24af5c36  D[0]=6e302c08
A[1]=b9b20ba1  B[1]=c0eba9a2  C[1]=2d53c8e4  D[1]=6743e6bb
A[2]=3e180b71  B[2]=35cdc0d1  C[2]=0e3d25c6  D[2]=d3c648a3
A[3]=a2a7ca7b  B[3]=01462e98  C[3]=094db610  D[3]=92fe7861

Step 11: (r=11, s=26)
A[0]=b18a7bca  B[0]=2b9bc5a1  C[0]=d604c0a4  D[0]=24af5c36
A[1]=a4cf3282  B[1]=905d0dcd  C[1]=c0eba9a2  D[1]=2d53c8e4
A[2]=003daad4  B[2]=c05b89f0  C[2]=35cdc0d1  D[2]=0e3d25c6
A[3]=9be0df66  B[3]=3e53dd15  C[3]=01462e98  D[3]=094db610

Step 12: (r=26, s= 4)
A[0]=eac0b8a7  B[0]=2ac629ef  C[0]=2b9bc5a1  D[0]=d604c0a4
A[1]=0f8230f5  B[1]=0a933cca  C[1]=905d0dcd  D[1]=c0eba9a2
A[2]=f4583659  B[2]=5000f6ab  C[2]=c05b89f0  D[2]=35cdc0d1
A[3]=fcf445d2  B[3]=9a6f837d  C[3]=3e53dd15  D[3]=01462e98

Step 13: (r= 4, s=23)
A[0]=965e91d6  B[0]=ac0b8a7e  C[0]=2ac629ef  D[0]=2b9bc5a1
A[1]=6e517f8d  B[1]=f8230f50  C[1]=0a933cca  D[1]=905d0dcd
A[2]=95f721a8  B[2]=4583659f  C[2]=5000f6ab  D[2]=c05b89f0
A[3]=d2ac1f4c  B[3]=cf445d2f  C[3]=9a6f837d  D[3]=3e53dd15

Step 14: (r=23, s=11)
A[0]=d2bd4157  B[0]=eb4b2f48  C[0]=ac0b8a7e  D[0]=2ac629ef
A[1]=becec495  B[1]=c6b728bf  C[1]=f8230f50  D[1]=0a933cca
A[2]=942ed4e3  B[2]=d44afb90  C[2]=4583659f  D[2]=5000f6ab
A[3]=23bfce96  B[3]=a669560f  C[3]=cf445d2f  D[3]=9a6f837d

Step 15: (r=11, s=26)
A[0]=3ae3423a  B[0]=ea0abe95  C[0]=eb4b2f48  D[0]=ac0b8a7e
A[1]=aee7a6db  B[1]=7624adf6  C[1]=c6b728bf  D[1]=f8230f50
A[2]=33cd56dc  B[2]=76a71ca1  C[2]=d44afb90  D[2]=4583659f
A[3]=ff82da46  B[3]=fe74b11d  C[3]=a669560f  D[3]=cf445d2f

Step 16: (r=19, s=28)
A[0]=0b06e821  B[0]=11d1d71a  C[0]=ea0abe95  D[0]=eb4b2f48
A[1]=ff4847ad  B[1]=36dd773d  C[1]=7624adf6  D[1]=c6b728bf
A[2]=b34dc0f2  B[2]=b6e19e6a  C[2]=76a71ca1  D[2]=d44afb90
A[3]=74722068  B[3]=d237fc16  C[3]=fe74b11d  D[3]=a669560f

Step 17: (r=28, s= 7)
A[0]=f39a2c12  B[0]=10b06e82  C[0]=11d1d71a  D[0]=ea0abe95
A[1]=d7d18306  B[1]=dff4847a  C[1]=36dd773d  D[1]=7624adf6
A[2]=8e1d8246  B[2]=2b34dc0f  C[2]=b6e19e6a  D[2]=76a71ca1
A[3]=13ed3345  B[3]=87472206  C[3]=d237fc16  D[3]=fe74b11d
```

```
Step 18: (r= 7, s=22)
A[0]=23026858  B[0]=cd160979  C[0]=10b06e82  D[0]=11d1d71a
A[1]=20761e96  B[1]=e8c1836b  C[1]=dff4847a  D[1]=36dd773d
A[2]=ef3544c7  B[2]=0ec12347  C[2]=2b34dc0f  D[2]=b6e19e6a
A[3]=2cc1e9e5  B[3]=f699a289  C[3]=87472206  D[3]=d237fc16

Step 19: (r=22, s=19)
A[0]=619ce970  B[0]=1608c09a  C[0]=cd160979  D[0]=10b06e82
A[1]=e668458e  B[1]=a5881d87  C[1]=e8c1836b  D[1]=dff4847a
A[2]=424e713c  B[2]=31fbcd51  C[2]=0ec12347  D[2]=2b34dc0f
A[3]=edf397e4  B[3]=794b307a  C[3]=f699a289  D[3]=87472206

Step 20: (r=19, s=28)
A[0]=1587d30d  B[0]=4b830ce7  C[0]=1608c09a  D[0]=cd160979
A[1]=79109830  B[1]=2c773342  C[1]=a5881d87  D[1]=e8c1836b
A[2]=44dc409d  B[2]=89e21273  C[2]=31fbcd51  D[2]=0ec12347
A[3]=97a4e666  B[3]=bf276f9c  C[3]=794b307a  D[3]=f699a289

Step 21: (r=28, s= 7)
A[0]=beb02b7d  B[0]=d1587d30  C[0]=4b830ce7  D[0]=1608c09a
A[1]=7ee158d8  B[1]=07910983  C[1]=2c773342  D[1]=a5881d87
A[2]=b69ec223  B[2]=d44dc409  C[2]=89e21273  D[2]=31fbcd51
A[3]=64921161  B[3]=697a4e66  C[3]=bf276f9c  D[3]=794b307a

Step 22: (r= 7, s=22)
A[0]=642862fa  B[0]=5815bedf  C[0]=d1587d30  D[0]=4b830ce7
A[1]=d43c7dc2  B[1]=70ac6c3f  C[1]=07910983  D[1]=2c773342
A[2]=f2f0969f  B[2]=4f6111db  C[2]=d44dc409  D[2]=89e21273
A[3]=7bf73217  B[3]=4908b0b2  C[3]=697a4e66  D[3]=bf276f9c

Step 23: (r=22, s=19)
A[0]=a406fc03  B[0]=be990a18  C[0]=5815bedf  D[0]=d1587d30
A[1]=ef0da46e  B[1]=70b50f1f  C[1]=70ac6c3f  D[1]=07910983
A[2]=1d2de61b  B[2]=a7fcbc25  C[2]=4f6111db  D[2]=d44dc409
A[3]=408e92eb  B[3]=85defdcc  C[3]=4908b0b2  D[3]=697a4e66

Step 24: (r=15, s= 5)
A[0]=a069581e  B[0]=7e01d203  C[0]=be990a18  D[0]=5815bedf
A[1]=ea955247  B[1]=d2377786  C[1]=70b50f1f  D[1]=70ac6c3f
A[2]=4b994ed6  B[2]=f30d8e96  C[2]=a7fcbc25  D[2]=4f6111db
A[3]=237e7594  B[3]=4975a047  C[3]=85defdcc  D[3]=4908b0b2

Step 25: (r= 5, s=29)
A[0]=50fe31e5  B[0]=0d2b03d4  C[0]=7e01d203  D[0]=be990a18
A[1]=cc845796  B[1]=52aa48fd  C[1]=d2377786  D[1]=70b50f1f
A[2]=f8eb58ff  B[2]=7329dac9  C[2]=f30d8e96  D[2]=a7fcbc25
A[3]=f6e229c4  B[3]=6fceb284  C[3]=4975a047  D[3]=85defdcc

Step 26: (r=29, s= 9)
```

```
A[0]=551e58d9  B[0]=aa1fc63c  C[0]=0d2b03d4  D[0]=7e01d203
A[1]=96020ca0  B[1]=d9908af2  C[1]=52aa48fd  D[1]=d2377786
A[2]=fec218be  B[2]=ff1d6b1f  C[2]=7329dac9  D[2]=f30d8e96
A[3]=55213062  B[3]=9edc4538  C[3]=6fceb284  D[3]=4975a047

Step 27: (r= 9, s=15)
A[0]=bf1990c5  B[0]=3cb1b2aa  C[0]=aa1fc63c  D[0]=0d2b03d4
A[1]=253f937c  B[1]=0419412c  C[1]=d9908af2  D[1]=52aa48fd
A[2]=ed87a76a  B[2]=84317dfd  C[2]=ff1d6b1f  D[2]=7329dac9
A[3]=66853458  B[3]=4260c4aa  C[3]=9edc4538  D[3]=6fceb284

Step 28: (r=15, s= 5)
A[0]=044810c1  B[0]=c862df8c  C[0]=3cb1b2aa  D[0]=aa1fc63c
A[1]=ae142408  B[1]=c9be129f  C[1]=0419412c  D[1]=d9908af2
A[2]=fdbc20a7  B[2]=d3b576c3  C[2]=84317dfd  D[2]=ff1d6b1f
A[3]=f42d5db7  B[3]=9a2c3342  C[3]=4260c4aa  D[3]=9edc4538

Step 29: (r= 5, s=29)
A[0]=631d0b4e  B[0]=89021820  C[0]=c862df8c  D[0]=3cb1b2aa
A[1]=fe3fbc7f  B[1]=c2848115  C[1]=c9be129f  D[1]=0419412c
A[2]=3c889b34  B[2]=b78414ff  C[2]=d3b576c3  D[2]=84317dfd
A[3]=5d0f6806  B[3]=85abb6fe  C[3]=9a2c3342  D[3]=4260c4aa

Step 30: (r=29, s= 9)
A[0]=ec87e075  B[0]=cc63a169  C[0]=89021820  D[0]=c862df8c
A[1]=59f8883e  B[1]=ffc7f78f  C[1]=c2848115  D[1]=c9be129f
A[2]=b905533d  B[2]=87911366  C[2]=b78414ff  D[2]=d3b576c3
A[3]=8b12e466  B[3]=cba1ed00  C[3]=85abb6fe  D[3]=9a2c3342

Step 31: (r= 9, s=15)
A[0]=2834e80e  B[0]=0fc0ebd9  C[0]=cc63a169  D[0]=89021820
A[1]=5892b6ed  B[1]=f1107cb3  C[1]=ffc7f78f  D[1]=c2848115
A[2]=78990dbf  B[2]=0aa67b72  C[2]=87911366  D[2]=b78414ff
A[3]=9934734b  B[3]=25c8cd16  C[3]=cba1ed00  D[3]=85abb6fe

Feed-Forward Step 0: (r=15, s= 5)
A[0]=dc342bf1  B[0]=7407141a  C[0]=0fc0ebd9  D[0]=cc63a169
A[1]=da7efc11  B[1]=5b76ac49  C[1]=f1107cb3  D[1]=ffc7f78f
A[2]=849cbdcc  B[2]=86dfbc4c  C[2]=0aa67b72  D[2]=87911366
A[3]=7a8c5ebd  B[3]=39a5cc9a  C[3]=25c8cd16  D[3]=cba1ed00

Feed-Forward Step 1: (r= 5, s=29)
A[0]=ec621b73  B[0]=86857e3b  C[0]=7407141a  D[0]=0fc0ebd9
A[1]=295cf686  B[1]=4fdf823b  C[1]=5b76ac49  D[1]=f1107cb3
A[2]=2ffb45bc  B[2]=9397b990  C[2]=86dfbc4c  D[2]=0aa67b72
A[3]=61b0d07c  B[3]=518bd7af  C[3]=39a5cc9a  D[3]=25c8cd16

Feed-Forward Step 2: (r=29, s= 9)
A[0]=cb208459  B[0]=7d8c436e  C[0]=86857e3b  D[0]=7407141a
```

```
A[1]=0f7f9a8d  B[1]=c52b9ed0  C[1]=4fdf823b  D[1]=5b76ac49
A[2]=c0e66fc7  B[2]=85ff68b7  C[2]=9397b990  D[2]=86dfbc4c
A[3]=30a0fe08  B[3]=8c361a0f  C[3]=518bd7af  D[3]=39a5cc9a

Feed-Forward Step 3: (r= 9, s=15)
A[0]=01233eee  B[0]=4108b396  C[0]=7d8c436e  D[0]=86857e3b
A[1]=e39a37f2  B[1]=ff351a1e  C[1]=c52b9ed0  D[1]=4fdf823b
A[2]=eb5e6115  B[2]=ccdf8f81  C[2]=85ff68b7  D[2]=9397b990
A[3]=d454270d  B[3]=41fc1061  C[3]=8c361a0f  D[3]=518bd7af
```

Compression Function Output

```
A[0]=01233eee  B[0]=4108b396  C[0]=7d8c436e  D[0]=86857e3b
A[1]=e39a37f2  B[1]=ff351a1e  C[1]=c52b9ed0  D[1]=4fdf823b
A[2]=eb5e6115  B[2]=ccdf8f81  C[2]=85ff68b7  D[2]=9397b990
A[3]=d454270d  B[3]=41fc1061  C[3]=8c361a0f  D[3]=518bd7af
```

Hash Function Output

```
ee 3e 23 01 f2 37 9a e3 15 61 5e eb 0d 27 54 d4
96 b3 08 41 1e 1a 35 ff 81 8f df cc
```

6.1.2 One block message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
y[ 24.. 31] =  124   92  110  120  191  202  211   82
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
```

```
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e341de07  0b534a0b  2aaf44d1  4bc99cb2
Z[17] = 124bc840  67a9c3e5  beab915f  0ecfe79c
Z[18] = a6472575  e5deeb18  6ce3ac60  9bd3edb5
Z[19] = 476e6c04  99365fd2  a489c682  0ecfd7ee
Z[20] = f052d7ee  fba5ae1e  1f5c0619  ef73a805
Z[21] = 273395ba  0df0f908  a3aad393  ea39d551
Z[22] = 4e66563d  e5deb437  cc9b93fc  0df036e1
Z[23] = 923e23b7  053aa2cb  d1d52f0a  f90821f9
Z[24] = 061916a6  468fd1d5  ab81923e  ff21476e
Z[25] = e95a931d  c682b971  f74ada8b  caddba50
Z[26] = 1d9e07d7  2c6d3f97  915fd472  a1eca726
Z[27] = 50245024  d0176888  4a0bd017  e4ff476e
Z[28] = 28f1db6a  cc9b1e7d  07d71cbf  f4add8cd
Z[29] = edb5e183  36e13c1b  ee942fe9  07d7d8cd
Z[30] = 4e664bc9  f210555e  ce59c3e5  6b25ba50
Z[31] = 00df2b8e  bc0e1b01  b892d1d5  a9c3dfc5
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
```

```
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 124bc840  67a9c3e5  beab915f  0ecfe79c
W[17] = a6472575  e5deeb18  6ce3ac60  9bd3edb5
W[18] = 923e23b7  053aa2cb  d1d52f0a  f90821f9
W[19] = f052d7ee  fba5ae1e  1f5c0619  ef73a805
W[20] = 4e66563d  e5deb437  cc9b93fc  0df036e1
W[21] = 273395ba  0df0f908  a3aad393  ea39d551
W[22] = e341de07  0b534a0b  2aaf44d1  4bc99cb2
W[23] = 476e6c04  99365fd2  a489c682  0ecfd7ee
W[24] = 4e664bc9  f210555e  ce59c3e5  6b25ba50
W[25] = 061916a6  468fd1d5  ab81923e  ff21476e
W[26] = e95a931d  c682b971  f74ada8b  caddba50
W[27] = 00df2b8e  bc0e1b01  b892d1d5  a9c3dfc5
W[28] = 50245024  d0176888  4a0bd017  e4ff476e
W[29] = edb5e183  36e13c1b  ee942fe9  07d7d8cd
W[30] = 28f1db6a  cc9b1e7d  07d71cbf  f4add8cd
W[31] = 1d9e07d7  2c6d3f97  915fd472  a1eca726
```

Feistel Steps

```
IV :
A[0]=eebfea74  B[0]=a22aad99  C[0]=20bcf05e  D[0]=9d4dda03
A[1]=70c30346  B[1]=434a528c  C[1]=9eb5b91a  D[1]=ae00fc41
A[2]=4b538718  B[2]=355e2a29  C[2]=4ddc22e8  D[2]=40279fc8
A[3]=4f06a655  B[3]=8523b76e  C[3]=ce0ae099  D[3]=9f0ec1f5

IV XOR M :
A[0]=edbdeb74  B[0]=b138bc89  C[0]=039ed17e  D[0]=ae7feb33
A[1]=77c50642  B[1]=545c4798  C[1]=b9939c3e  D[1]=9936c975
A[2]=40598e10  B[2]=2e443331  C[2]=66f60bc0  D[2]=7b1da6f0
A[3]=4008ab59  B[3]=9a3daa72  C[3]=e124cdb5  D[3]=a030fcc9

Step  0: (r= 3, s=20)
A[0]=de1b682b  B[0]=6def5ba7  C[0]=b138bc89  D[0]=039ed17e
A[1]=3f055e14  B[1]=be283213  C[1]=545c4798  D[1]=b9939c3e
A[2]=fd40f894  B[2]=02cc7082  C[2]=2e443331  D[2]=66f60bc0
A[3]=99f16941  B[3]=00455aca  C[3]=9a3daa72  D[3]=e124cdb5

Step  1: (r=20, s=14)
A[0]=06bafff9  B[0]=82bde1b6  C[0]=6def5ba7  D[0]=b138bc89
A[1]=30577ec5  B[1]=e143f055  C[1]=be283213  D[1]=545c4798
```

```
A[2]=0c2f2f8d  B[2]=894fd40f  C[2]=02cc7082  D[2]=2e443331
A[3]=92af9abd  B[3]=94199f16  C[3]=00455aca  D[3]=9a3daa72

Step  2: (r=14, s=27)
A[0]=61315825  B[0]=bffe41ae  C[0]=82bde1b6  D[0]=6def5ba7
A[1]=b2c71ab5  B[1]=dfb14c15  C[1]=e143f055  D[1]=be283213
A[2]=a59f92ad  B[2]=cbe3430b  C[2]=894fd40f  D[2]=02cc7082
A[3]=f32c9341  B[3]=e6af64ab  C[3]=94199f16  D[3]=00455aca

Step  3: (r=27, s= 3)
A[0]=2e97e015  B[0]=2b098ac1  C[0]=bffe41ae  D[0]=82bde1b6
A[1]=42f9ad20  B[1]=ad9638d5  C[1]=dfb14c15  D[1]=e143f055
A[2]=6e7d142c  B[2]=6d2cfc95  C[2]=cbe3430b  D[2]=894fd40f
A[3]=9400f679  B[3]=0f99649a  C[3]=e6af64ab  D[3]=94199f16

Step  4: (r= 3, s=20)
A[0]=159ad0fd  B[0]=74bf00a9  C[0]=2b098ac1  D[0]=bffe41ae
A[1]=6565172f  B[1]=17cd6902  C[1]=ad9638d5  D[1]=dfb14c15
A[2]=9234dad0  B[2]=73e8a163  C[2]=6d2cfc95  D[2]=cbe3430b
A[3]=74ceff0b  B[3]=a007b3cc  C[3]=0f99649a  D[3]=e6af64ab

Step  5: (r=20, s=14)
A[0]=87a49a60  B[0]=0fd159ad  C[0]=74bf00a9  D[0]=2b098ac1
A[1]=108c5ac4  B[1]=72f65651  C[1]=17cd6902  D[1]=ad9638d5
A[2]=1591b361  B[2]=ad09234d  C[2]=73e8a163  D[2]=6d2cfc95
A[3]=412990ff  B[3]=f0b74cef  C[3]=a007b3cc  D[3]=0f99649a

Step  6: (r=14, s=27)
A[0]=4a5adc0b  B[0]=269821e9  C[0]=0fd159ad  D[0]=74bf00a9
A[1]=05911c78  B[1]=16b10423  C[1]=72f65651  D[1]=17cd6902
A[2]=881793cc  B[2]=6cd84564  C[2]=ad09234d  D[2]=73e8a163
A[3]=7ff0408b  B[3]=643fd04a  C[3]=f0b74cef  D[3]=a007b3cc

Step  7: (r=27, s= 3)
A[0]=ae5a1d2f  B[0]=5a52d6e0  C[0]=269821e9  D[0]=0fd159ad
A[1]=fbb1debb  B[1]=c02c88e3  C[1]=16b10423  D[1]=72f65651
A[2]=61cd1e20  B[2]=6440bc9e  C[2]=6cd84564  D[2]=ad09234d
A[3]=97ab8bc1  B[3]=5bff8204  C[3]=643fd04a  D[3]=f0b74cef

Step  8: (r=26, s= 4)
A[0]=a5c1ff6b  B[0]=beb96874  C[0]=5a52d6e0  D[0]=269821e9
A[1]=6d156927  B[1]=efeec77a  C[1]=c02c88e3  D[1]=16b10423
A[2]=e7e4527c  B[2]=81873478  C[2]=6440bc9e  D[2]=6cd84564
A[3]=8d8afb85  B[3]=065eae2f  C[3]=5bff8204  D[3]=643fd04a

Step  9: (r= 4, s=23)
A[0]=83f8fbb1  B[0]=5c1ff6ba  C[0]=beb96874  D[0]=5a52d6e0
A[1]=389dc810  B[1]=d1569276  C[1]=efeec77a  D[1]=c02c88e3
A[2]=9ab5dc15  B[2]=7e4527ce  C[2]=81873478  D[2]=6440bc9e
```

```
A[3]=1da8beb9  B[3]=d8afb858  C[3]=065eae2f  D[3]=5bff8204

Step 10: (r=23, s=11)
A[0]=2e02e4a7  B[0]=d8c1fc7d  C[0]=5c1ff6ba  D[0]=beb96874
A[1]=13335e56  B[1]=081c4ee4  C[1]=d1569276  D[1]=efeec77a
A[2]=a467488d  B[2]=0acd5aee  C[2]=7e4527ce  D[2]=81873478
A[3]=aa2537e9  B[3]=5c8ed45f  C[3]=d8afb858  D[3]=065eae2f

Step 11: (r=11, s=26)
A[0]=9ab40a3e  B[0]=17253970  C[0]=d8c1fc7d  D[0]=5c1ff6ba
A[1]=396a7fce  B[1]=9af2b099  C[1]=081c4ee4  D[1]=d1569276
A[2]=d57c088e  B[2]=3a446d23  C[2]=0acd5aee  D[2]=7e4527ce
A[3]=386b82be  B[3]=29bf4d51  C[3]=5c8ed45f  D[3]=d8afb858

Step 12: (r=26, s= 4)
A[0]=7899903d  B[0]=fa6ad028  C[0]=17253970  D[0]=d8c1fc7d
A[1]=dd4c643d  B[1]=38e5a9ff  C[1]=9af2b099  D[1]=081c4ee4
A[2]=0e6552a3  B[2]=3b55f022  C[2]=3a446d23  D[2]=0acd5aee
A[3]=4f136036  B[3]=f8e1ae0a  C[3]=29bf4d51  D[3]=5c8ed45f

Step 13: (r= 4, s=23)
A[0]=83770986  B[0]=899903d7  C[0]=fa6ad028  D[0]=17253970
A[1]=8a1d4761  B[1]=d4c643dd  C[1]=38e5a9ff  D[1]=9af2b099
A[2]=c5345396  B[2]=e6552a30  C[2]=3b55f022  D[2]=3a446d23
A[3]=052ca5f4  B[3]=f1360364  C[3]=f8e1ae0a  D[3]=29bf4d51

Step 14: (r=23, s=11)
A[0]=48494c7c  B[0]=c341bb84  C[0]=899903d7  D[0]=fa6ad028
A[1]=6a59dced  B[1]=b0c50ea3  C[1]=d4c643dd  D[1]=38e5a9ff
A[2]=93cfec80  B[2]=cb629a29  C[2]=e6552a30  D[2]=3b55f022
A[3]=884e91ea  B[3]=fa029652  C[3]=f1360364  D[3]=f8e1ae0a

Step 15: (r=11, s=26)
A[0]=9776fd12  B[0]=4a63e242  C[0]=c341bb84  D[0]=899903d7
A[1]=6d07c3ce  B[1]=cee76b52  C[1]=b0c50ea3  D[1]=d4c643dd
A[2]=c9b99800  B[2]=7f64049e  C[2]=cb629a29  D[2]=e6552a30
A[3]=c00e9885  B[3]=748f5442  C[3]=fa029652  D[3]=f1360364

Step 16: (r=19, s=28)
A[0]=fc57f327  B[0]=e894bbb7  C[0]=4a63e242  D[0]=c341bb84
A[1]=1199c33e  B[1]=1e73683e  C[1]=cee76b52  D[1]=b0c50ea3
A[2]=53342c4f  B[2]=c0064dcc  C[2]=7f64049e  D[2]=cb629a29
A[3]=1035fbcc  B[3]=c42e0074  C[3]=748f5442  D[3]=fa029652

Step 17: (r=28, s= 7)
A[0]=d3fd72ed  B[0]=7fc57f32  C[0]=e894bbb7  D[0]=4a63e242
A[1]=4eb47c76  B[1]=e1199c33  C[1]=1e73683e  D[1]=cee76b52
A[2]=c4ef3204  B[2]=f53342c4  C[2]=c0064dcc  D[2]=7f64049e
A[3]=235dc330  B[3]=c1035fbc  C[3]=c42e0074  D[3]=748f5442
```

```
Step 18: (r= 7, s=22)
A[0]=a5145527  B[0]=feb976e9  C[0]=7fc57f32  D[0]=e894bbb7
A[1]=0d621fac  B[1]=5a3e3b27  C[1]=e1199c33  D[1]=1e73683e
A[2]=8be6ef31  B[2]=77990262  C[2]=f53342c4  D[2]=c0064dcc
A[3]=6a862597  B[3]=aee19811  C[3]=c1035fbc  D[3]=c42e0074

Step 19: (r=22, s=19)
A[0]=5b19b783  B[0]=49e94515  C[0]=feb976e9  D[0]=7fc57f32
A[1]=f272b42e  B[1]=eb035887  C[1]=5a3e3b27  D[1]=e1199c33
A[2]=0033fcaf  B[2]=cc62f9bb  C[2]=77990262  D[2]=f53342c4
A[3]=0096519f  B[3]=65daa189  C[3]=aee19811  D[3]=c1035fbc

Step 20: (r=19, s=28)
A[0]=a415e864  B[0]=bc1ad8cd  C[0]=49e94515  D[0]=feb976e9
A[1]=018aaa28  B[1]=a1779395  C[1]=eb035887  D[1]=5a3e3b27
A[2]=3d5831a8  B[2]=e578019f  C[2]=cc62f9bb  D[2]=77990262
A[3]=2b573b50  B[3]=8cf804b2  C[3]=65daa189  D[3]=aee19811

Step 21: (r=28, s= 7)
A[0]=873ff783  B[0]=4a415e86  C[0]=bc1ad8cd  D[0]=49e94515
A[1]=9c1ccdb9  B[1]=8018aaa2  C[1]=a1779395  D[1]=eb035887
A[2]=a845368a  B[2]=83d5831a  C[2]=e578019f  D[2]=cc62f9bb
A[3]=fae02405  B[3]=02b573b5  C[3]=8cf804b2  D[3]=65daa189

Step 22: (r= 7, s=22)
A[0]=7755ae8e  B[0]=9ffbc1c3  C[0]=4a415e86  D[0]=bc1ad8cd
A[1]=b378e21f  B[1]=0e66dcce  C[1]=8018aaa2  D[1]=a1779395
A[2]=f9b81ccd  B[2]=229b4554  C[2]=83d5831a  D[2]=e578019f
A[3]=5c0ae6db  B[3]=701202fd  C[3]=02b573b5  D[3]=8cf804b2

Step 23: (r=22, s=19)
A[0]=ce3984df  B[0]=a39dd56b  C[0]=9ffbc1c3  D[0]=4a415e86
A[1]=a684ebef  B[1]=87ecde38  C[1]=0e66dcce  D[1]=8018aaa2
A[2]=0f874241  B[2]=337e6e07  C[2]=229b4554  D[2]=83d5831a
A[3]=84dc3d09  B[3]=b6d702b9  C[3]=701202fd  D[3]=02b573b5

Step 24: (r=15, s= 5)
A[0]=0665c687  B[0]=c26fe71c  C[0]=a39dd56b  D[0]=9ffbc1c3
A[1]=c31c4cc3  B[1]=75f7d342  C[1]=87ecde38  D[1]=0e66dcce
A[2]=c83684fc  B[2]=a12087c3  C[2]=337e6e07  D[2]=229b4554
A[3]=18960768  B[3]=1e84c26e  C[3]=b6d702b9  D[3]=701202fd

Step 25: (r= 5, s=29)
A[0]=b012f593  B[0]=ccb8d0e0  C[0]=c26fe71c  D[0]=a39dd56b
A[1]=c61e5d26  B[1]=63899878  C[1]=75f7d342  D[1]=87ecde38
A[2]=7ce989aa  B[2]=06d09f99  C[2]=a12087c3  D[2]=337e6e07
A[3]=e948a224  B[3]=12c0ed03  C[3]=1e84c26e  D[3]=b6d702b9
```

```
Step 26: (r=29, s= 9)
A[0]=c539f442  B[0]=76025eb2  C[0]=ccb8d0e0  D[0]=c26fe71c
A[1]=020144b9  B[1]=d8c3cba4  C[1]=63899878  D[1]=75f7d342
A[2]=b0d9cba5  B[2]=4f9d3135  C[2]=06d09f99  D[2]=a12087c3
A[3]=693d05e2  B[3]=9d291444  C[3]=12c0ed03  D[3]=1e84c26e

Step 27: (r= 9, s=15)
A[0]=673d5348  B[0]=73e8858a  C[0]=76025eb2  D[0]=ccb8d0e0
A[1]=5d9d8e99  B[1]=02897204  C[1]=d8c3cba4  D[1]=63899878
A[2]=ab5335b0  B[2]=b3974b61  C[2]=4f9d3135  D[2]=06d09f99
A[3]=49c3e41d  B[3]=7a0bc4d2  C[3]=9d291444  D[3]=12c0ed03

Step 28: (r=15, s= 5)
A[0]=47fbc0a0  B[0]=a9a4339e  C[0]=73e8858a  D[0]=76025eb2
A[1]=2031c63a  B[1]=c74caece  C[1]=02897204  D[1]=d8c3cba4
A[2]=8082c120  B[2]=9ad855a9  C[2]=b3974b61  D[2]=4f9d3135
A[3]=c3234c48  B[3]=f20ea4e1  C[3]=7a0bc4d2  D[3]=9d291444

Step 29: (r= 5, s=29)
A[0]=094c3c47  B[0]=ff781408  C[0]=a9a4339e  D[0]=73e8858a
A[1]=069f66d1  B[1]=0638c744  C[1]=c74caece  D[1]=02897204
A[2]=f990884f  B[2]=10582410  C[2]=9ad855a9  D[2]=b3974b61
A[3]=391a5d7e  B[3]=64698918  C[3]=f20ea4e1  D[3]=7a0bc4d2

Step 30: (r=29, s= 9)
A[0]=adfdf166  B[0]=e1298788  C[0]=ff781408  D[0]=a9a4339e
A[1]=82209cb3  B[1]=20d3ecda  C[1]=0638c744  D[1]=c74caece
A[2]=53fb9e57  B[2]=ff321109  C[2]=10582410  D[2]=9ad855a9
A[3]=697fb745  B[3]=c7234baf  C[3]=64698918  D[3]=f20ea4e1

Step 31: (r= 9, s=15)
A[0]=df7b8904  B[0]=fbe2cd5b  C[0]=e1298788  D[0]=ff781408
A[1]=5d0a85c7  B[1]=41396704  C[1]=20d3ecda  D[1]=0638c744
A[2]=1af90d34  B[2]=f73caea7  C[2]=ff321109  D[2]=10582410
A[3]=acc3e3b7  B[3]=ff6e8ad2  C[3]=c7234baf  D[3]=64698918

Feed-Forward Step 0: (r=15, s= 5)
A[0]=76356f22  B[0]=c4826fbd  C[0]=fbe2cd5b  D[0]=e1298788
A[1]=a1410257  B[1]=42e3ae85  C[1]=41396704  D[1]=20d3ecda
A[2]=4e94c10b  B[2]=869a0d7c  C[2]=f73caea7  D[2]=ff321109
A[3]=1ed9b0b1  B[3]=f1dbd661  C[3]=ff6e8ad2  D[3]=c7234baf

Feed-Forward Step 1: (r= 5, s=29)
A[0]=1cbb05fc  B[0]=c6ade44e  C[0]=c4826fbd  D[0]=fbe2cd5b
A[1]=4fc90af0  B[1]=28204af4  C[1]=42e3ae85  D[1]=41396704
A[2]=a436f1a9  B[2]=d2982169  C[2]=869a0d7c  D[2]=f73caea7
A[3]=2fe91ea4  B[3]=db361623  C[3]=f1dbd661  D[3]=ff6e8ad2

Feed-Forward Step 2: (r=29, s= 9)
```

```
A[0]=9c512f20  B[0]=839760bf  C[0]=c6ade44e  D[0]=c4826fbd
A[1]=58250605  B[1]=09f9215e  C[1]=28204af4  D[1]=42e3ae85
A[2]=e7fb3d63  B[2]=3486de35  C[2]=d2982169  D[2]=869a0d7c
A[3]=dc1afa10  B[3]=85fd23d4  C[3]=db361623  D[3]=f1dbd661

Feed-Forward Step 3: (r= 9, s=15)
A[0]=0b91da16  B[0]=a25e4138  C[0]=839760bf  D[0]=c6ade44e
A[1]=2fd12e3a  B[1]=4a0c0ab0  C[1]=09f9215e  D[1]=28204af4
A[2]=87153ed9  B[2]=f67ac7cf  C[2]=3486de35  D[2]=d2982169
A[3]=a95096c3  B[3]=35f421b8  C[3]=85fd23d4  D[3]=db361623
```

Compression Function Output

```
A[0]=0b91da16  B[0]=a25e4138  C[0]=839760bf  D[0]=c6ade44e
A[1]=2fd12e3a  B[1]=4a0c0ab0  C[1]=09f9215e  D[1]=28204af4
A[2]=87153ed9  B[2]=f67ac7cf  C[2]=3486de35  D[2]=d2982169
A[3]=a95096c3  B[3]=35f421b8  C[3]=85fd23d4  D[3]=db361623
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
y[ 88.. 95] =  145  170  131  192  136  139   53   98
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc84037c  28f1d70f  5024afdc  1409ebf7
Z[17] = a80557fb  67a99857  e4201be0  65eb9a15
Z[18] = 3444cbbc  a2cb5d35  db6a2496  28f1d70f
Z[19] = 9e706190  923e6dc2  96996967  2e2bd1d5
Z[20] = e4201be0  c91f36e1  67a99857  4234bdcc
Z[21] = cd7a3286  484db7b3  e4201be0  c0693f97
Z[22] = cbbc3444  4234bdcc  476eb892  afdc5024
Z[23] = 0995f66b  ae1e51e2  f1310ecf  b3584ca8
Z[24] = 45b0ba50  d8cd2733  3cfac306  dd2822d8
Z[25] = e2621d9e  69679699  d3932c6d  124bedb5
Z[26] = fba5045b  2654d9ac  0faef052  b0bb4f45
Z[27] = b4374bc9  c761389f  993666ca  555eaaa2
Z[28] = 28f1d70f  5e14a1ec  5fd2a02e  2496db6a
Z[29] = fc84037c  203bdfc5  e0a41f5c  ae1e51e2
Z[30] = c5a33a5d  9a1565eb  aefd5103  6f809080
Z[31] = 1864e79c  dfc5203b  5c56a3aa  28f1d70f
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
```

```
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a80557fb  67a99857  e4201be0  65eb9a15
W[17] = 3444cbbc  a2cb5d35  db6a2496  28f1d70f
W[18] = 0995f66b  ae1e51e2  f1310ecf  b3584ca8
W[19] = e4201be0  c91f36e1  67a99857  4234bdcc
W[20] = cbbc3444  4234bdcc  476eb892  afdc5024
W[21] = cd7a3286  484db7b3  e4201be0  c0693f97
W[22] = fc84037c  28f1d70f  5024afdc  1409ebf7
W[23] = 9e706190  923e6dc2  96996967  2e2bd1d5
W[24] = c5a33a5d  9a1565eb  aefd5103  6f809080
W[25] = 45b0ba50  d8cd2733  3cfac306  dd2822d8
W[26] = e2621d9e  69679699  d3932c6d  124bedb5
W[27] = 1864e79c  dfc5203b  5c56a3aa  28f1d70f
W[28] = b4374bc9  c761389f  993666ca  555eaaa2
W[29] = fc84037c  203bdfc5  e0a41f5c  ae1e51e2
W[30] = 28f1d70f  5e14a1ec  5fd2a02e  2496db6a
W[31] = fba5045b  2654d9ac  0faef052  b0bb4f45
```

Feistel Steps

```
IV :
A[0]=0b91da16  B[0]=a25e4138  C[0]=839760bf  D[0]=c6ade44e
A[1]=2fd12e3a  B[1]=4a0c0ab0  C[1]=09f9215e  D[1]=28204af4
A[2]=87153ed9  B[2]=f67ac7cf  C[2]=3486de35  D[2]=d2982169
A[3]=a95096c3  B[3]=35f421b8  C[3]=85fd23d4  D[3]=db361623

IV XOR M :
A[0]=0b91d816  B[0]=a25e4138  C[0]=839760bf  D[0]=c6ade44e
A[1]=2fd12e3a  B[1]=4a0c0ab0  C[1]=09f9215e  D[1]=28204af4
A[2]=87153ed9  B[2]=f67ac7cf  C[2]=3486de35  D[2]=d2982169
A[3]=a95096c3  B[3]=35f421b8  C[3]=85fd23d4  D[3]=db361623

Step  0: (r= 3, s=20)
A[0]=40fbdea6  B[0]=5c8ec0b0  C[0]=a25e4138  D[0]=839760bf
A[1]=77a83a94  B[1]=7e8971d1  C[1]=4a0c0ab0  D[1]=09f9215e
A[2]=6ff850f6  B[2]=38a9f6cc  C[2]=f67ac7cf  D[2]=3486de35
A[3]=694cee50  B[3]=4a84b61d  C[3]=35f421b8  D[3]=85fd23d4

Step  1: (r=20, s=14)
A[0]=62dbe529  B[0]=ea640fbd  C[0]=5c8ec0b0  D[0]=a25e4138
A[1]=abcf4c12  B[1]=a9477a83  C[1]=7e8971d1  D[1]=4a0c0ab0
A[2]=c9141bd6  B[2]=0f66ff85  C[2]=38a9f6cc  D[2]=f67ac7cf
A[3]=2cc99c0f  B[3]=e50694ce  C[3]=4a84b61d  D[3]=35f421b8

Step  2: (r=14, s=27)
A[0]=823b3d41  B[0]=f94a58b6  C[0]=ea640fbd  D[0]=5c8ec0b0
A[1]=ea347d58  B[1]=d304aaf3  C[1]=a9477a83  D[1]=7e8971d1
```

```
A[2]=66f06758  B[2]=06f5b245  C[2]=0f66ff85  D[2]=38a9f6cc
A[3]=b71166ef  B[3]=6703cb32  C[3]=e50694ce  D[3]=4a84b61d

Step  3: (r=27, s= 3)
A[0]=070d03bc  B[0]=0c11d9ea  C[0]=f94a58b6  D[0]=ea640fbd
A[1]=8ddfdaf0  B[1]=c751a3ea  C[1]=d304aaf3  D[1]=a9477a83
A[2]=e9085943  B[2]=c337833a  C[2]=06f5b245  D[2]=0f66ff85
A[3]=61d4d631  B[3]=7db88b37  C[3]=6703cb32  D[3]=e50694ce

Step  4: (r= 3, s=20)
A[0]=878d0aaa  B[0]=38681de0  C[0]=0c11d9ea  D[0]=f94a58b6
A[1]=de7b7fc5  B[1]=6efed784  C[1]=c751a3ea  D[1]=d304aaf3
A[2]=ffbf11b4  B[2]=4842ca1f  C[2]=c337833a  D[2]=06f5b245
A[3]=31faa7e9  B[3]=0ea6b18b  C[3]=7db88b37  D[3]=6703cb32

Step  5: (r=20, s=14)
A[0]=02727dfe  B[0]=aaa878d0  C[0]=38681de0  D[0]=0c11d9ea
A[1]=9842415b  B[1]=fc5de7b7  C[1]=6efed784  D[1]=c751a3ea
A[2]=fdd173dc  B[2]=1b4ffbf1  C[2]=4842ca1f  D[2]=c337833a
A[3]=2545a1e2  B[3]=7e931faa  C[3]=0ea6b18b  D[3]=7db88b37

Step  6: (r=14, s=27)
A[0]=e401b356  B[0]=9f7f809c  C[0]=aaa878d0  D[0]=38681de0
A[1]=dc8c8da8  B[1]=9056e610  C[1]=fc5de7b7  D[1]=6efed784
A[2]=ac069805  B[2]=5cf73f74  C[2]=1b4ffbf1  D[2]=4842ca1f
A[3]=42aaf950  B[3]=68788951  C[3]=7e931faa  D[3]=0ea6b18b

Step  7: (r=27, s= 3)
A[0]=2680f24f  B[0]=b7200d9a  C[0]=9f7f809c  D[0]=aaa878d0
A[1]=2170a179  B[1]=46e4646d  C[1]=9056e610  D[1]=fc5de7b7
A[2]=024cf33e  B[2]=2d6034c0  C[2]=5cf73f74  D[2]=1b4ffbf1
A[3]=988c16e0  B[3]=821557ca  C[3]=68788951  D[3]=7e931faa

Step  8: (r=26, s= 4)
A[0]=cabdd85c  B[0]=3c9a03c9  C[0]=b7200d9a  D[0]=9f7f809c
A[1]=1889d6f3  B[1]=e485c285  C[1]=46e4646d  D[1]=9056e610
A[2]=d044eee7  B[2]=f80933cc  C[2]=2d6034c0  D[2]=5cf73f74
A[3]=4c920201  B[3]=8262305b  C[3]=821557ca  D[3]=68788951

Step  9: (r= 4, s=23)
A[0]=bf9e0b17  B[0]=abdd85cc  C[0]=3c9a03c9  D[0]=b7200d9a
A[1]=90f4424a  B[1]=889d6f31  C[1]=e485c285  D[1]=46e4646d
A[2]=0f5feed9  B[2]=044eee7d  C[2]=f80933cc  D[2]=2d6034c0
A[3]=3d361833  B[3]=c9202014  C[3]=8262305b  D[3]=821557ca

Step 10: (r=23, s=11)
A[0]=c50aae46  B[0]=8bdfcf05  C[0]=abdd85cc  D[0]=3c9a03c9
A[1]=a4530bc3  B[1]=25487a21  C[1]=889d6f31  D[1]=e485c285
A[2]=85ef7e95  B[2]=6c87aff7  C[2]=044eee7d  D[2]=f80933cc
```

```
A[3]=09584063  B[3]=199e9b0c  C[3]=c9202014  D[3]=8262305b

Step 11: (r=11, s=26)
A[0]=407dd670  B[0]=55723628  C[0]=8bdfcf05  D[0]=abdd85cc
A[1]=79c64d94  B[1]=985e1d22  C[1]=25487a21  D[1]=889d6f31
A[2]=6a2ed2bd  B[2]=7bf4ac2f  C[2]=6c87aff7  D[2]=044eee7d
A[3]=d118e6a6  B[3]=c203184a  C[3]=199e9b0c  D[3]=c9202014

Step 12: (r=26, s= 4)
A[0]=9ea84833  B[0]=c101f759  C[0]=55723628  D[0]=8bdfcf05
A[1]=8b7ae04b  B[1]=51e71936  C[1]=985e1d22  D[1]=25487a21
A[2]=3cfcc55e  B[2]=f5a8bb4a  C[2]=7bf4ac2f  D[2]=6c87aff7
A[3]=5782e253  B[3]=9b44639a  C[3]=c203184a  D[3]=199e9b0c

Step 13: (r= 4, s=23)
A[0]=79fb6470  B[0]=ea848339  C[0]=c101f759  D[0]=55723628
A[1]=179ae71c  B[1]=b7ae04b8  C[1]=51e71936  D[1]=985e1d22
A[2]=fd6cc3dc  B[2]=cfcc55e3  C[2]=f5a8bb4a  D[2]=7bf4ac2f
A[3]=0a825e9c  B[3]=782e2535  C[3]=9b44639a  D[3]=c203184a

Step 14: (r=23, s=11)
A[0]=4853b74d  B[0]=383cfdb2  C[0]=ea848339  D[0]=c101f759
A[1]=b52714df  B[1]=8e0bcd73  C[1]=b7ae04b8  D[1]=51e71936
A[2]=71123d66  B[2]=ee7eb661  C[2]=cfcc55e3  D[2]=f5a8bb4a
A[3]=6d4bea84  B[3]=4e05412f  C[3]=782e2535  D[3]=9b44639a

Step 15: (r=11, s=26)
A[0]=6dcde594  B[0]=9dba6a42  C[0]=383cfdb2  D[0]=ea848339
A[1]=d62648be  B[1]=38a6fda9  C[1]=8e0bcd73  D[1]=b7ae04b8
A[2]=5c41b2f1  B[2]=91eb3388  C[2]=ee7eb661  D[2]=cfcc55e3
A[3]=46364fb2  B[3]=5f54236a  C[3]=4e05412f  D[3]=782e2535

Step 16: (r=19, s=28)
A[0]=b0fad667  B[0]=2ca36e6f  C[0]=9dba6a42  D[0]=383cfdb2
A[1]=1b0358bc  B[1]=45f6b132  C[1]=38a6fda9  D[1]=8e0bcd73
A[2]=b3f8ec36  B[2]=978ae20d  C[2]=91eb3388  D[2]=ee7eb661
A[3]=bf665a96  B[3]=7d9231b2  C[3]=5f54236a  D[3]=4e05412f

Step 17: (r=28, s= 7)
A[0]=7d5b7990  B[0]=7b0fad66  C[0]=2ca36e6f  D[0]=9dba6a42
A[1]=aae65252  B[1]=c1b0358b  C[1]=45f6b132  D[1]=38a6fda9
A[2]=3576ef14  B[2]=6b3f8ec3  C[2]=978ae20d  D[2]=91eb3388
A[3]=c6555205  B[3]=6bf665a9  C[3]=7d9231b2  D[3]=5f54236a

Step 18: (r= 7, s=22)
A[0]=7a316839  B[0]=adbcc83e  C[0]=7b0fad66  D[0]=2ca36e6f
A[1]=e6e2a79a  B[1]=73292955  C[1]=c1b0358b  D[1]=45f6b132
A[2]=42b2b997  B[2]=bb778a1a  C[2]=6b3f8ec3  D[2]=978ae20d
A[3]=1f2068f2  B[3]=2aa902e3  C[3]=6bf665a9  D[3]=7d9231b2
```

```
Step 19: (r=22, s=19)
A[0]=243a7cc0  B[0]=0e5e8c5a  C[0]=adbcc83e  D[0]=7b0fad66
A[1]=05ab5a4a  B[1]=e6b9b8a9  C[1]=73292955  D[1]=c1b0358b
A[2]=540fdffa  B[2]=65d0acae  C[2]=bb778a1a  D[2]=6b3f8ec3
A[3]=92030e90  B[3]=3c87c81a  C[3]=2aa902e3  D[3]=6bf665a9

Step 20: (r=19, s=28)
A[0]=1980d83a  B[0]=e60121d3  C[0]=0e5e8c5a  D[0]=adbcc83e
A[1]=068b8338  B[1]=d2502d5a  C[1]=e6b9b8a9  D[1]=73292955
A[2]=6704ed78  B[2]=ffd2a07e  C[2]=65d0acae  D[2]=bb778a1a
A[3]=db667dd8  B[3]=74849018  C[3]=3c87c81a  D[3]=2aa902e3

Step 21: (r=28, s= 7)
A[0]=2231de1b  B[0]=a1980d83  C[0]=e60121d3  D[0]=0e5e8c5a
A[1]=95fb881e  B[1]=8068b833  C[1]=d2502d5a  D[1]=e6b9b8a9
A[2]=55c14986  B[2]=86704ed7  C[2]=ffd2a07e  D[2]=65d0acae
A[3]=4cf60166  B[3]=8db667dd  C[3]=74849018  D[3]=3c87c81a

Step 22: (r= 7, s=22)
A[0]=582f4c31  B[0]=18ef0d91  C[0]=a1980d83  D[0]=e60121d3
A[1]=d54ccc37  B[1]=fdc40f4a  C[1]=8068b833  D[1]=d2502d5a
A[2]=d324248f  B[2]=e0a4c32a  C[2]=86704ed7  D[2]=ffd2a07e
A[3]=74565f7e  B[3]=7b00b326  C[3]=8db667dd  D[3]=74849018

Step 23: (r=22, s=19)
A[0]=ab99b20d  B[0]=0c560bd3  C[0]=18ef0d91  D[0]=a1980d83
A[1]=1a16e470  B[1]=0df55333  C[1]=fdc40f4a  D[1]=8068b833
A[2]=8ff8d055  B[2]=23f4c909  C[2]=e0a4c32a  D[2]=86704ed7
A[3]=d94e5169  B[3]=df9d1597  C[3]=7b00b326  D[3]=8db667dd

Step 24: (r=15, s= 5)
A[0]=6862fb3a  B[0]=d906d5cc  C[0]=0c560bd3  D[0]=18ef0d91
A[1]=7277f2fd  B[1]=72380d0b  C[1]=0df55333  D[1]=fdc40f4a
A[2]=55014d5a  B[2]=682ac7fc  C[2]=23f4c909  D[2]=e0a4c32a
A[3]=e17c426b  B[3]=28b4eca7  C[3]=df9d1597  D[3]=7b00b326

Step 25: (r= 5, s=29)
A[0]=f5807e7f  B[0]=0c5f674d  C[0]=d906d5cc  D[0]=0c560bd3
A[1]=3a50746d  B[1]=4efe5fae  C[1]=72380d0b  D[1]=0df55333
A[2]=3c71f0be  B[2]=a029ab4a  C[2]=682ac7fc  D[2]=23f4c909
A[3]=01da2524  B[3]=2f884d7c  C[3]=28b4eca7  D[3]=df9d1597

Step 26: (r=29, s= 9)
A[0]=256c8c82  B[0]=feb00fcf  C[0]=0c5f674d  D[0]=d906d5cc
A[1]=721c339a  B[1]=a74a0e8d  C[1]=4efe5fae  D[1]=72380d0b
A[2]=e774c553  B[2]=c78e3e17  C[2]=a029ab4a  D[2]=682ac7fc
A[3]=2a51f606  B[3]=803b44a4  C[3]=2f884d7c  D[3]=28b4eca7
```

```
Step 27: (r= 9, s=15)
A[0]=8026369d  B[0]=d919044a  C[0]=feb00fcf  D[0]=0c5f674d
A[1]=61e54cc7  B[1]=386734e4  C[1]=a74a0e8d  D[1]=4efe5fae
A[2]=25f9ca11  B[2]=e98aa7ce  C[2]=c78e3e17  D[2]=a029ab4a
A[3]=41006084  B[3]=a3ec0c54  C[3]=803b44a4  D[3]=2f884d7c

Step 28: (r=15, s= 5)
A[0]=bf3aeda5  B[0]=1b4ec013  C[0]=d919044a  D[0]=feb00fcf
A[1]=dddd3542  B[1]=a663b0f2  C[1]=386734e4  D[1]=a74a0e8d
A[2]=0d9a25e3  B[2]=e50892fc  C[2]=e98aa7ce  D[2]=c78e3e17
A[3]=dd365453  B[3]=30422080  C[3]=a3ec0c54  D[3]=803b44a4

Step 29: (r= 5, s=29)
A[0]=860e974a  B[0]=e75db4b7  C[0]=1b4ec013  D[0]=d919044a
A[1]=37482ee1  B[1]=bba6a85b  C[1]=a663b0f2  D[1]=386734e4
A[2]=1a155563  B[2]=b344bc61  C[2]=e50892fc  D[2]=e98aa7ce
A[3]=979e9bb5  B[3]=a6ca8a7b  C[3]=30422080  D[3]=a3ec0c54

Step 30: (r=29, s= 9)
A[0]=d9c7deee  B[0]=50c1d2e9  C[0]=e75db4b7  D[0]=1b4ec013
A[1]=20423147  B[1]=26e905dc  C[1]=bba6a85b  D[1]=a663b0f2
A[2]=76ac8f6e  B[2]=6342aaac  C[2]=b344bc61  D[2]=e50892fc
A[3]=eba6b1e7  B[3]=b2f3d376  C[3]=a6ca8a7b  D[3]=30422080

Step 31: (r= 9, s=15)
A[0]=26cdd149  B[0]=8fbdddb3  C[0]=50c1d2e9  D[0]=e75db4b7
A[1]=a362c7a4  B[1]=84628e40  C[1]=26e905dc  D[1]=bba6a85b
A[2]=a89b11b1  B[2]=591edced  C[2]=6342aaac  D[2]=b344bc61
A[3]=8600d030  B[3]=4d63cfd7  C[3]=b2f3d376  D[3]=a6ca8a7b

Feed-Forward Step 0: (r=15, s= 5)
A[0]=937e9f7a  B[0]=e8a49366  C[0]=8fbdddb3  D[0]=50c1d2e9
A[1]=954471fb  B[1]=63d251b1  C[1]=84628e40  D[1]=26e905dc
A[2]=1eaefff0  B[2]=88d8d44d  C[2]=591edced  D[2]=6342aaac
A[3]=8a8125f6  B[3]=68184300  C[3]=4d63cfd7  D[3]=b2f3d376

Feed-Forward Step 1: (r= 5, s=29)
A[0]=65d8bb03  B[0]=6fd3ef52  C[0]=e8a49366  D[0]=8fbdddb3
A[1]=fe6fbcd8  B[1]=a88e3f72  C[1]=63d251b1  D[1]=84628e40
A[2]=843eb82b  B[2]=d5dffe03  C[2]=88d8d44d  D[2]=591edced
A[3]=8f579777  B[3]=5024bed1  C[3]=68184300  D[3]=4d63cfd7

Feed-Forward Step 2: (r=29, s= 9)
A[0]=b3a1a79d  B[0]=6cbb1760  C[0]=6fd3ef52  D[0]=e8a49366
A[1]=64e1f574  B[1]=1fcdf79b  C[1]=a88e3f72  D[1]=63d251b1
A[2]=fb59c523  B[2]=7087d705  C[2]=d5dffe03  D[2]=88d8d44d
A[3]=484f0fc6  B[3]=f1eaf2ee  C[3]=5024bed1  D[3]=68184300

Feed-Forward Step 3: (r= 9, s=15)
```

```
A[0]=97055618  B[0]=434f3b67  C[0]=6cbb1760  D[0]=6fd3ef52
A[1]=ebfb18f1  B[1]=c3eae8c9  C[1]=1fcdf79b  D[1]=a88e3f72
A[2]=bdab2363  B[2]=b38a47f6  C[2]=7087d705  D[2]=d5dffe03
A[3]=49e832a5  B[3]=9e1f8c90  C[3]=f1eaf2ee  D[3]=5024bed1
```

Compression Function Output

```
A[0]=97055618  B[0]=434f3b67  C[0]=6cbb1760  D[0]=6fd3ef52
A[1]=ebfb18f1  B[1]=c3eae8c9  C[1]=1fcdf79b  D[1]=a88e3f72
A[2]=bdab2363  B[2]=b38a47f6  C[2]=7087d705  D[2]=d5dffe03
A[3]=49e832a5  B[3]=9e1f8c90  C[3]=f1eaf2ee  D[3]=5024bed1
```

Hash Function Output

```
18 56 05 97 f1 18 fb eb 63 23 ab bd a5 32 e8 49
67 3b 4f 43 c9 e8 ea c3 f6 47 8a b3
```

6.1.3 Two blocks message

We use the message made of 700 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
y[ 88.. 95] =   32   58  213  108  189   44  222  244
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff21915f  ad3f52c1  e5de1a22  ebf71409
Z[17] = 6f809080  468fb971  f2ef0d11  65eb9a15
Z[18] = 37c0c840  b3584ca8  69679699  c3063cfa
Z[19] = 1be0e420  d9ac2654  c4c43b3c  e1831e7d
Z[20] = 0df0f210  ecd6132a  e2621d9e  60b19f4f
Z[21] = 06f8f908  f66b0995  f1310ecf  c0693f97
Z[22] = 037cfc84  6b2594db  68889778  5024afdc
Z[23] = 01befe42  c5a33a5d  3444cbbc  2812d7ee
Z[24] = bdcc9936  beab4e66  6a4606f8  bc0e31a7
Z[25] = 4f45a489  d47295ba  642d4aea  e4ff2e2b
Z[26] = 45b01d9e  ab811d9e  6888e95a  24960619
Z[27] = 32864155  5e143eb8  26546ea1  f4ad6888
Z[28] = f829a3aa  06f83cfa  93fcc840  d70fae1e
Z[29] = bced116c  c840dee6  ef734076  a8e4ecd6
Z[30] = ba502b8e  3cfaecd6  4a0b44d1  b5165024
Z[31] = 4234c91f  dd28aaa2  c5a32654  51e25024
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
```

```
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 6f809080  468fb971  f2ef0d11  65eb9a15
W[17] = 37c0c840  b3584ca8  69679699  c3063cfa
W[18] = 01befe42  c5a33a5d  3444cbbc  2812d7ee
W[19] = 0df0f210  ecd6132a  e2621d9e  60b19f4f
W[20] = 037cfc84  6b2594db  68889778  5024afdc
W[21] = 06f8f908  f66b0995  f1310ecf  c0693f97
W[22] = ff21915f  ad3f52c1  e5de1a22  ebf71409
W[23] = 1be0e420  d9ac2654  c4c43b3c  e1831e7d
W[24] = ba502b8e  3cfaecd6  4a0b44d1  b5165024
W[25] = bdcc9936  beab4e66  6a4606f8  bc0e31a7
W[26] = 4f45a489  d47295ba  642d4aea  e4ff2e2b
W[27] = 4234c91f  dd28aaa2  c5a32654  51e25024
W[28] = 32864155  5e143eb8  26546ea1  f4ad6888
W[29] = bced116c  c840dee6  ef734076  a8e4ecd6
W[30] = f829a3aa  06f83cfa  93fcc840  d70fae1e
W[31] = 45b01d9e  ab811d9e  6888e95a  24960619
```

Feistel Steps

```
IV :
A[0]=eebfea74  B[0]=a22aad99  C[0]=20bcf05e  D[0]=9d4dda03
A[1]=70c30346  B[1]=434a528c  C[1]=9eb5b91a  D[1]=ae00fc41
A[2]=4b538718  B[2]=355e2a29  C[2]=4ddc22e8  D[2]=40279fc8
A[3]=4f06a655  B[3]=8523b76e  C[3]=ce0ae099  D[3]=9f0ec1f5

IV XOR M :
A[0]=1140158b  B[0]=5dd55266  C[0]=df430fa1  D[0]=62b225fc
A[1]=8f3cfcb9  B[1]=bcb5ad73  C[1]=614a46e5  D[1]=51ff03be
A[2]=b4ac78e7  B[2]=caa1d5d6  C[2]=b223dd17  D[2]=bfd86037
A[3]=b0f959aa  B[3]=7adc4891  C[3]=31f51f66  D[3]=60f13e0a

Step  0: (r= 3, s=20)
A[0]=c2d73b8f  B[0]=8a00ac58  C[0]=5dd55266  D[0]=df430fa1
A[1]=c6fad7f9  B[1]=79e7e5cc  C[1]=bcb5ad73  D[1]=614a46e5
A[2]=71bc1119  B[2]=a563c73d  C[2]=caa1d5d6  D[2]=b223dd17
A[3]=53759a5b  B[3]=87cacd55  C[3]=7adc4891  D[3]=31f51f66

Step  1: (r=20, s=14)
A[0]=aee0845a  B[0]=b8fc2d73  C[0]=8a00ac58  D[0]=5dd55266
A[1]=dca869ec  B[1]=7f9c6fad  C[1]=79e7e5cc  D[1]=bcb5ad73
A[2]=0c0bd30a  B[2]=11971bc1  C[2]=a563c73d  D[2]=caa1d5d6
A[3]=290b57bb  B[3]=a5b53759  C[3]=87cacd55  D[3]=7adc4891

Step  2: (r=14, s=27)
A[0]=a806b841  B[0]=2116abb8  C[0]=b8fc2d73  D[0]=8a00ac58
A[1]=289f0200  B[1]=1a7b372a  C[1]=7f9c6fad  D[1]=79e7e5cc
```

```
A[2]=a17d3257  B[2]=f4c28302  C[2]=11971bc1  D[2]=a563c73d
A[3]=8b75237c  B[3]=d5eeca42  C[3]=a5b53759  D[3]=87cacd55

Step  3: (r=27, s= 3)
A[0]=599d43e8  B[0]=0d4035c2  C[0]=2116abb8  D[0]=b8fc2d73
A[1]=710851aa  B[1]=0144f810  C[1]=1a7b372a  D[1]=7f9c6fad
A[2]=28241034  B[2]=bd0be992  C[2]=f4c28302  D[2]=11971bc1
A[3]=9735a971  B[3]=e45ba91b  C[3]=d5eeca42  D[3]=a5b53759

Step  4: (r= 3, s=20)
A[0]=86dbd5f7  B[0]=ccea1f42  C[0]=0d4035c2  D[0]=2116abb8
A[1]=554522d2  B[1]=88428d53  C[1]=0144f810  D[1]=1a7b372a
A[2]=d12c21f3  B[2]=412081a1  C[2]=bd0be992  D[2]=f4c28302
A[3]=c3d5fa5d  B[3]=b9ad4b8c  C[3]=e45ba91b  D[3]=d5eeca42

Step  5: (r=20, s=14)
A[0]=8e29c1d7  B[0]=5f786dbd  C[0]=ccea1f42  D[0]=0d4035c2
A[1]=1fb7fd71  B[1]=2d255452  C[1]=88428d53  D[1]=0144f810
A[2]=abb82c96  B[2]=1f3d12c2  C[2]=412081a1  D[2]=bd0be992
A[3]=e7ad7e4b  B[3]=a5dc3d5f  C[3]=b9ad4b8c  D[3]=e45ba91b

Step  6: (r=14, s=27)
A[0]=c7eb2b50  B[0]=7075e38a  C[0]=5f786dbd  D[0]=ccea1f42
A[1]=85395297  B[1]=ff5c47ed  C[1]=2d255452  D[1]=88428d53
A[2]=20b352c4  B[2]=0b25aaee  C[2]=1f3d12c2  D[2]=412081a1
A[3]=1f7bed97  B[3]=5f92f9eb  C[3]=a5dc3d5f  D[3]=b9ad4b8c

Step  7: (r=27, s= 3)
A[0]=e51f0d6c  B[0]=863f595a  C[0]=7075e38a  D[0]=5f786dbd
A[1]=a3b12c7a  B[1]=bc29ca94  C[1]=ff5c47ed  D[1]=2d255452
A[2]=da1c534e  B[2]=21059a96  C[2]=0b25aaee  D[2]=1f3d12c2
A[3]=bad9718b  B[3]=b8fbdf6c  C[3]=5f92f9eb  D[3]=a5dc3d5f

Step  8: (r=26, s= 4)
A[0]=98d47443  B[0]=b3947c35  C[0]=863f595a  D[0]=7075e38a
A[1]=061f690d  B[1]=ea8ec4b1  C[1]=bc29ca94  D[1]=ff5c47ed
A[2]=2e6af214  B[2]=3b68714d  C[2]=21059a96  D[2]=0b25aaee
A[3]=2df7fc93  B[3]=2eeb65c6  C[3]=b8fbdf6c  D[3]=5f92f9eb

Step  9: (r= 4, s=23)
A[0]=c847b0fd  B[0]=8d474439  C[0]=b3947c35  D[0]=863f595a
A[1]=38839527  B[1]=61f690d0  C[1]=ea8ec4b1  D[1]=bc29ca94
A[2]=b5727432  B[2]=e6af2142  C[2]=3b68714d  D[2]=21059a96
A[3]=a9001df4  B[3]=df7fc932  C[3]=2eeb65c6  D[3]=b8fbdf6c

Step 10: (r=23, s=11)
A[0]=41255ba6  B[0]=7ee423d8  C[0]=8d474439  D[0]=b3947c35
A[1]=25b4ae5e  B[1]=939c41ca  C[1]=61f690d0  D[1]=ea8ec4b1
A[2]=9f6f1bba  B[2]=195ab93a  C[2]=e6af2142  D[2]=3b68714d
```

```
A[3]=03aacd0f  B[3]=fa54800e  C[3]=df7fc932  D[3]=2eeb65c6

Step 11: (r=11, s=26)
A[0]=ce021307  B[0]=2add3209  C[0]=7ee423d8  D[0]=8d474439
A[1]=aa414260  B[1]=a572f12d  C[1]=939c41ca  D[1]=61f690d0
A[2]=8f12a85d  B[2]=78ddd4fb  C[2]=195ab93a  D[2]=e6af2142
A[3]=3cc68082  B[3]=5668781d  C[3]=fa54800e  D[3]=df7fc932

Step 12: (r=26, s= 4)
A[0]=5f96412c  B[0]=1f38084c  C[0]=2add3209  D[0]=7ee423d8
A[1]=888d16bf  B[1]=82a90509  C[1]=a572f12d  D[1]=939c41ca
A[2]=3b500867  B[2]=763c4aa1  C[2]=78ddd4fb  D[2]=195ab93a
A[3]=9511e520  B[3]=08f31a02  C[3]=5668781d  D[3]=fa54800e

Step 13: (r= 4, s=23)
A[0]=8b33f407  B[0]=f96412c5  C[0]=1f38084c  D[0]=2add3209
A[1]=d3915530  B[1]=88d16bf8  C[1]=82a90509  D[1]=a572f12d
A[2]=e3a7113f  B[2]=b5008673  C[2]=763c4aa1  D[2]=78ddd4fb
A[3]=2fb4ad59  B[3]=511e5209  C[3]=08f31a02  D[3]=5668781d

Step 14: (r=23, s=11)
A[0]=83ee40a8  B[0]=03c599fa  C[0]=f96412c5  D[0]=1f38084c
A[1]=ffa84297  B[1]=9869c8aa  C[1]=88d16bf8  D[1]=82a90509
A[2]=7e0cd88b  B[2]=9ff1d388  C[2]=b5008673  D[2]=763c4aa1
A[3]=cec21ded  B[3]=ac97da56  C[3]=511e5209  D[3]=08f31a02

Step 15: (r=11, s=26)
A[0]=c8698c60  B[0]=7205441f  C[0]=03c599fa  D[0]=f96412c5
A[1]=aa281118  B[1]=4214bffd  C[1]=9869c8aa  D[1]=88d16bf8
A[2]=03cfedee  B[2]=66c45bf0  C[2]=9ff1d388  D[2]=b5008673
A[3]=70724ed8  B[3]=10ef6e76  C[3]=ac97da56  D[3]=511e5209

Step 16: (r=19, s=28)
A[0]=838beccd  B[0]=6306434c  C[0]=7205441f  D[0]=03c599fa
A[1]=ad8a4e71  B[1]=88c55140  C[1]=4214bffd  D[1]=9869c8aa
A[2]=bb31c288  B[2]=6f701e7f  C[2]=66c45bf0  D[2]=9ff1d388
A[3]=a8455ff3  B[3]=76c38392  C[3]=10ef6e76  D[3]=ac97da56

Step 17: (r=28, s= 7)
A[0]=d204687f  B[0]=d838becc  C[0]=6306434c  D[0]=7205441f
A[1]=6607e50a  B[1]=1ad8a4e7  C[1]=88c55140  D[1]=4214bffd
A[2]=7efb8b88  B[2]=8bb31c28  C[2]=6f701e7f  D[2]=66c45bf0
A[3]=5f761837  B[3]=3a8455ff  C[3]=76c38392  D[3]=10ef6e76

Step 18: (r= 7, s=22)
A[0]=6f4bb6ce  B[0]=02343fe9  C[0]=d838becc  D[0]=6306434c
A[1]=24ea626a  B[1]=03f28533  C[1]=1ad8a4e7  D[1]=88c55140
A[2]=c5f5cac0  B[2]=7dc5c43f  C[2]=8bb31c28  D[2]=6f701e7f
A[3]=891121df  B[3]=bb0c1baf  C[3]=3a8455ff  D[3]=76c38392
```

```
Step 19: (r=22, s=19)
A[0]=515196ad  B[0]=b39bd2ed  C[0]=02343fe9  D[0]=d838becc
A[1]=c06ec8b7  B[1]=9a893a98  C[1]=03f28533  D[1]=1ad8a4e7
A[2]=35c8dfbd  B[2]=b0317d72  C[2]=7dc5c43f  D[2]=8bb31c28
A[3]=5f0dd263  B[3]=77e24448  C[3]=bb0c1baf  D[3]=3a8455ff

Step 20: (r=19, s=28)
A[0]=24aa7899  B[0]=b56a8a8c  C[0]=b39bd2ed  D[0]=02343fe9
A[1]=4e783a6d  B[1]=45be0376  C[1]=9a893a98  D[1]=03f28533
A[2]=85bad17b  B[2]=fde9ae46  C[2]=b0317d72  D[2]=7dc5c43f
A[3]=1605e010  B[3]=931af86e  C[3]=77e24448  D[3]=bb0c1baf

Step 21: (r=28, s= 7)
A[0]=24656c76  B[0]=924aa789  C[0]=b56a8a8c  D[0]=b39bd2ed
A[1]=8c450025  B[1]=d4e783a6  C[1]=45be0376  D[1]=9a893a98
A[2]=eab2e79b  B[2]=b85bad17  C[2]=fde9ae46  D[2]=b0317d72
A[3]=11054aef  B[3]=01605e01  C[3]=931af86e  D[3]=77e24448

Step 22: (r= 7, s=22)
A[0]=d899dcca  B[0]=32b63b12  C[0]=924aa789  D[0]=b56a8a8c
A[1]=7936f9d9  B[1]=228012c6  C[1]=d4e783a6  D[1]=45be0376
A[2]=2d893a59  B[2]=5973cdf5  C[2]=b85bad17  D[2]=fde9ae46
A[3]=e2d3717e  B[3]=82a57788  C[3]=01605e01  D[3]=931af86e

Step 23: (r=22, s=19)
A[0]=07fe817f  B[0]=32b62677  C[0]=32b63b12  D[0]=924aa789
A[1]=4c3d3561  B[1]=765e4dbe  C[1]=228012c6  D[1]=d4e783a6
A[2]=e97606c3  B[2]=964b624e  C[2]=5973cdf5  D[2]=b85bad17
A[3]=e5fe09ba  B[3]=5fb8b4dc  C[3]=82a57788  D[3]=01605e01

Step 24: (r=15, s= 5)
A[0]=84d257ed  B[0]=40bf83ff  C[0]=32b62677  D[0]=32b63b12
A[1]=1330f90a  B[1]=9ab0a61e  C[1]=765e4dbe  D[1]=228012c6
A[2]=5a351ed1  B[2]=0361f4bb  C[2]=964b624e  D[2]=5973cdf5
A[3]=06c41bbe  B[3]=04dd72ff  C[3]=5fb8b4dc  D[3]=82a57788

Step 25: (r= 5, s=29)
A[0]=2b0af933  B[0]=9a4afdb0  C[0]=40bf83ff  D[0]=32b62677
A[1]=2378b87d  B[1]=661f2142  C[1]=9ab0a61e  D[1]=765e4dbe
A[2]=238fa6e1  B[2]=46a3da2b  C[2]=0361f4bb  D[2]=964b624e
A[3]=19b52d47  B[3]=d88377c0  C[3]=04dd72ff  D[3]=5fb8b4dc

Step 26: (r=29, s= 9)
A[0]=1bfd10a8  B[0]=65615f26  C[0]=9a4afdb0  D[0]=40bf83ff
A[1]=f68568e6  B[1]=a46f170f  C[1]=661f2142  D[1]=9ab0a61e
A[2]=9c358da2  B[2]=2471f4dc  C[2]=46a3da2b  D[2]=0361f4bb
A[3]=68175de9  B[3]=e336a5a8  C[3]=d88377c0  D[3]=04dd72ff
```

```
Step 27: (r= 9, s=15)
A[0]=90424764  B[0]=fa215037  C[0]=65615f26  D[0]=9a4afdb0
A[1]=579ee0cc  B[1]=0ad1cded  C[1]=a46f170f  D[1]=661f2142
A[2]=72ed5813  B[2]=6b1b4538  C[2]=2471f4dc  D[2]=46a3da2b
A[3]=00377197  B[3]=2ebbd2d0  C[3]=e336a5a8  D[3]=d88377c0

Step 28: (r=15, s= 5)
A[0]=16b8f146  B[0]=23b24821  C[0]=fa215037  D[0]=65615f26
A[1]=0e6e726f  B[1]=70662bcf  C[1]=0ad1cded  D[1]=a46f170f
A[2]=a6ff1cb4  B[2]=ac09b976  C[2]=6b1b4538  D[2]=2471f4dc
A[3]=10cc833e  B[3]=b8cb801b  C[3]=2ebbd2d0  D[3]=e336a5a8

Step 29: (r= 5, s=29)
A[0]=0a836eab  B[0]=d71e28c2  C[0]=23b24821  D[0]=fa215037
A[1]=a87333fe  B[1]=cdce4de1  C[1]=70662bcf  D[1]=0ad1cded
A[2]=af5e3312  B[2]=dfe39694  C[2]=ac09b976  D[2]=6b1b4538
A[3]=e66b3074  B[3]=199067c2  C[3]=b8cb801b  D[3]=2ebbd2d0

Step 30: (r=29, s= 9)
A[0]=8fc7706a  B[0]=61506dd5  C[0]=d71e28c2  D[0]=23b24821
A[1]=b6597456  B[1]=d50e667f  C[1]=cdce4de1  D[1]=70662bcf
A[2]=644e836a  B[2]=55ebc662  C[2]=dfe39694  D[2]=ac09b976
A[3]=8e92ef52  B[3]=9ccd660e  C[3]=199067c2  D[3]=b8cb801b

Step 31: (r= 9, s=15)
A[0]=04476d24  B[0]=8ee0d51f  C[0]=61506dd5  D[0]=d71e28c2
A[1]=fcd11db7  B[1]=b2e8ad6c  C[1]=d50e667f  D[1]=cdce4de1
A[2]=a37a0a5e  B[2]=9d06d4c8  C[2]=55ebc662  D[2]=dfe39694
A[3]=a9a3ea64  B[3]=25dea51d  C[3]=9ccd660e  D[3]=199067c2

Feed-Forward Step 0: (r=15, s= 5)
A[0]=f4a71fcd  B[0]=b6920223  C[0]=8ee0d51f  D[0]=61506dd5
A[1]=1127643b  B[1]=8edbfe68  C[1]=b2e8ad6c  D[1]=d50e667f
A[2]=0c8e9751  B[2]=052f51bd  C[2]=9d06d4c8  D[2]=55ebc662
A[3]=834846d6  B[3]=f53254d1  C[3]=25dea51d  D[3]=9ccd660e

Feed-Forward Step 1: (r= 5, s=29)
A[0]=ca1aa5d1  B[0]=94e3f9be  C[0]=b6920223  D[0]=8ee0d51f
A[1]=606d6f9e  B[1]=24ec8762  C[1]=8edbfe68  D[1]=b2e8ad6c
A[2]=18ef0202  B[2]=91d2ea21  C[2]=052f51bd  D[2]=9d06d4c8
A[3]=dddd87cc  B[3]=6908dad0  C[3]=f53254d1  D[3]=25dea51d

Feed-Forward Step 2: (r=29, s= 9)
A[0]=0ce00cbb  B[0]=394354ba  C[0]=94e3f9be  D[0]=b6920223
A[1]=7d19b041  B[1]=cc0dadf3  C[1]=24ec8762  D[1]=8edbfe68
A[2]=e6528afa  B[2]=431de040  C[2]=91d2ea21  D[2]=052f51bd
A[3]=61f46374  B[3]=9bbbb0f9  C[3]=6908dad0  D[3]=f53254d1

Feed-Forward Step 3: (r= 9, s=15)
```

```
A[0]=8e086bdd  B[0]=c0197619  C[0]=394354ba  D[0]=94e3f9be
A[1]=39cd2da8  B[1]=336082fa  C[1]=cc0dadf3  D[1]=24ec8762
A[2]=a8fcc28c  B[2]=a515f5cc  C[2]=431de040  D[2]=91d2ea21
A[3]=1b3bd1f6  B[3]=e8c6e8c3  C[3]=9bbbb0f9  D[3]=6908dad0
```

Compression Function Output

```
A[0]=8e086bdd  B[0]=c0197619  C[0]=394354ba  D[0]=94e3f9be
A[1]=39cd2da8  B[1]=336082fa  C[1]=cc0dadf3  D[1]=24ec8762
A[2]=a8fcc28c  B[2]=a515f5cc  C[2]=431de040  D[2]=91d2ea21
A[3]=1b3bd1f6  B[3]=e8c6e8c3  C[3]=9bbbb0f9  D[3]=6908dad0
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
```

```
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0c32c9fe  4155e87b  0df02d4c  9bd3ef73
Z[17] = ad3f0a74  ff21db6a  f131c761  4aea547f
Z[18] = 931d6ce3  1a22fc84  4e6643f2  e26260b1
Z[19] = e4ff4234  2c6dfd63  f74a2b8e  a647ecd6
Z[20] = 1cbfe341  60b15e14  108d2654  547f5d35
Z[21] = 2b8ea647  3523a10d  389f626f  2d4c468f
Z[22] = cf3830c8  fac6a10d  389fa3aa  cf38a568
Z[23] = 14e82c6d  cadda568  626f0619  484ddee6
Z[24] = 116c9e70  5a9828f1  db6ad0f6  d2b4f908
Z[25] = 555e53a0  d63094db  397ea1ec  116c4aea
Z[26] = 26543dd9  045b1943  26545e14  6dc20c32
Z[27] = a3aa3602  f908b892  2654116c  44d10df0
Z[28] = f2101cbf  9f4fe6bd  57fb5ef3  dc492496
Z[29] = 9a15f66b  b5f59699  65eb65eb  6dc2b7b3
Z[30] = edb56dc2  08b63602  f74a2c6d  d630d8cd
Z[31] = 28129af4  2fe90c32  52c1d630  cadd2812
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = ad3f0a74  ff21db6a  f131c761  4aea547f
W[17] = 931d6ce3  1a22fc84  4e6643f2  e26260b1
W[18] = 14e82c6d  cadda568  626f0619  484ddee6
W[19] = 1cbfe341  60b15e14  108d2654  547f5d35
```

```
W[20] = cf3830c8  fac6a10d  389fa3aa  cf38a568
W[21] = 2b8ea647  3523a10d  389f626f  2d4c468f
W[22] = 0c32c9fe  4155e87b  0df02d4c  9bd3ef73
W[23] = e4ff4234  2c6dfd63  f74a2b8e  a647ecd6
W[24] = edb56dc2  08b63602  f74a2c6d  d630d8cd
W[25] = 116c9e70  5a9828f1  db6ad0f6  d2b4f908
W[26] = 555e53a0  d63094db  397ea1ec  116c4aea
W[27] = 28129af4  2fe90c32  52c1d630  cadd2812
W[28] = a3aa3602  f908b892  2654116c  44d10df0
W[29] = 9a15f66b  b5f59699  65eb65eb  6dc2b7b3
W[30] = f2101cbf  9f4fe6bd  57fb5ef3  dc492496
W[31] = 26543dd9  045b1943  26545e14  6dc20c32
```

Feistel Steps

```
IV :
A[0]=8e086bdd  B[0]=c0197619  C[0]=394354ba  D[0]=94e3f9be
A[1]=39cd2da8  B[1]=336082fa  C[1]=cc0dadf3  D[1]=24ec8762
A[2]=a8fcc28c  B[2]=a515f5cc  C[2]=431de040  D[2]=91d2ea21
A[3]=1b3bd1f6  B[3]=e8c6e8c3  C[3]=9bbbb0f9  D[3]=6908dad0

IV XOR M :
A[0]=71f79422  B[0]=3fe689e6  C[0]=394354ba  D[0]=94e3f9be
A[1]=c632d257  B[1]=c39f7d05  C[1]=cc0dadf3  D[1]=24ec8762
A[2]=57033d73  B[2]=a515f5cc  C[2]=431de040  D[2]=91d2ea21
A[3]=e4c42e09  B[3]=e8c6e8c3  C[3]=9bbbb0f9  D[3]=6908dad0

Step  0: (r= 3, s=20)
A[0]=5b94fd08  B[0]=8fbca113  C[0]=3fe689e6  D[0]=394354ba
A[1]=e9578d0f  B[1]=319692be  C[1]=c39f7d05  D[1]=cc0dadf3
A[2]=18ffcbae  B[2]=b819eb9a  C[2]=a515f5cc  D[2]=431de040
A[3]=a104d741  B[3]=2621704f  C[3]=e8c6e8c3  D[3]=9bbbb0f9

Step  1: (r=20, s=14)
A[0]=c2a7c10e  B[0]=d085b94f  C[0]=8fbca113  D[0]=3fe689e6
A[1]=47e9176b  B[1]=d0fe9578  C[1]=319692be  D[1]=c39f7d05
A[2]=b561c293  B[2]=bae18ffc  C[2]=b819eb9a  D[2]=a515f5cc
A[3]=48a3ce76  B[3]=741a104d  C[3]=2621704f  D[3]=e8c6e8c3

Step  2: (r=14, s=27)
A[0]=03bf79eb  B[0]=f043b0a9  C[0]=d085b94f  D[0]=8fbca113
A[1]=63599d53  B[1]=45dad1fa  C[1]=d0fe9578  D[1]=319692be
A[2]=b551e05f  B[2]=70a4ed58  C[2]=bae18ffc  D[2]=b819eb9a
A[3]=9a8bc103  B[3]=f39d9228  C[3]=741a104d  D[3]=2621704f

Step  3: (r=27, s= 3)
A[0]=9627efae  B[0]=581dfbcf  C[0]=f043b0a9  D[0]=d085b94f
A[1]=e12d68a8  B[1]=9b1accea  C[1]=45dad1fa  D[1]=d0fe9578
A[2]=5e569b51  B[2]=fdaa8f02  C[2]=70a4ed58  D[2]=bae18ffc
```

```
A[3]=d1e5537b  B[3]=1cd45e08  C[3]=f39d9228  D[3]=741a104d

Step  4: (r= 3, s=20)
A[0]=a70010e4  B[0]=b13f7d74  C[0]=581dfbcf  D[0]=f043b0a9
A[1]=265e9e0b  B[1]=096b4547  C[1]=9b1accea  D[1]=45dad1fa
A[2]=d4dbe960  B[2]=f2b4da8a  C[2]=fdaa8f02  D[2]=70a4ed58
A[3]=2135f058  B[3]=8f2a9bde  C[3]=1cd45e08  D[3]=f39d9228

Step  5: (r=20, s=14)
A[0]=4e14f419  B[0]=0e4a7001  C[0]=b13f7d74  D[0]=581dfbcf
A[1]=596251d0  B[1]=e0b265e9  C[1]=096b4547  D[1]=9b1accea
A[2]=50cb5e7c  B[2]=960d4dbe  C[2]=f2b4da8a  D[2]=fdaa8f02
A[3]=ca74d71e  B[3]=0582135f  C[3]=8f2a9bde  D[3]=1cd45e08

Step  6: (r=14, s=27)
A[0]=f90c6b8e  B[0]=3d065385  C[0]=0e4a7001  D[0]=b13f7d74
A[1]=dce8f4b6  B[1]=94741658  C[1]=e0b265e9  D[1]=096b4547
A[2]=4cbd132c  B[2]=d79f1432  C[2]=960d4dbe  D[2]=f2b4da8a
A[3]=42c29291  B[3]=35c7b29d  C[3]=0582135f  D[3]=8f2a9bde

Step  7: (r=27, s= 3)
A[0]=ffd5b5c2  B[0]=77c8635c  C[0]=3d065385  D[0]=0e4a7001
A[1]=b5e2f3c0  B[1]=b6e747a5  C[1]=94741658  D[1]=e0b265e9
A[2]=51fe69d7  B[2]=6265e899  C[2]=d79f1432  D[2]=960d4dbe
A[3]=4f82ec4b  B[3]=8a161494  C[3]=35c7b29d  D[3]=0582135f

Step  8: (r=26, s= 4)
A[0]=7785d5b9  B[0]=0bff56d7  C[0]=77c8635c  D[0]=3d065385
A[1]=33d01072  B[1]=02d78bcf  C[1]=b6e747a5  D[1]=94741658
A[2]=3edfcd3b  B[2]=5d47f9a7  C[2]=6265e899  D[2]=d79f1432
A[3]=4745b5b8  B[3]=2d3e0bb1  C[3]=8a161494  D[3]=35c7b29d

Step  9: (r= 4, s=23)
A[0]=e7f6f10c  B[0]=785d5b97  C[0]=0bff56d7  D[0]=77c8635c
A[1]=f1662d45  B[1]=3d010723  C[1]=02d78bcf  D[1]=b6e747a5
A[2]=c6074592  B[2]=edfcd3b3  C[2]=5d47f9a7  D[2]=6265e899
A[3]=2e7f01d7  B[3]=745b5b84  C[3]=2d3e0bb1  D[3]=8a161494

Step 10: (r=23, s=11)
A[0]=519119ba  B[0]=8673fb78  C[0]=785d5b97  D[0]=0bff56d7
A[1]=da5e4074  B[1]=a2f8b316  C[1]=3d010723  D[1]=02d78bcf
A[2]=2b179bc5  B[2]=c96303a2  C[2]=edfcd3b3  D[2]=5d47f9a7
A[3]=09a68806  B[3]=eb973f80  C[3]=745b5b84  D[3]=2d3e0bb1

Step 11: (r=11, s=26)
A[0]=85e96c48  B[0]=88cdd28c  C[0]=8673fb78  D[0]=785d5b97
A[1]=9c159371  B[1]=f203a6d2  C[1]=a2f8b316  D[1]=3d010723
A[2]=2d0137af  B[2]=bcde2958  C[2]=c96303a2  D[2]=edfcd3b3
A[3]=4c19cf22  B[3]=3440304d  C[3]=eb973f80  D[3]=745b5b84
```

```
Step 12: (r=26, s= 4)
A[0]=081169d1  B[0]=2217a5b1  C[0]=88cdd28c  D[0]=8673fb78
A[1]=82efa0aa  B[1]=c670564d  C[1]=f203a6d2  D[1]=a2f8b316
A[2]=385f1888  B[2]=bcb404de  C[2]=bcde2958  D[2]=c96303a2
A[3]=1025305f  B[3]=8930673c  C[3]=3440304d  D[3]=eb973f80

Step 13: (r= 4, s=23)
A[0]=1b8e8703  B[0]=81169d10  C[0]=2217a5b1  D[0]=88cdd28c
A[1]=fce6fdb3  B[1]=2efa0aa8  C[1]=c670564d  D[1]=f203a6d2
A[2]=3b04042d  B[2]=85f18883  C[2]=bcb404de  D[2]=bcde2958
A[3]=e7a56d72  B[3]=025305f1  C[3]=8930673c  D[3]=3440304d

Step 14: (r=23, s=11)
A[0]=61e8b8db  B[0]=818dc743  C[0]=81169d10  D[0]=2217a5b1
A[1]=af76d126  B[1]=d9fe737e  C[1]=2efa0aa8  D[1]=c670564d
A[2]=aceb5f88  B[2]=169d8202  C[2]=85f18883  D[2]=bcb404de
A[3]=85771fd7  B[3]=b973d2b6  C[3]=025305f1  D[3]=8930673c

Step 15: (r=11, s=26)
A[0]=8d4e25d1  B[0]=45c6db0f  C[0]=818dc743  D[0]=81169d10
A[1]=4ef562bf  B[1]=b689357b  C[1]=d9fe737e  D[1]=2efa0aa8
A[2]=aab0aa08  B[2]=5afc4567  C[2]=169d8202  D[2]=85f18883
A[3]=a62906d5  B[3]=b8febc2b  C[3]=b973d2b6  D[3]=025305f1

Step 16: (r=19, s=28)
A[0]=893c4e53  B[0]=2e8c6a71  C[0]=45c6db0f  D[0]=818dc743
A[1]=2c9fc6fd  B[1]=15fa77ab  C[1]=b689357b  D[1]=d9fe737e
A[2]=a00b3646  B[2]=50455585  C[2]=5afc4567  D[2]=169d8202
A[3]=5ef7ed5a  B[3]=36ad3148  C[3]=b8febc2b  D[3]=b973d2b6

Step 17: (r=28, s= 7)
A[0]=27087514  B[0]=3893c4e5  C[0]=2e8c6a71  D[0]=45c6db0f
A[1]=03e3559a  B[1]=d2c9fc6f  C[1]=15fa77ab  D[1]=b689357b
A[2]=352151c4  B[2]=6a00b364  C[2]=50455585  D[2]=5afc4567
A[3]=147c6498  B[3]=a5ef7ed5  C[3]=36ad3148  D[3]=b8febc2b

Step 18: (r= 7, s=22)
A[0]=6a0b99d6  B[0]=843a8a13  C[0]=3893c4e5  D[0]=2e8c6a71
A[1]=d44ef22e  B[1]=f1aacd01  C[1]=d2c9fc6f  D[1]=15fa77ab
A[2]=6f79b7e2  B[2]=90a8e21a  C[2]=6a00b364  D[2]=50455585
A[3]=bc849897  B[3]=3e324c0a  C[3]=a5ef7ed5  D[3]=36ad3148

Step 19: (r=22, s=19)
A[0]=c7c6bda5  B[0]=759a82e6  C[0]=843a8a13  D[0]=3893c4e5
A[1]=35f16ae3  B[1]=8bb513bc  C[1]=f1aacd01  D[1]=d2c9fc6f
A[2]=64958abe  B[2]=f89bde6d  C[2]=90a8e21a  D[2]=6a00b364
A[3]=71b3587b  B[3]=25ef2126  C[3]=3e324c0a  D[3]=a5ef7ed5
```

```
Step 20: (r=19, s=28)
A[0]=a3f01790  B[0]=ed2e3e35  C[0]=759a82e6  D[0]=843a8a13
A[1]=2de7433d  B[1]=5719af8b  C[1]=8bb513bc  D[1]=f1aacd01
A[2]=8d0f2fae  B[2]=55f324ac  C[2]=f89bde6d  D[2]=90a8e21a
A[3]=67dbf4fb  B[3]=c3db8d9a  C[3]=25ef2126  D[3]=3e324c0a

Step 21: (r=28, s= 7)
A[0]=aa747a44  B[0]=0a3f0179  C[0]=ed2e3e35  D[0]=759a82e6
A[1]=f836a4ea  B[1]=d2de7433  C[1]=5719af8b  D[1]=8bb513bc
A[2]=7bf89c4c  B[2]=e8d0f2fa  C[2]=55f324ac  D[2]=f89bde6d
A[3]=7ffa9e1c  B[3]=b67dbf4f  C[3]=c3db8d9a  D[3]=25ef2126

Step 22: (r= 7, s=22)
A[0]=f19d785d  B[0]=3a3d2255  C[0]=0a3f0179  D[0]=ed2e3e35
A[1]=34f5f0a5  B[1]=1b52757c  C[1]=d2de7433  D[1]=5719af8b
A[2]=26af2d6f  B[2]=fc4e263d  C[2]=e8d0f2fa  D[2]=55f324ac
A[3]=282b9200  B[3]=fd4f0e3f  C[3]=b67dbf4f  D[3]=c3db8d9a

Step 23: (r=22, s=19)
A[0]=61fa0f20  B[0]=177c675e  C[0]=3a3d2255  D[0]=0a3f0179
A[1]=8926bdd5  B[1]=294d3d7c  C[1]=1b52757c  D[1]=d2de7433
A[2]=cd4637b9  B[2]=5bc9abcb  C[2]=fc4e263d  D[2]=e8d0f2fa
A[3]=ed467214  B[3]=800a0ae4  C[3]=fd4f0e3f  D[3]=b67dbf4f

Step 24: (r=15, s= 5)
A[0]=cd1d9695  B[0]=079030fd  C[0]=177c675e  D[0]=3a3d2255
A[1]=f901dce1  B[1]=5eeac493  C[1]=294d3d7c  D[1]=1b52757c
A[2]=6572d52e  B[2]=1bdce6a3  C[2]=5bc9abcb  D[2]=fc4e263d
A[3]=9ec4fa60  B[3]=390a76a3  C[3]=800a0ae4  D[3]=fd4f0e3f

Step 25: (r= 5, s=29)
A[0]=3abdec20  B[0]=a3b2d2b9  C[0]=079030fd  D[0]=177c675e
A[1]=32663c94  B[1]=203b9c3f  C[1]=5eeac493  D[1]=294d3d7c
A[2]=82252f7b  B[2]=ae5aa5cc  C[2]=1bdce6a3  D[2]=5bc9abcb
A[3]=9d3d6b7c  B[3]=d89f4c13  C[3]=390a76a3  D[3]=800a0ae4

Step 26: (r=29, s= 9)
A[0]=9d64bebb  B[0]=0757bd84  C[0]=a3b2d2b9  D[0]=079030fd
A[1]=c1a182c7  B[1]=864cc792  C[1]=203b9c3f  D[1]=5eeac493
A[2]=d60eabd1  B[2]=7044a5ef  C[2]=ae5aa5cc  D[2]=1bdce6a3
A[3]=32bc8017  B[3]=93a7ad6f  C[3]=d89f4c13  D[3]=390a76a3

Step 27: (r= 9, s=15)
A[0]=01904f68  B[0]=c97d773a  C[0]=0757bd84  D[0]=a3b2d2b9
A[1]=b0bfc5dc  B[1]=43058f83  C[1]=864cc792  D[1]=203b9c3f
A[2]=7acdeab3  B[2]=1d57a3ac  C[2]=7044a5ef  D[2]=ae5aa5cc
A[3]=f863feca  B[3]=79002e65  C[3]=93a7ad6f  D[3]=d89f4c13

Step 28: (r=15, s= 5)
```

```
A[0]=f93f54c8  B[0]=27b400c8  C[0]=c97d773a  D[0]=0757bd84
A[1]=5f9d49d9  B[1]=e2ee585f  C[1]=43058f83  D[1]=864cc792
A[2]=9df0d91a  B[2]=f559bd66  C[2]=1d57a3ac  D[2]=7044a5ef
A[3]=fa350f0a  B[3]=ff657c31  C[3]=79002e65  D[3]=93a7ad6f

Step 29: (r= 5, s=29)
A[0]=af708469  B[0]=27ea991f  C[0]=27b400c8  D[0]=c97d773a
A[1]=169bd65f  B[1]=f3a93b2b  C[1]=e2ee585f  D[1]=43058f83
A[2]=365ad1c0  B[2]=be1b2353  C[2]=f559bd66  D[2]=1d57a3ac
A[3]=733b2d93  B[3]=46a1e15f  C[3]=ff657c31  D[3]=79002e65

Step 30: (r=29, s= 9)
A[0]=defc0091  B[0]=35ee108d  C[0]=27ea991f  D[0]=27b400c8
A[1]=086c99e2  B[1]=e2d37acb  C[1]=f3a93b2b  D[1]=e2ee585f
A[2]=cbcf2809  B[2]=06cb5a38  C[2]=be1b2353  D[2]=f559bd66
A[3]=0b6e2e25  B[3]=6e6765b2  C[3]=46a1e15f  D[3]=ff657c31

Step 31: (r= 9, s=15)
A[0]=c5ef5692  B[0]=f80123bd  C[0]=35ee108d  D[0]=27ea991f
A[1]=33232f2f  B[1]=d933c410  C[1]=e2d37acb  D[1]=f3a93b2b
A[2]=9acaf8f9  B[2]=9e501397  C[2]=06cb5a38  D[2]=be1b2353
A[3]=500121d7  B[3]=dc5c4a16  C[3]=6e6765b2  D[3]=46a1e15f

Feed-Forward Step 0: (r=15, s= 5)
A[0]=56188cc5  B[0]=ab4962f7  C[0]=f80123bd  D[0]=35ee108d
A[1]=69b47fe4  B[1]=97979991  C[1]=d933c410  D[1]=e2d37acb
A[2]=3c0ab600  B[2]=7c7ccd65  C[2]=9e501397  D[2]=06cb5a38
A[3]=b3c85473  B[3]=90eba800  C[3]=dc5c4a16  D[3]=6e6765b2

Feed-Forward Step 1: (r= 5, s=29)
A[0]=f558d55b  B[0]=c31198aa  C[0]=ab4962f7  D[0]=f80123bd
A[1]=2e040160  B[1]=368ffc8d  C[1]=97979991  D[1]=d933c410
A[2]=3058d35d  B[2]=8156c007  C[2]=7c7ccd65  D[2]=9e501397
A[3]=5d11479c  B[3]=790a8e76  C[3]=90eba800  D[3]=dc5c4a16

Feed-Forward Step 2: (r=29, s= 9)
A[0]=b216cc24  B[0]=7eab1aab  C[0]=c31198aa  D[0]=ab4962f7
A[1]=58204324  B[1]=05c0802c  C[1]=368ffc8d  D[1]=97979991
A[2]=5122214e  B[2]=a60b1a6b  C[2]=8156c007  D[2]=7c7ccd65
A[3]=83fd614f  B[3]=8ba228f3  C[3]=790a8e76  D[3]=90eba800

Feed-Forward Step 3: (r= 9, s=15)
A[0]=7ef2763a  B[0]=2d984964  C[0]=7eab1aab  D[0]=c31198aa
A[1]=e9931090  B[1]=408648b0  C[1]=05c0802c  D[1]=368ffc8d
A[2]=698110b7  B[2]=44429ca2  C[2]=a60b1a6b  D[2]=8156c007
A[3]=d928437b  B[3]=fac29f07  C[3]=8ba228f3  D[3]=790a8e76
```

Compression Function Output

```
A[0]=7ef2763a  B[0]=2d984964  C[0]=7eab1aab  D[0]=c31198aa
```

```
A[1]=e9931090  B[1]=408648b0  C[1]=05c0802c  D[1]=368ffc8d
A[2]=698110b7  B[2]=44429ca2  C[2]=a60b1a6b  D[2]=8156c007
A[3]=d928437b  B[3]=fac29f07  C[3]=8ba228f3  D[3]=790a8e76
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
```

```
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = c069c761  ecd69af4  140953a0  d7eeafdc
Z[17] = 4bc91be0  2b8e3c1b  a805dfc5  29d03dd9
Z[18] = f8296f80  468f211a  9f4fe87b  ecd69af4
Z[19] = 42342575  360231a7  3a5d2d4c  f21095ba
Z[20] = a805dfc5  6ce3fac6  2b8e3c1b  06196190
Z[21] = 915ff66b  0c325b77  a805dfc5  642d037c
Z[22] = 6f80f829  06196190  0b535c56  53a01409
Z[23] = cd7aba50  51e215c7  b516d2b4  571c108d
Z[24] = 09955e14  9cb2eb18  00df66ca  a10de6bd
Z[25] = a647e183  2d4c3a5d  9778f052  d630b19a
Z[26] = bf8ac840  ea399d91  d393b437  547f132a
Z[27] = 57fb0fae  6b25fc84  3cfa2aaf  19434e66
Z[28] = ecd69af4  21f945b0  23b743f2  e87b9f4f
Z[29] = c069c761  e420a3aa  a489e341  51e215c7
Z[30] = 6967fe42  3dd929d0  52c114e8  33653444
Z[31] = dc49ab81  a3aae420  203b476e  ecd69af4
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4bc91be0  2b8e3c1b  a805dfc5  29d03dd9
W[17] = f8296f80  468f211a  9f4fe87b  ecd69af4
W[18] = cd7aba50  51e215c7  b516d2b4  571c108d
W[19] = a805dfc5  6ce3fac6  2b8e3c1b  06196190
W[20] = 6f80f829  06196190  0b535c56  53a01409
W[21] = 915ff66b  0c325b77  a805dfc5  642d037c
W[22] = c069c761  ecd69af4  140953a0  d7eeafdc
W[23] = 42342575  360231a7  3a5d2d4c  f21095ba
W[24] = 6967fe42  3dd929d0  52c114e8  33653444
W[25] = 09955e14  9cb2eb18  00df66ca  a10de6bd
W[26] = a647e183  2d4c3a5d  9778f052  d630b19a
W[27] = dc49ab81  a3aae420  203b476e  ecd69af4
```

```
W[28] = 57fb0fae  6b25fc84  3cfa2aaf  19434e66
W[29] = c069c761  e420a3aa  a489e341  51e215c7
W[30] = ecd69af4  21f945b0  23b743f2  e87b9f4f
W[31] = bf8ac840  ea399d91  d393b437  547f132a
```

Feistel Steps

```
IV :
A[0]=7ef2763a  B[0]=2d984964  C[0]=7eab1aab  D[0]=c31198aa
A[1]=e9931090  B[1]=408648b0  C[1]=05c0802c  D[1]=368ffc8d
A[2]=698110b7  B[2]=44429ca2  C[2]=a60b1a6b  D[2]=8156c007
A[3]=d928437b  B[3]=fac29f07  C[3]=8ba228f3  D[3]=790a8e76

IV XOR M :
A[0]=7ef27486  B[0]=2d984964  C[0]=7eab1aab  D[0]=c31198aa
A[1]=e9931090  B[1]=408648b0  C[1]=05c0802c  D[1]=368ffc8d
A[2]=698110b7  B[2]=44429ca2  C[2]=a60b1a6b  D[2]=8156c007
A[3]=d928437b  B[3]=fac29f07  C[3]=8ba228f3  D[3]=790a8e76

Step  0: (r= 3, s=20)
A[0]=ce424203  B[0]=f793a433  C[0]=2d984964  D[0]=7eab1aab
A[1]=db43d7f2  B[1]=4c988487  C[1]=408648b0  D[1]=05c0802c
A[2]=962a17ce  B[2]=4c0885bb  C[2]=44429ca2  D[2]=a60b1a6b
A[3]=a623d993  B[3]=c9421bde  C[3]=fac29f07  D[3]=8ba228f3

Step  1: (r=20, s=14)
A[0]=844dbbd6  B[0]=203ce424  C[0]=f793a433  D[0]=2d984964
A[1]=f0a1fe7a  B[1]=7f2db43d  C[1]=4c988487  D[1]=408648b0
A[2]=1d68e30e  B[2]=7ce962a1  C[2]=4c0885bb  D[2]=44429ca2
A[3]=9577d82d  B[3]=993a623d  C[3]=c9421bde  D[3]=fac29f07

Step  2: (r=14, s=27)
A[0]=0718da1c  B[0]=6ef5a113  C[0]=203ce424  D[0]=f793a433
A[1]=061ecca6  B[1]=7f9ebc28  C[1]=7f2db43d  D[1]=4c988487
A[2]=95baefa2  B[2]=38c3875a  C[2]=7ce962a1  D[2]=4c0885bb
A[3]=c4eda617  B[3]=f60b655d  C[3]=993a623d  D[3]=c9421bde

Step  3: (r=27, s= 3)
A[0]=90f2fe9c  B[0]=e038c6d0  C[0]=6ef5a113  D[0]=203ce424
A[1]=8fa24ee3  B[1]=3030f665  C[1]=7f9ebc28  D[1]=7f2db43d
A[2]=0fa890ac  B[2]=14add77d  C[2]=38c3875a  D[2]=7ce962a1
A[3]=e25258a2  B[3]=be276d30  C[3]=f60b655d  D[3]=993a623d

Step  4: (r= 3, s=20)
A[0]=8b5e2875  B[0]=8797f4e4  C[0]=e038c6d0  D[0]=6ef5a113
A[1]=c83f016c  B[1]=7d12771c  C[1]=3030f665  D[1]=7f9ebc28
A[2]=5b301274  B[2]=7d448560  C[2]=14add77d  D[2]=38c3875a
A[3]=5a1bab81  B[3]=1292c517  C[3]=be276d30  D[3]=f60b655d
```

```
Step  5: (r=20, s=14)
A[0]=46cae3c8  B[0]=8758b5e2  C[0]=8797f4e4  D[0]=e038c6d0
A[1]=97f30c87  B[1]=16cc83f0  C[1]=7d12771c  D[1]=3030f665
A[2]=885d1566  B[2]=2745b301  C[2]=7d448560  D[2]=14add77d
A[3]=2c210c7c  B[3]=b815a1ba  C[3]=1292c517  D[3]=be276d30

Step  6: (r=14, s=27)
A[0]=deca94da  B[0]=b8f211b2  C[0]=8758b5e2  D[0]=8797f4e4
A[1]=97829b50  B[1]=c321e5fc  C[1]=16cc83f0  D[1]=7d12771c
A[2]=ce49ef9b  B[2]=4559a217  C[2]=2745b301  D[2]=7d448560
A[3]=daac2e84  B[3]=431f0b08  C[3]=b815a1ba  D[3]=1292c517

Step  7: (r=27, s= 3)
A[0]=47af5f2c  B[0]=d6f654a6  C[0]=b8f211b2  D[0]=8758b5e2
A[1]=4ec6c8be  B[1]=84bc14da  C[1]=c321e5fc  D[1]=16cc83f0
A[2]=935ec25b  B[2]=de724f7c  C[2]=4559a217  D[2]=2745b301
A[3]=e1ed344f  B[3]=26d56174  C[3]=431f0b08  D[3]=b815a1ba

Step  8: (r=26, s= 4)
A[0]=84292608  B[0]=b11ebd7c  C[0]=d6f654a6  D[0]=b8f211b2
A[1]=6bcc568d  B[1]=f93b1b22  C[1]=84bc14da  D[1]=c321e5fc
A[2]=c4f52842  B[2]=6e4d7b09  C[2]=de724f7c  D[2]=4559a217
A[3]=619011a8  B[3]=3f87b4d1  C[3]=26d56174  D[3]=431f0b08

Step  9: (r= 4, s=23)
A[0]=f5bceb0a  B[0]=42926088  C[0]=b11ebd7c  D[0]=d6f654a6
A[1]=a705b918  B[1]=bcc568d6  C[1]=f93b1b22  D[1]=84bc14da
A[2]=21fd7c28  B[2]=4f52842c  C[2]=6e4d7b09  D[2]=de724f7c
A[3]=e305560e  B[3]=19011a86  C[3]=3f87b4d1  D[3]=26d56174

Step 10: (r=23, s=11)
A[0]=a854ab19  B[0]=857ade75  C[0]=42926088  D[0]=b11ebd7c
A[1]=68dc0ba7  B[1]=8c5382dc  C[1]=bcc568d6  D[1]=f93b1b22
A[2]=2347bd06  B[2]=1410febe  C[2]=4f52842c  D[2]=6e4d7b09
A[3]=3645affb  B[3]=077182ab  C[3]=19011a86  D[3]=3f87b4d1

Step 11: (r=11, s=26)
A[0]=6fd7c667  B[0]=a558cd42  C[0]=857ade75  D[0]=42926088
A[1]=6e8c876a  B[1]=e05d3b46  C[1]=8c5382dc  D[1]=bcc568d6
A[2]=00452a61  B[2]=3de8311a  C[2]=1410febe  D[2]=4f52842c
A[3]=e85d4fdf  B[3]=2d7fd9b2  C[3]=077182ab  D[3]=19011a86

Step 12: (r=26, s= 4)
A[0]=81a10f06  B[0]=9dbf5f19  C[0]=a558cd42  D[0]=857ade75
A[1]=6f721915  B[1]=a9ba321d  C[1]=e05d3b46  D[1]=8c5382dc
A[2]=4d58cbcf  B[2]=840114a9  C[2]=3de8311a  D[2]=1410febe
A[3]=daafee2b  B[3]=7fa1753f  C[3]=2d7fd9b2  D[3]=077182ab

Step 13: (r= 4, s=23)
```

```
A[0]=adf7f6dc  B[0]=1a10f068  C[0]=9dbf5f19  D[0]=a558cd42
A[1]=b2ae39a1  B[1]=f7219156  C[1]=a9ba321d  D[1]=e05d3b46
A[2]=c07baccb  B[2]=d58cbcf4  C[2]=840114a9  D[2]=3de8311a
A[3]=7807193f  B[3]=aafee2bd  C[3]=7fa1753f  D[3]=2d7fd9b2

Step 14: (r=23, s=11)
A[0]=8ec21f88  B[0]=6e56fbfb  C[0]=1a10f068  D[0]=9dbf5f19
A[1]=1b1761e5  B[1]=d0d9571c  C[1]=f7219156  D[1]=a9ba321d
A[2]=5caa6a74  B[2]=65e03dd6  C[2]=d58cbcf4  D[2]=840114a9
A[3]=782f5b6d  B[3]=9fbc038c  C[3]=aafee2bd  D[3]=7fa1753f

Step 15: (r=11, s=26)
A[0]=5761b1c3  B[0]=10fc4476  C[0]=6e56fbfb  D[0]=1a10f068
A[1]=7d9bd5e3  B[1]=bb0f28d8  C[1]=d0d9571c  D[1]=f7219156
A[2]=197585e2  B[2]=5353a2e5  C[2]=65e03dd6  D[2]=d58cbcf4
A[3]=eca334d1  B[3]=7adb6bc1  C[3]=9fbc038c  D[3]=aafee2bd

Step 16: (r=19, s=28)
A[0]=d900f24a  B[0]=8e1abb0d  C[0]=10fc4476  D[0]=6e56fbfb
A[1]=0cd078b0  B[1]=af1becde  C[1]=bb0f28d8  D[1]=d0d9571c
A[2]=85c5aa73  B[2]=2f10cbac  C[2]=5353a2e5  D[2]=65e03dd6
A[3]=c3219f53  B[3]=a68f6519  C[3]=7adb6bc1  D[3]=9fbc038c

Step 17: (r=28, s= 7)
A[0]=f6ed369e  B[0]=ad900f24  C[0]=8e1abb0d  D[0]=10fc4476
A[1]=8022a160  B[1]=00cd078b  C[1]=af1becde  D[1]=bb0f28d8
A[2]=cee889d2  B[2]=385c5aa7  C[2]=2f10cbac  D[2]=5353a2e5
A[3]=b7cf102e  B[3]=3c3219f5  C[3]=a68f6519  D[3]=7adb6bc1

Step 18: (r= 7, s=22)
A[0]=843372a3  B[0]=769b4f7b  C[0]=ad900f24  D[0]=8e1abb0d
A[1]=8393ec0a  B[1]=1150b040  C[1]=00cd078b  D[1]=af1becde
A[2]=f954880b  B[2]=7444e967  C[2]=385c5aa7  D[2]=2f10cbac
A[3]=d75ccdf7  B[3]=e788175b  C[3]=3c3219f5  D[3]=a68f6519

Step 19: (r=22, s=19)
A[0]=52c972c1  B[0]=a8e10cdc  C[0]=769b4f7b  D[0]=ad900f24
A[1]=d71ec217  B[1]=02a0e4fb  C[1]=1150b040  D[1]=00cd078b
A[2]=bc57643b  B[2]=02fe5522  C[2]=7444e967  D[2]=385c5aa7
A[3]=e285c391  B[3]=7df5d733  C[3]=e788175b  D[3]=3c3219f5

Step 20: (r=19, s=28)
A[0]=79bc5e58  B[0]=960a964b  C[0]=a8e10cdc  D[0]=769b4f7b
A[1]=037d5751  B[1]=10beb8f6  C[1]=02a0e4fb  D[1]=1150b040
A[2]=240f75f0  B[2]=21dde2bb  C[2]=02fe5522  D[2]=7444e967
A[3]=ad80169c  B[3]=1c8f142e  C[3]=7df5d733  D[3]=e788175b

Step 21: (r=28, s= 7)
A[0]=53f316bf  B[0]=879bc5e5  C[0]=960a964b  D[0]=a8e10cdc
```

```
A[1]=ead85679  B[1]=1037d575  C[1]=10beb8f6  D[1]=02a0e4fb
A[2]=1cbb3503  B[2]=0240f75f  C[2]=21dde2bb  D[2]=02fe5522
A[3]=ad506039  B[3]=cad80169  C[3]=1c8f142e  D[3]=7df5d733

Step 22: (r= 7, s=22)
A[0]=372b768f  B[0]=f98b5fa9  C[0]=879bc5e5  D[0]=960a964b
A[1]=769a8f23  B[1]=6c2b3cf5  C[1]=1037d575  D[1]=10beb8f6
A[2]=9f76153d  B[2]=5d9a818e  C[2]=0240f75f  D[2]=21dde2bb
A[3]=c7c40eca  B[3]=a8301cd6  C[3]=cad80169  D[3]=1c8f142e

Step 23: (r=22, s=19)
A[0]=ead45bd5  B[0]=a3cdcadd  C[0]=f98b5fa9  D[0]=879bc5e5
A[1]=f347c8e7  B[1]=c8dda6a3  C[1]=6c2b3cf5  D[1]=1037d575
A[2]=cd01a74a  B[2]=4f67dd85  C[2]=5d9a818e  D[2]=0240f75f
A[3]=7e747220  B[3]=b2b1f103  C[3]=a8301cd6  D[3]=cad80169

Step 24: (r=15, s= 5)
A[0]=7ed65e37  B[0]=2deaf56a  C[0]=a3cdcadd  D[0]=f98b5fa9
A[1]=237be583  B[1]=e473f9a3  C[1]=c8dda6a3  D[1]=6c2b3cf5
A[2]=8cc278b0  B[2]=d3a56680  C[2]=4f67dd85  D[2]=5d9a818e
A[3]=3ba145e0  B[3]=39103f3a  C[3]=b2b1f103  D[3]=a8301cd6

Step 25: (r= 5, s=29)
A[0]=8e6ca865  B[0]=dacbc6ef  C[0]=2deaf56a  D[0]=a3cdcadd
A[1]=92637d7d  B[1]=6f7cb064  C[1]=e473f9a3  D[1]=c8dda6a3
A[2]=7f0fc0aa  B[2]=984f1611  C[2]=d3a56680  D[2]=4f67dd85
A[3]=2fc6877a  B[3]=7428bc07  C[3]=39103f3a  D[3]=b2b1f103

Step 26: (r=29, s= 9)
A[0]=73500f9a  B[0]=b1cd950c  C[0]=dacbc6ef  D[0]=2deaf56a
A[1]=8505c4ce  B[1]=b24c6faf  C[1]=6f7cb064  D[1]=e473f9a3
A[2]=65e07fee  B[2]=4fe1f815  C[2]=984f1611  D[2]=d3a56680
A[3]=988ad485  B[3]=45f8d0ef  C[3]=7428bc07  D[3]=39103f3a

Step 27: (r= 9, s=15)
A[0]=f42c3ecb  B[0]=a01f34e6  C[0]=b1cd950c  D[0]=dacbc6ef
A[1]=bee1c47e  B[1]=0b899d0a  C[1]=b24c6faf  D[1]=6f7cb064
A[2]=b3211dce  B[2]=c0ffdccb  C[2]=4fe1f815  D[2]=984f1611
A[3]=f4e46251  B[3]=15a90b31  C[3]=45f8d0ef  D[3]=7428bc07

Step 28: (r=15, s= 5)
A[0]=3cc0ccec  B[0]=1f65fa16  C[0]=a01f34e6  D[0]=b1cd950c
A[1]=3c769c62  B[1]=e23f5f70  C[1]=0b899d0a  D[1]=b24c6faf
A[2]=568cac65  B[2]=8ee75990  C[2]=c0ffdccb  D[2]=4fe1f815
A[3]=89ef95f2  B[3]=3128fa72  C[3]=15a90b31  D[3]=45f8d0ef

Step 29: (r= 5, s=29)
A[0]=476537d4  B[0]=98199d87  C[0]=1f65fa16  D[0]=a01f34e6
A[1]=b6085468  B[1]=8ed38c47  C[1]=e23f5f70  D[1]=0b899d0a
```

```
A[2]=8f851489  B[2]=d1958caa  C[2]=8ee75990  D[2]=c0ffdccb
A[3]=a4041c8c  B[3]=3df2be51  C[3]=3128fa72  D[3]=15a90b31

Step 30: (r=29, s= 9)
A[0]=cddfebe5  B[0]=88eca6fa  C[0]=98199d87  D[0]=1f65fa16
A[1]=6e6ed838  B[1]=16c10a8d  C[1]=8ed38c47  D[1]=e23f5f70
A[2]=0cfb0e79  B[2]=31f0a291  C[2]=d1958caa  D[2]=8ee75990
A[3]=13be4760  B[3]=94808391  C[3]=3df2be51  D[3]=3128fa72

Step 31: (r= 9, s=15)
A[0]=2f3ba600  B[0]=bfd7cb9b  C[0]=88eca6fa  D[0]=98199d87
A[1]=bf162dc5  B[1]=ddb070dc  C[1]=16c10a8d  D[1]=8ed38c47
A[2]=0e1805d1  B[2]=f61cf219  C[2]=31f0a291  D[2]=d1958caa
A[3]=28273e89  B[3]=7c8ec027  C[3]=94808391  D[3]=3df2be51

Feed-Forward Step 0: (r=15, s= 5)
A[0]=f355b703  B[0]=d300179d  C[0]=bfd7cb9b  D[0]=88eca6fa
A[1]=c9e07b6e  B[1]=16e2df8b  C[1]=ddb070dc  D[1]=16c10a8d
A[2]=012c8261  B[2]=02e8870c  C[2]=f61cf219  D[2]=31f0a291
A[3]=47307357  B[3]=9f449413  C[3]=7c8ec027  D[3]=94808391

Feed-Forward Step 1: (r= 5, s=29)
A[0]=1851361e  B[0]=6ab6e07e  C[0]=d300179d  D[0]=bfd7cb9b
A[1]=d39560c2  B[1]=3c0f6dd9  C[1]=16e2df8b  D[1]=ddb070dc
A[2]=d84466a7  B[2]=25904c20  C[2]=02e8870c  D[2]=f61cf219
A[3]=b5e9a432  B[3]=e60e6ae8  C[3]=9f449413  D[3]=7c8ec027

Feed-Forward Step 2: (r=29, s= 9)
A[0]=8082762b  B[0]=c30a26c3  C[0]=6ab6e07e  D[0]=d300179d
A[1]=acea30c3  B[1]=5a72ac18  C[1]=3c0f6dd9  D[1]=16e2df8b
A[2]=f8608dc3  B[2]=fb088cd4  C[2]=25904c20  D[2]=02e8870c
A[3]=3d3c9e2f  B[3]=56bd3486  C[3]=e60e6ae8  D[3]=9f449413

Feed-Forward Step 3: (r= 9, s=15)
A[0]=ec6ac814  B[0]=04ec5701  C[0]=c30a26c3  D[0]=6ab6e07e
A[1]=9dd49167  B[1]=d4618759  C[1]=5a72ac18  D[1]=3c0f6dd9
A[2]=0ee617e9  B[2]=c11b87f0  C[2]=fb088cd4  D[2]=25904c20
A[3]=a0097e9f  B[3]=793c5e7a  C[3]=56bd3486  D[3]=e60e6ae8
```

Compression Function Output

```
A[0]=ec6ac814  B[0]=04ec5701  C[0]=c30a26c3  D[0]=6ab6e07e
A[1]=9dd49167  B[1]=d4618759  C[1]=5a72ac18  D[1]=3c0f6dd9
A[2]=0ee617e9  B[2]=c11b87f0  C[2]=fb088cd4  D[2]=25904c20
A[3]=a0097e9f  B[3]=793c5e7a  C[3]=56bd3486  D[3]=e60e6ae8
```

Hash Function Output

```
14 c8 6a ec 67 91 d4 9d e9 17 e6 0e 9f 7e 09 a0
01 57 ec 04 59 87 61 d4 f0 87 1b c1
```

6.2 SIMD-256

6.2.1 Empty message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  156  118  107   45  212  111  162
y[  8.. 15] =   97  249  211    3   49  101  151  223
y[ 16.. 23] =  189  178  253  204   76   82  232   65
y[ 24.. 31] =   96  176  161   47  189   61  248  107
y[ 32.. 39] =    0  131  133  113   17   33   12  111
y[ 40.. 47] =  251  103   57  148   47   65  249  143
y[ 48.. 55] =  189    8  204  230  205  151  187  227
y[ 56.. 63] =  247  111  140    6   77   10   21  149
y[ 64.. 71] =  255  101  139  150  212   45  146   95
y[ 72.. 79] =  160    8   46  254  208  156  106   34
y[ 80.. 87] =   68   79    4   53  181  175   25  192
y[ 88.. 95] =  161   81   96  210   68  196    9  150
y[ 96..103] =    0  126  124  144  240  224  245  146
y[104..111] =    6  154  200  109  210  192    8  114
y[112..119] =   68  249   53   27   52  106   70   30
y[120..127] =   10  146  117  251  180  247  236  108
```

Intermediate Expanded Message

```
Z[ 0] = b7030172  4d535546  df7b2085  bb595037
Z[ 1] = fa384619  022bdec2  48fd2369  e76eb366
Z[ 2] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
Z[ 3] = c5774560  21f7baa0  2c15cedc  4d53f97f
Z[ 4] = a4f20000  51a9a664  17d90c49  503708ac
Z[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
Z[ 6] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
Z[ 7] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
Z[ 8] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
Z[ 9] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
Z[10] = 39173124  264d02e4  c4bec914  d1071211
```

```
Z[11] = 3a89baa0  de094560  d3eb3124  b2ad0681
Z[12] = 5b0e0000  ae57599c  e827f3b7  afc9f754
Z[13] = b5910456  4ec5d6cf  d107de09  526205c8
Z[14] = fa383124  1383264d  4c9a2594  15ae3296
Z[15] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
Z[16] = fe4201be  993666ca  d8cd2733  9f4f60b1
Z[17] = ab81547f  2812d7ee  d5512aaf  5c56a3aa
Z[18] = 3b3cc4c4  037cfc84  bdcc4234  15c7ea39
Z[19] = ac6053a0  53a0ac60  3b3cc4c4  07d7f829
Z[20] = 00000000  6c0493fc  f1310ecf  f58c0a74
Z[21] = 053afac6  ce5931a7  d70f28f1  06f8f908
Z[22] = 3b3cc4c4  2e2bd1d5  2d4cd2b4  3cfac306
Z[23] = 08b6f74a  65eb9a15  bced4313  edb5124b
Z[24] = 57fba805  a2cb5d35  2733d8cd  52c1ad3f
Z[25] = 06f8f908  fd63029d  a80557fb  1d9ee262
Z[26] = 44d1bb2f  2e2bd1d5  b892476e  c761389f
Z[27] = 468fb971  d70f28f1  cadd3523  a2cb5d35
Z[28] = 6dc2923e  9d91626f  e3411cbf  9f4f60b1
Z[29] = a64759b9  5ef3a10d  c761389f  634e9cb2
Z[30] = f90806f8  1785e87b  5c56a3aa  1a22e5de
Z[31] = 9f4f60b1  fac6053a  f74a08b6  5e14a1ec
```

Expanded Message

```
W[ 0] = a4f20000  51a9a664  17d90c49  503708ac
W[ 1] = 05c8cedc  ec7dd9b3  b366da6c  ea52cd6a
W[ 2] = b7030172  4d535546  df7b2085  bb595037
W[ 3] = c6e9cedc  d9b3fd1c  3b4236ec  2ef9edef
W[ 4] = 5037f8c6  0456ab73  073a37a5  b1f40f2d
W[ 5] = 4a6ffbaa  b13b2931  2ef921f7  ad9efa38
W[ 6] = c5774560  21f7baa0  2c15cedc  4d53f97f
W[ 7] = fa384619  022bdec2  48fd2369  e76eb366
W[ 8] = afc9073a  fbaa548d  f8c6c85b  4e0cf0d3
W[ 9] = 3a89baa0  de094560  d3eb3124  b2ad0681
W[10] = 5b0e0000  ae57599c  e827f3b7  afc9f754
W[11] = 48fdfe8e  b2adaaba  2085df7b  44a7afc9
W[12] = 05c8b9e7  fdd5213e  b703dc97  18924c9a
W[13] = b5910456  4ec5d6cf  d107de09  526205c8
W[14] = 39173124  264d02e4  c4bec914  d1071211
W[15] = fa383124  1383264d  4c9a2594  15ae3296
W[16] = ab81547f  2812d7ee  d5512aaf  5c56a3aa
W[17] = 3b3cc4c4  037cfc84  bdcc4234  15c7ea39
W[18] = 08b6f74a  65eb9a15  bced4313  edb5124b
W[19] = 00000000  6c0493fc  f1310ecf  f58c0a74
W[20] = 3b3cc4c4  2e2bd1d5  2d4cd2b4  3cfac306
W[21] = 053afac6  ce5931a7  d70f28f1  06f8f908
W[22] = fe4201be  993666ca  d8cd2733  9f4f60b1
W[23] = ac6053a0  53a0ac60  3b3cc4c4  07d7f829
W[24] = f90806f8  1785e87b  5c56a3aa  1a22e5de
```

```
W[25] = 57fba805  a2cb5d35  2733d8cd  52c1ad3f
W[26] = 06f8f908  fd63029d  a80557fb  1d9ee262
W[27] = 9f4f60b1  fac6053a  f74a08b6  5e14a1ec
W[28] = 468fb971  d70f28f1  cadd3523  a2cb5d35
W[29] = a64759b9  5ef3a10d  c761389f  634e9cb2
W[30] = 6dc2923e  9d91626f  e3411cbf  9f4f60b1
W[31] = 44d1bb2f  2e2bd1d5  b892476e  c761389f
```

Feistel Steps

```
IV :
A[0]=99dae06a  B[0]=da4d98d0  C[0]=fd892a60  D[0]=fad01f14
A[1]=c3d43239  B[1]=cf5c52be  C[1]=8a471f8c  D[1]=9eeef3b3
A[2]=4979de73  B[2]=655cbaf9  C[2]=86ce033f  D[2]=68aec37a
A[3]=3ee5d052  B[3]=2a9d238e  C[3]=0ff768d3  D[3]=6b209d72

IV XOR M :
A[0]=99dae06a  B[0]=da4d98d0  C[0]=fd892a60  D[0]=fad01f14
A[1]=c3d43239  B[1]=cf5c52be  C[1]=8a471f8c  D[1]=9eeef3b3
A[2]=4979de73  B[2]=655cbaf9  C[2]=86ce033f  D[2]=68aec37a
A[3]=3ee5d052  B[3]=2a9d238e  C[3]=0ff768d3  D[3]=6b209d72

Step  0: (r= 3, s=20)
A[0]=b3eb5288  B[0]=ced70354  C[0]=da4d98d0  D[0]=fd892a60
A[1]=e90ab295  B[1]=1ea191ce  C[1]=cf5c52be  D[1]=8a471f8c
A[2]=ab3308f7  B[2]=4bcef39a  C[2]=655cbaf9  D[2]=86ce033f
A[3]=b8f57240  B[3]=f72e8291  C[3]=2a9d238e  D[3]=0ff768d3

Step  1: (r=20, s=14)
A[0]=f05de6b6  B[0]=288b3eb5  C[0]=ced70354  D[0]=da4d98d0
A[1]=9686f09d  B[1]=295e90ab  C[1]=1ea191ce  D[1]=cf5c52be
A[2]=0c9ca115  B[2]=8f7ab330  C[2]=4bcef39a  D[2]=655cbaf9
A[3]=b7d17bc8  B[3]=240b8f57  C[3]=f72e8291  D[3]=2a9d238e

Step  2: (r=14, s=27)
A[0]=722643b2  B[0]=79adbc17  C[0]=288b3eb5  D[0]=ced70354
A[1]=a16bfcf5  B[1]=bc2765a1  C[1]=295e90ab  D[1]=1ea191ce
A[2]=2393c46c  B[2]=28454327  C[2]=8f7ab330  D[2]=4bcef39a
A[3]=2bfeec0f  B[3]=5ef22df4  C[3]=240b8f57  D[3]=f72e8291

Step  3: (r=27, s= 3)
A[0]=d48d105b  B[0]=9391321d  C[0]=79adbc17  D[0]=288b3eb5
A[1]=7dc7940d  B[1]=ad0b5fe7  C[1]=bc2765a1  D[1]=295e90ab
A[2]=2f661fee  B[2]=611c9e23  C[2]=28454327  D[2]=8f7ab330
A[3]=55e85e88  B[3]=795ff760  C[3]=5ef22df4  D[3]=240b8f57

Step  4: (r= 3, s=20)
A[0]=67e14571  B[0]=a46882de  C[0]=9391321d  D[0]=79adbc17
A[1]=976fab3a  B[1]=ee3ca06b  C[1]=ad0b5fe7  D[1]=bc2765a1
```

```
A[2]=4f0ef3d2  B[2]=7b30ff71  C[2]=611c9e23  D[2]=28454327
A[3]=8aabc27f  B[3]=af42f442  C[3]=795ff760  D[3]=5ef22df4

Step  5: (r=20, s=14)
A[0]=ebac8bee  B[0]=57167e14  C[0]=a46882de  D[0]=9391321d
A[1]=b687f1e0  B[1]=b3a976fa  C[1]=ee3ca06b  D[1]=ad0b5fe7
A[2]=303aeeaa  B[2]=3d24f0ef  C[2]=7b30ff71  D[2]=611c9e23
A[3]=fb4d24f1  B[3]=27f8aabc  C[3]=af42f442  D[3]=795ff760

Step  6: (r=14, s=27)
A[0]=d679d5b3  B[0]=22fbbaeb  C[0]=57167e14  D[0]=a46882de
A[1]=47d81469  B[1]=fc782da1  C[1]=b3a976fa  D[1]=ee3ca06b
A[2]=9f6f9a32  B[2]=bbaa8c0e  C[2]=3d24f0ef  D[2]=7b30ff71
A[3]=9eab9f99  B[3]=493c7ed3  C[3]=27f8aabc  D[3]=af42f442

Step  7: (r=27, s= 3)
A[0]=3de1ba28  B[0]=9eb3cead  C[0]=22fbbaeb  D[0]=57167e14
A[1]=0ffafdb3  B[1]=4a3ec0a3  C[1]=fc782da1  D[1]=b3a976fa
A[2]=b999a6f1  B[2]=94fb7cd1  C[2]=bbaa8c0e  D[2]=3d24f0ef
A[3]=7d91f2b0  B[3]=ccf55cfc  C[3]=493c7ed3  D[3]=27f8aabc

Step  8: (r=26, s= 4)
A[0]=25f0ef88  B[0]=a0f786e8  C[0]=9eb3cead  D[0]=22fbbaeb
A[1]=5fcf2945  B[1]=cc3febf6  C[1]=4a3ec0a3  D[1]=fc782da1
A[2]=4c64aa66  B[2]=c6e6669b  C[2]=94fb7cd1  D[2]=bbaa8c0e
A[3]=cd270f14  B[3]=c1f647ca  C[3]=ccf55cfc  D[3]=493c7ed3

Step  9: (r= 4, s=23)
A[0]=e256e2e2  B[0]=5f0ef882  C[0]=a0f786e8  D[0]=9eb3cead
A[1]=460451fa  B[1]=fcf29455  C[1]=cc3febf6  D[1]=4a3ec0a3
A[2]=41c1431b  B[2]=c64aa664  C[2]=c6e6669b  D[2]=94fb7cd1
A[3]=9b518443  B[3]=d270f14c  C[3]=c1f647ca  D[3]=ccf55cfc

Step 10: (r=23, s=11)
A[0]=4abcbc0b  B[0]=71712b71  C[0]=5f0ef882  D[0]=a0f786e8
A[1]=1c457ec7  B[1]=fd230228  C[1]=fcf29455  D[1]=cc3febf6
A[2]=6e85eade  B[2]=8da0e0a1  C[2]=c64aa664  D[2]=c6e6669b
A[3]=2231edee  B[3]=21cda8c2  C[3]=d270f14c  D[3]=c1f647ca

Step 11: (r=11, s=26)
A[0]=0c53932b  B[0]=e5e05a55  C[0]=71712b71  D[0]=5f0ef882
A[1]=915df574  B[1]=2bf638e2  C[1]=fd230228  D[1]=fcf29455
A[2]=bfb136ff  B[2]=2f56f374  C[2]=8da0e0a1  D[2]=c64aa664
A[3]=83d1b7a3  B[3]=8f6f7111  C[3]=21cda8c2  D[3]=d270f14c

Step 12: (r=26, s= 4)
A[0]=76d25581  B[0]=ac314e4c  C[0]=e5e05a55  D[0]=71712b71
A[1]=42ed2416  B[1]=d24577d5  C[1]=2bf638e2  D[1]=fd230228
A[2]=5e06a5e0  B[2]=fefec4db  C[2]=2f56f374  D[2]=8da0e0a1
```

```
A[3]=994044e2  B[3]=8e0f46de  C[3]=8f6f7111  D[3]=21cda8c2

Step 13: (r= 4, s=23)
A[0]=e670574c  B[0]=6d255817  C[0]=ac314e4c  D[0]=e5e05a55
A[1]=7acbb52f  B[1]=2ed24164  C[1]=d24577d5  D[1]=2bf638e2
A[2]=ba93d7e9  B[2]=e06a5e05  C[2]=fefec4db  D[2]=2f56f374
A[3]=dcd400dd  B[3]=94044e29  C[3]=8e0f46de  D[3]=8f6f7111

Step 14: (r=23, s=11)
A[0]=df0b8e33  B[0]=a673382b  C[0]=6d255817  D[0]=ac314e4c
A[1]=2a66a853  B[1]=97bd65da  C[1]=2ed24164  D[1]=d24577d5
A[2]=f388f978  B[2]=f4dd49eb  C[2]=e06a5e05  D[2]=fefec4db
A[3]=7cc3380e  B[3]=6eee6a00  C[3]=94044e29  D[3]=8e0f46de

Step 15: (r=11, s=26)
A[0]=d621f9fa  B[0]=5c719ef8  C[0]=a673382b  D[0]=6d255817
A[1]=ea136fe3  B[1]=35429953  C[1]=97bd65da  D[1]=2ed24164
A[2]=bd632407  B[2]=47cbc79c  C[2]=f4dd49eb  D[2]=e06a5e05
A[3]=25c4a8e0  B[3]=19c073e6  C[3]=6eee6a00  D[3]=94044e29

Step 16: (r=19, s=28)
A[0]=77f0f4f3  B[0]=cfd6b10f  C[0]=5c719ef8  D[0]=a673382b
A[1]=f9071d43  B[1]=7f1f509b  C[1]=35429953  D[1]=97bd65da
A[2]=56badb8f  B[2]=203deb19  C[2]=47cbc79c  D[2]=f4dd49eb
A[3]=039b065a  B[3]=47012e25  C[3]=19c073e6  D[3]=6eee6a00

Step 17: (r=28, s= 7)
A[0]=b6472ad0  B[0]=377f0f4f  C[0]=cfd6b10f  D[0]=5c719ef8
A[1]=e132e8f1  B[1]=3f9071d4  C[1]=7f1f509b  D[1]=35429953
A[2]=492caba9  B[2]=f56badb8  C[2]=203deb19  D[2]=47cbc79c
A[3]=3b7660a3  B[3]=a039b065  C[3]=47012e25  D[3]=19c073e6

Step 18: (r= 7, s=22)
A[0]=fdedb8fc  B[0]=2395685b  C[0]=377f0f4f  D[0]=cfd6b10f
A[1]=a70c678d  B[1]=997478f0  C[1]=3f9071d4  D[1]=7f1f509b
A[2]=d509ce5a  B[2]=9655d4a4  C[2]=f56badb8  D[2]=203deb19
A[3]=39305208  B[3]=bb30519d  C[3]=a039b065  D[3]=47012e25

Step 19: (r=22, s=19)
A[0]=9a0cdde2  B[0]=3f3f7b6e  C[0]=2395685b  D[0]=377f0f4f
A[1]=2d4a71d6  B[1]=e369c319  C[1]=997478f0  D[1]=3f9071d4
A[2]=3b85aa04  B[2]=96b54273  C[2]=9655d4a4  D[2]=f56badb8
A[3]=2ba17152  B[3]=820e4c14  C[3]=bb30519d  D[3]=a039b065

Step 20: (r=19, s=28)
A[0]=698eff2a  B[0]=ef14d066  C[0]=3f3f7b6e  D[0]=2395685b
A[1]=e1942784  B[1]=8eb16a53  C[1]=e369c319  D[1]=997478f0
A[2]=96264134  B[2]=5021dc2d  C[2]=96b54273  D[2]=9655d4a4
A[3]=e79a1cad  B[3]=8a915d0b  C[3]=820e4c14  D[3]=bb30519d
```

```
Step 21: (r=28, s= 7)
A[0]=4111abde  B[0]=a698eff2  C[0]=ef14d066  D[0]=3f3f7b6e
A[1]=9e0075ef  B[1]=4e194278  C[1]=8eb16a53  D[1]=e369c319
A[2]=6bb7d4f3  B[2]=49626413  C[2]=5021dc2d  D[2]=96b54273
A[3]=afec9b9a  B[3]=de79a1ca  C[3]=8a915d0b  D[3]=820e4c14

Step 22: (r= 7, s=22)
A[0]=48c41c69  B[0]=88d5ef20  C[0]=a698eff2  D[0]=ef14d066
A[1]=f36d2618  B[1]=003af7cf  C[1]=4e194278  D[1]=8eb16a53
A[2]=6cbbf6e6  B[2]=dbea79b5  C[2]=49626413  D[2]=5021dc2d
A[3]=1cc204f1  B[3]=f64dcd57  C[3]=de79a1ca  D[3]=8a915d0b

Step 23: (r=22, s=19)
A[0]=54cc514d  B[0]=1a523107  C[0]=88d5ef20  D[0]=a698eff2
A[1]=24a054dc  B[1]=863cdb49  C[1]=003af7cf  D[1]=4e194278
A[2]=c798db4f  B[2]=b99b2efd  C[2]=dbea79b5  D[2]=49626413
A[3]=5e7860df  B[3]=3c473081  C[3]=f64dcd57  D[3]=de79a1ca

Step 24: (r=15, s= 5)
A[0]=28c4d436  B[0]=28a6aa66  C[0]=1a523107  D[0]=88d5ef20
A[1]=a8ebab99  B[1]=2a6e1250  C[1]=863cdb49  D[1]=003af7cf
A[2]=26d60683  B[2]=6da7e3cc  C[2]=b99b2efd  D[2]=dbea79b5
A[3]=c4ed4f9c  B[3]=306faf3c  C[3]=3c473081  D[3]=f64dcd57

Step 25: (r= 5, s=29)
A[0]=5e2dd76d  B[0]=189a86c5  C[0]=28a6aa66  D[0]=1a523107
A[1]=37da8882  B[1]=1d757335  C[1]=2a6e1250  D[1]=863cdb49
A[2]=f0b03674  B[2]=dac0d064  C[2]=6da7e3cc  D[2]=b99b2efd
A[3]=8da54a6b  B[3]=9da9f398  C[3]=306faf3c  D[3]=3c473081

Step 26: (r=29, s= 9)
A[0]=f2abfdc3  B[0]=abc5baed  C[0]=189a86c5  D[0]=28a6aa66
A[1]=c5f67410  B[1]=46fb5110  C[1]=1d757335  D[1]=2a6e1250
A[2]=c26671cb  B[2]=9e1606ce  C[2]=dac0d064  D[2]=6da7e3cc
A[3]=4fb9b91c  B[3]=71b4a94d  C[3]=9da9f398  D[3]=306faf3c

Step 27: (r= 9, s=15)
A[0]=afd1d0c7  B[0]=57fb87e5  C[0]=abc5baed  D[0]=189a86c5
A[1]=28d1f9b2  B[1]=ece8218b  C[1]=46fb5110  D[1]=1d757335
A[2]=8eb407a1  B[2]=cce39784  C[2]=9e1606ce  D[2]=dac0d064
A[3]=8b4251a5  B[3]=7372389f  C[3]=71b4a94d  D[3]=9da9f398

Step 28: (r=15, s= 5)
A[0]=dc5377c9  B[0]=e863d7e8  C[0]=57fb87e5  D[0]=abc5baed
A[1]=33927e66  B[1]=fcd91468  C[1]=ece8218b  D[1]=46fb5110
A[2]=b3546707  B[2]=03d0c75a  C[2]=cce39784  D[2]=9e1606ce
A[3]=6555233e  B[3]=28d2c5a1  C[3]=7372389f  D[3]=71b4a94d
```

```
Step 29: (r= 5, s=29)
A[0]=505cfe87  B[0]=8a6ef93b  C[0]=e863d7e8  D[0]=57fb87e5
A[1]=9efd4c9c  B[1]=724fccc6  C[1]=fcd91468  D[1]=ece8218b
A[2]=0797fa09  B[2]=6a8ce0f6  C[2]=03d0c75a  D[2]=cce39784
A[3]=391a79bd  B[3]=aaa467cc  C[3]=28d2c5a1  D[3]=7372389f

Step 30: (r=29, s= 9)
A[0]=ee1346af  B[0]=ea0b9fd0  C[0]=8a6ef93b  D[0]=e863d7e8
A[1]=ce948c53  B[1]=93dfa993  C[1]=724fccc6  D[1]=fcd91468
A[2]=1a508a9e  B[2]=20f2ff41  C[2]=6a8ce0f6  D[2]=03d0c75a
A[3]=92099a46  B[3]=a7234f37  C[3]=aaa467cc  D[3]=28d2c5a1

Step 31: (r= 9, s=15)
A[0]=5a7e47d4  B[0]=268d5fdc  C[0]=ea0b9fd0  D[0]=8a6ef93b
A[1]=4cbd0c16  B[1]=2918a79d  C[1]=93dfa993  D[1]=724fccc6
A[2]=235cd375  B[2]=a1153c34  C[2]=20f2ff41  D[2]=6a8ce0f6
A[3]=cfdbf0c7  B[3]=13348d24  C[3]=a7234f37  D[3]=aaa467cc

Feed-Forward Step 0: (r=15, s= 5)
A[0]=51025596  B[0]=23ea2d3f  C[0]=268d5fdc  D[0]=ea0b9fd0
A[1]=998f2448  B[1]=860b265e  C[1]=2918a79d  D[1]=93dfa993
A[2]=b0035ba7  B[2]=69ba91ae  C[2]=a1153c34  D[2]=20f2ff41
A[3]=bb431780  B[3]=f863e7ed  C[3]=13348d24  D[3]=a7234f37

Feed-Forward Step 1: (r= 5, s=29)
A[0]=dde87df5  B[0]=204ab2ca  C[0]=23ea2d3f  D[0]=268d5fdc
A[1]=28cde49c  B[1]=31e48913  C[1]=860b265e  D[1]=2918a79d
A[2]=353770c8  B[2]=006b74f6  C[2]=69ba91ae  D[2]=a1153c34
A[3]=632b8960  B[3]=6862f017  C[3]=f863e7ed  D[3]=13348d24

Feed-Forward Step 2: (r=29, s= 9)
A[0]=468fc91f  B[0]=bbbd0fbe  C[0]=204ab2ca  D[0]=23ea2d3f
A[1]=5339e4cd  B[1]=8519bc93  C[1]=31e48913  D[1]=860b265e
A[2]=2ac8240d  B[2]=06a6ee19  C[2]=006b74f6  D[2]=69ba91ae
A[3]=d97617f5  B[3]=0c65712c  C[3]=6862f017  D[3]=f863e7ed

Feed-Forward Step 3: (r= 9, s=15)
A[0]=5460bb18  B[0]=1f923e8d  C[0]=bbbd0fbe  D[0]=204ab2ca
A[1]=d0020f1d  B[1]=73c99aa6  C[1]=8519bc93  D[1]=31e48913
A[2]=84a42913  B[2]=90481a55  C[2]=06a6ee19  D[2]=006b74f6
A[3]=2f0c609a  B[3]=ec2febb2  C[3]=0c65712c  D[3]=6862f017
```

Compression Function Output

```
A[0]=5460bb18  B[0]=1f923e8d  C[0]=bbbd0fbe  D[0]=204ab2ca
A[1]=d0020f1d  B[1]=73c99aa6  C[1]=8519bc93  D[1]=31e48913
A[2]=84a42913  B[2]=90481a55  C[2]=06a6ee19  D[2]=006b74f6
A[3]=2f0c609a  B[3]=ec2febb2  C[3]=0c65712c  D[3]=6862f017
```

Hash Function Output

```
18 bb 60 54 1d 0f 02 d0 13 29 a4 84 9a 60 0c 2f
8d 3e 92 1f a6 9a c9 73 55 1a 48 90 b2 eb 2f ec
```

6.2.2 One block message

We use the message block 0x00 0x01 0x02 ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
```

NTT Output

```
y[  0..  7] =  218   26   85  204   79  131  143   82
y[  8.. 15] =  193  132  188  176  130  214  229  177
y[ 16.. 23] =   43    9  233   73  161  207  236  155
y[ 24.. 31] =  124   92  110  120  191  202  211   82
y[ 32.. 39] =  211  215  163   35    7   33  156  212
y[ 40.. 47] =  135  222  249   69  206   55  208  212
y[ 48.. 55] =   99   87  170   98  133  188   63  177
y[ 56.. 63] =   41   50  150   31   54  204   39  220
y[ 64.. 71] =  224    7   13   81   49  160   87  256
y[ 72.. 79] =   21  231  119  191  182  247   17  196
y[ 80.. 87] =  154   34  227   51  125  130  142  149
y[ 88.. 95] =   82   92  139  202  152   85   17  226
y[ 96..103] =  239   47  252  198   36    9  238  244
y[104..111] =   45  236   16   63  151  237  232    9
y[112..119] =   90   90  227  241  198  200   16  123
y[120..127] =  131    1    6  179  204  175  249  158
```

Intermediate Expanded Message

```
Z[ 0] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
Z[ 1] = a5abd1c0  c577ce23  e0eda439  c630ebc4
Z[ 2] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
Z[ 3] = 427c599c  56b84f7e  d841d04e  3b42dec2
Z[ 4] = e1a6dec2  194bbc12  17d9050f  df7bb703
Z[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
Z[ 6] = 3edf478b  46d2c121  ce23a664  c6302d87
Z[ 7] = 24221da1  1667b2ad  d9b32706  e5431c2f
Z[ 8] = 050fe827  3a890965  b9e72369  ff473edf
```

```
Z[ 9] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
Z[10] = 1892b591  24dbea52  a4395a55  b1f4ace5
Z[11] = 427c3b42  d841aaba  3d6db41f  e9990c49
Z[12] = 21f7f2fe  d55dfc63  06811a04  f69bf245
Z[13] = f0d32085  2d870b90  f18cb366  0681edef
Z[14] = 410a410a  f470ea52  d6cfd55d  58e30b90
Z[15] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
Z[16] = e341de07  0b534a0b  2aaf44d1  4bc99cb2
Z[17] = 124bc840  67a9c3e5  beab915f  0ecfe79c
Z[18] = a6472575  e5deeb18  6ce3ac60  9bd3edb5
Z[19] = 476e6c04  99365fd2  a489c682  0ecfd7ee
Z[20] = f052d7ee  fba5ae1e  1f5c0619  ef73a805
Z[21] = 273395ba  0df0f908  a3aad393  ea39d551
Z[22] = 4e66563d  e5deb437  cc9b93fc  0df036e1
Z[23] = 923e23b7  053aa2cb  d1d52f0a  f90821f9
Z[24] = 061916a6  468fd1d5  ab81923e  ff21476e
Z[25] = e95a931d  c682b971  f74ada8b  caddba50
Z[26] = 1d9e07d7  2c6d3f97  915fd472  a1eca726
Z[27] = 50245024  d0176888  4a0bd017  e4ff476e
Z[28] = 28f1db6a  cc9b1e7d  07d71cbf  f4add8cd
Z[29] = edb5e183  36e13c1b  ee942fe9  07d7d8cd
Z[30] = 4e664bc9  f210555e  ce59c3e5  6b25ba50
Z[31] = 00df2b8e  bc0e1b01  b892d1d5  a9c3dfc5
```

Expanded Message

```
W[ 0] = e1a6dec2  194bbc12  17d9050f  df7bb703
W[ 1] = 3edf478b  46d2c121  ce23a664  c6302d87
W[ 2] = 12cae3d1  d9b33d6d  a4f23917  3b42ad9e
W[ 3] = 06811f13  34c1eea8  dbdebaa0  b64af0d3
W[ 4] = 24221da1  1667b2ad  d9b32706  e5431c2f
W[ 5] = e6b5a7d6  31ddfa38  27bfdb25  df7bdc97
W[ 6] = 427c599c  56b84f7e  d841d04e  3b42dec2
W[ 7] = a5abd1c0  c577ce23  e0eda439  c630ebc4
W[ 8] = 00b9a4f2  c7a20456  c4bed9b3  b875fa38
W[ 9] = 427c3b42  d841aaba  3d6db41f  e9990c49
W[10] = 21f7f2fe  d55dfc63  06811a04  f69bf245
W[11] = 050fe827  3a890965  b9e72369  ff473edf
W[12] = ed360f2d  d04e55ff  f8c6c9cd  d3eb0c49
W[13] = f0d32085  2d870b90  f18cb366  0681edef
W[14] = 1892b591  24dbea52  a4395a55  b1f4ace5
W[15] = 410a410a  f470ea52  d6cfd55d  58e30b90
W[16] = 124bc840  67a9c3e5  beab915f  0ecfe79c
W[17] = a6472575  e5deeb18  6ce3ac60  9bd3edb5
W[18] = 923e23b7  053aa2cb  d1d52f0a  f90821f9
W[19] = f052d7ee  fba5ae1e  1f5c0619  ef73a805
W[20] = 4e66563d  e5deb437  cc9b93fc  0df036e1
W[21] = 273395ba  0df0f908  a3aad393  ea39d551
W[22] = e341de07  0b534a0b  2aaf44d1  4bc99cb2
```

```
W[23] = 476e6c04  99365fd2  a489c682  0ecfd7ee
W[24] = 4e664bc9  f210555e  ce59c3e5  6b25ba50
W[25] = 061916a6  468fd1d5  ab81923e  ff21476e
W[26] = e95a931d  c682b971  f74ada8b  caddba50
W[27] = 00df2b8e  bc0e1b01  b892d1d5  a9c3dfc5
W[28] = 50245024  d0176888  4a0bd017  e4ff476e
W[29] = edb5e183  36e13c1b  ee942fe9  07d7d8cd
W[30] = 28f1db6a  cc9b1e7d  07d71cbf  f4add8cd
W[31] = 1d9e07d7  2c6d3f97  915fd472  a1eca726
```

Feistel Steps

```
IV :
A[0]=99dae06a  B[0]=da4d98d0  C[0]=fd892a60  D[0]=fad01f14
A[1]=c3d43239  B[1]=cf5c52be  C[1]=8a471f8c  D[1]=9eeef3b3
A[2]=4979de73  B[2]=655cbaf9  C[2]=86ce033f  D[2]=68aec37a
A[3]=3ee5d052  B[3]=2a9d238e  C[3]=0ff768d3  D[3]=6b209d72

IV XOR M :
A[0]=9ad8e16a  B[0]=c95f89c0  C[0]=deab0b40  D[0]=c9e22e24
A[1]=c4d2373d  B[1]=d84a47aa  C[1]=ad613aa8  D[1]=a9d8c687
A[2]=4273d77b  B[2]=7e46a3e1  C[2]=ade42a17  D[2]=5394fa42
A[3]=31ebdd5e  B[3]=35833e92  C[3]=20d945ff  D[3]=541ea04e

Step  0: (r= 3, s=20)
A[0]=a8f93a37  B[0]=d6c70b54  C[0]=c95f89c0  D[0]=deab0b40
A[1]=37b98453  B[1]=2691b9ee  C[1]=d84a47aa  D[1]=ad613aa8
A[2]=3ac49e3b  B[2]=139ebbda  C[2]=7e46a3e1  D[2]=ade42a17
A[3]=170d5e2b  B[3]=8f5eeaf1  C[3]=35833e92  D[3]=20d945ff

Step  1: (r=20, s=14)
A[0]=5b5ba41d  B[0]=a37a8f93  C[0]=d6c70b54  D[0]=c95f89c0
A[1]=d29e6996  B[1]=45337b98  C[1]=2691b9ee  D[1]=d84a47aa
A[2]=46900436  B[2]=e3b3ac49  C[2]=139ebbda  D[2]=7e46a3e1
A[3]=3cc13f3d  B[3]=e2b170d5  C[3]=8f5eeaf1  D[3]=35833e92

Step  2: (r=14, s=27)
A[0]=ad85fc8e  B[0]=e90756d6  C[0]=a37a8f93  D[0]=d6c70b54
A[1]=79be1d9c  B[1]=9a65b4a7  C[1]=45337b98  D[1]=2691b9ee
A[2]=53860c16  B[2]=010d91a4  C[2]=e3b3ac49  D[2]=139ebbda
A[3]=11aa85be  B[3]=4fcf4f30  C[3]=e2b170d5  D[3]=8f5eeaf1

Step  3: (r=27, s= 3)
A[0]=f8d84054  B[0]=756c2fe4  C[0]=e90756d6  D[0]=a37a8f93
A[1]=ac564d00  B[1]=e3cdf0ec  C[1]=9a65b4a7  D[1]=45337b98
A[2]=fb04e620  B[2]=b29c3060  C[2]=010d91a4  D[2]=e3b3ac49
A[3]=2df87a95  B[3]=f08d542d  C[3]=4fcf4f30  D[3]=e2b170d5

Step  4: (r= 3, s=20)
```

```
A[0]=a33e7694  B[0]=c6c202a7  C[0]=756c2fe4  D[0]=e90756d6
A[1]=06b78f19  B[1]=62b26805  C[1]=e3cdf0ec  D[1]=9a65b4a7
A[2]=a6badbe1  B[2]=d8273107  C[2]=b29c3060  D[2]=010d91a4
A[3]=7a555ec5  B[3]=6fc3d4a9  C[3]=f08d542d  D[3]=4fcf4f30

Step  5: (r=20, s=14)
A[0]=876e9977  B[0]=694a33e7  C[0]=c6c202a7  D[0]=756c2fe4
A[1]=d212b113  B[1]=f1906b78  C[1]=62b26805  D[1]=e3cdf0ec
A[2]=50d4eac9  B[2]=be1a6bad  C[2]=d8273107  D[2]=b29c3060
A[3]=11ad95fc  B[3]=ec57a555  C[3]=6fc3d4a9  D[3]=f08d542d

Step  6: (r=14, s=27)
A[0]=e83e896f  B[0]=a65de1db  C[0]=694a33e7  D[0]=c6c202a7
A[1]=141b1980  B[1]=ac44f484  C[1]=f1906b78  D[1]=62b26805
A[2]=4096a7cc  B[2]=3ab25435  C[2]=be1a6bad  D[2]=d8273107
A[3]=0b2aa022  B[3]=657f046b  C[3]=ec57a555  D[3]=6fc3d4a9

Step  7: (r=27, s= 3)
A[0]=086867f0  B[0]=7f41f44b  C[0]=a65de1db  D[0]=694a33e7
A[1]=f22ed247  B[1]=00a0d8cc  C[1]=ac44f484  D[1]=f1906b78
A[2]=1c7bdbba  B[2]=6204b53e  C[2]=3ab25435  D[2]=be1a6bad
A[3]=1c43ff51  B[3]=10595501  C[3]=657f046b  D[3]=ec57a555

Step  8: (r=26, s= 4)
A[0]=a5648d8a  B[0]=c021a19f  C[0]=7f41f44b  D[0]=a65de1db
A[1]=41a8389a  B[1]=1fc8bb49  C[1]=00a0d8cc  D[1]=ac44f484
A[2]=9a0eb9f7  B[2]=e871ef6e  C[2]=6204b53e  D[2]=3ab25435
A[3]=24d0ed20  B[3]=44710ffd  C[3]=10595501  D[3]=657f046b

Step  9: (r= 4, s=23)
A[0]=154d1d80  B[0]=5648d8aa  C[0]=c021a19f  D[0]=7f41f44b
A[1]=1251d9cd  B[1]=1a8389a4  C[1]=1fc8bb49  D[1]=00a0d8cc
A[2]=3778e904  B[2]=a0eb9f79  C[2]=e871ef6e  D[2]=6204b53e
A[3]=0535423a  B[3]=4d0ed202  C[3]=44710ffd  D[3]=10595501

Step 10: (r=23, s=11)
A[0]=fb886c99  B[0]=c00aa68e  C[0]=5648d8aa  D[0]=c021a19f
A[1]=c6215c20  B[1]=e68928ec  C[1]=1a8389a4  D[1]=1fc8bb49
A[2]=97f7fd28  B[2]=821bbc74  C[2]=a0eb9f79  D[2]=e871ef6e
A[3]=8cc310ef  B[3]=1d029aa1  C[3]=4d0ed202  D[3]=44710ffd

Step 11: (r=11, s=26)
A[0]=820f2db8  B[0]=4364cfdc  C[0]=c00aa68e  D[0]=5648d8aa
A[1]=616ad19f  B[1]=0ae10631  C[1]=e68928ec  D[1]=1a8389a4
A[2]=6476a321  B[2]=bfe944bf  C[2]=821bbc74  D[2]=a0eb9f79
A[3]=012422b6  B[3]=18877c66  C[3]=1d029aa1  D[3]=4d0ed202

Step 12: (r=26, s= 4)
A[0]=d65f2276  B[0]=e2083cb6  C[0]=4364cfdc  D[0]=c00aa68e
```

```
A[1]=613fe090  B[1]=7d85ab46  C[1]=0ae10631  D[1]=e68928ec
A[2]=dae5683e  B[2]=8591da8c  C[2]=bfe944bf  D[2]=821bbc74
A[3]=8209cbc9  B[3]=d804908a  C[3]=18877c66  D[3]=1d029aa1

Step 13: (r= 4, s=23)
A[0]=b31018e8  B[0]=65f2276d  C[0]=e2083cb6  D[0]=4364cfdc
A[1]=66db9783  B[1]=13fe0906  C[1]=7d85ab46  D[1]=0ae10631
A[2]=b1fbec49  B[2]=ae5683ed  C[2]=8591da8c  D[2]=bfe944bf
A[3]=c15bce36  B[3]=209cbc98  C[3]=d804908a  D[3]=18877c66

Step 14: (r=23, s=11)
A[0]=ffc637c3  B[0]=7459880c  C[0]=65f2276d  D[0]=e2083cb6
A[1]=08b54b32  B[1]=c1b36dcb  C[1]=13fe0906  D[1]=7d85ab46
A[2]=ceafb636  B[2]=24d8fdf6  C[2]=ae5683ed  D[2]=8591da8c
A[3]=3a88b460  B[3]=1b60ade7  C[3]=209cbc98  D[3]=d804908a

Step 15: (r=11, s=26)
A[0]=b4154909  B[0]=31be1ffe  C[0]=7459880c  D[0]=65f2276d
A[1]=af71b94e  B[1]=aa599045  C[1]=c1b36dcb  D[1]=13fe0906
A[2]=adeb219d  B[2]=7db1b675  C[2]=24d8fdf6  D[2]=ae5683ed
A[3]=940751a8  B[3]=45a301d4  C[3]=1b60ade7  D[3]=209cbc98

Step 16: (r=19, s=28)
A[0]=68ff2318  B[0]=484da0aa  C[0]=31be1ffe  D[0]=7459880c
A[1]=13552974  B[1]=ca757b8d  C[1]=aa599045  D[1]=c1b36dcb
A[2]=c6efe156  B[2]=0ced6f59  C[2]=7db1b675  D[2]=24d8fdf6
A[3]=fc3aa5c9  B[3]=8d44a03a  C[3]=45a301d4  D[3]=1b60ade7

Step 17: (r=28, s= 7)
A[0]=636435ce  B[0]=868ff231  C[0]=484da0aa  D[0]=31be1ffe
A[1]=97cc9e84  B[1]=41355297  C[1]=ca757b8d  D[1]=aa599045
A[2]=63a0d618  B[2]=6c6efe15  C[2]=0ced6f59  D[2]=7db1b675
A[3]=9c532eb9  B[3]=9fc3aa5c  C[3]=8d44a03a  D[3]=45a301d4

Step 18: (r= 7, s=22)
A[0]=dbc2c4c7  B[0]=b21ae731  C[0]=868ff231  D[0]=484da0aa
A[1]=77e93e9a  B[1]=e64f424b  C[1]=41355297  D[1]=ca757b8d
A[2]=5dc65a07  B[2]=d06b0c31  C[2]=6c6efe15  D[2]=0ced6f59
A[3]=2c11e3e4  B[3]=29975cce  C[3]=9fc3aa5c  D[3]=8d44a03a

Step 19: (r=22, s=19)
A[0]=f825e719  B[0]=31f6f0b1  C[0]=b21ae731  D[0]=868ff231
A[1]=56dc683b  B[1]=a69dfa4f  C[1]=e64f424b  D[1]=41355297
A[2]=3e13d652  B[2]=81d77196  C[2]=d06b0c31  D[2]=6c6efe15
A[3]=2f77beab  B[3]=f90b0478  C[3]=29975cce  D[3]=9fc3aa5c

Step 20: (r=19, s=28)
A[0]=3a2d89dc  B[0]=38cfc12f  C[0]=31f6f0b1  D[0]=b21ae731
A[1]=437107af  B[1]=41dab6e3  C[1]=a69dfa4f  D[1]=e64f424b
```

```
A[2]=31ef5a1f  B[2]=b291f09e  C[2]=81d77196  D[2]=d06b0c31
A[3]=b63c7111  B[3]=f5597bbd  C[3]=f90b0478  D[3]=29975cce

Step 21: (r=28, s= 7)
A[0]=123e49aa  B[0]=c3a2d89d  C[0]=38cfc12f  D[0]=31f6f0b1
A[1]=285ce82d  B[1]=f437107a  C[1]=41dab6e3  D[1]=a69dfa4f
A[2]=ba4b09af  B[2]=f31ef5a1  C[2]=b291f09e  D[2]=81d77196
A[3]=6988bc7e  B[3]=1b63c711  C[3]=f5597bbd  D[3]=f90b0478

Step 22: (r= 7, s=22)
A[0]=483e107a  B[0]=1f24d509  C[0]=c3a2d89d  D[0]=38cfc12f
A[1]=56c96bda  B[1]=2e741694  C[1]=f437107a  D[1]=41dab6e3
A[2]=c9f5e7de  B[2]=2584d7dd  C[2]=f31ef5a1  D[2]=b291f09e
A[3]=39145cb1  B[3]=c45e3f34  C[3]=1b63c711  D[3]=f5597bbd

Step 23: (r=22, s=19)
A[0]=e218d8a0  B[0]=1e920f84  C[0]=1f24d509  D[0]=c3a2d89d
A[1]=78c8d148  B[1]=f695b25a  C[1]=2e741694  D[1]=f437107a
A[2]=967bd509  B[2]=f7b27d79  C[2]=2584d7dd  D[2]=f31ef5a1
A[3]=8d769e57  B[3]=2c4e4517  C[3]=c45e3f34  D[3]=1b63c711

Step 24: (r=15, s= 5)
A[0]=904a7a4a  B[0]=6c50710c  C[0]=1e920f84  D[0]=1f24d509
A[1]=8a0461c8  B[1]=68a43c64  C[1]=f695b25a  D[1]=2e741694
A[2]=750df32a  B[2]=ea84cb3d  C[2]=f7b27d79  D[2]=2584d7dd
A[3]=c7454426  B[3]=4f2bc6bb  C[3]=2c4e4517  D[3]=c45e3f34

Step 25: (r= 5, s=29)
A[0]=08403175  B[0]=094f4952  C[0]=6c50710c  D[0]=1e920f84
A[1]=66dbb82f  B[1]=408c3911  C[1]=68a43c64  D[1]=f695b25a
A[2]=9fc6f084  B[2]=a1be654e  C[2]=ea84cb3d  D[2]=f7b27d79
A[3]=e6dd928b  B[3]=e8a884d8  C[3]=4f2bc6bb  D[3]=2c4e4517

Step 26: (r=29, s= 9)
A[0]=66a369ed  B[0]=a108062e  C[0]=094f4952  D[0]=6c50710c
A[1]=1d48f61b  B[1]=ecdb7705  C[1]=408c3911  D[1]=68a43c64
A[2]=846235f2  B[2]=93f8de10  C[2]=a1be654e  D[2]=ea84cb3d
A[3]=4e9045ef  B[3]=7cdbb251  C[3]=e8a884d8  D[3]=4f2bc6bb

Step 27: (r= 9, s=15)
A[0]=92d83045  B[0]=46d3dacd  C[0]=a108062e  D[0]=094f4952
A[1]=8bbf175c  B[1]=91ec363a  C[1]=ecdb7705  D[1]=408c3911
A[2]=3f6afd56  B[2]=c46be508  C[2]=93f8de10  D[2]=a1be654e
A[3]=a555290e  B[3]=208bde9d  C[3]=7cdbb251  D[3]=e8a884d8

Step 28: (r=15, s= 5)
A[0]=1523be5a  B[0]=1822c96c  C[0]=46d3dacd  D[0]=a108062e
A[1]=d3063668  B[1]=8bae45df  C[1]=91ec363a  D[1]=ecdb7705
A[2]=fb2da15a  B[2]=7eab1fb5  C[2]=c46be508  D[2]=93f8de10
```

```
A[3]=689395ea  B[3]=948752aa  C[3]=208bde9d  D[3]=7cdbb251

Step 29: (r= 5, s=29)
A[0]=1a10639e  B[0]=a477cb42  C[0]=1822c96c  D[0]=46d3dacd
A[1]=69601a80  B[1]=60c6cd1a  C[1]=8bae45df  D[1]=91ec363a
A[2]=d48ee1a4  B[2]=65b42b5f  C[2]=7eab1fb5  D[2]=c46be508
A[3]=756db953  B[3]=1272bd4d  C[3]=948752aa  D[3]=208bde9d

Step 30: (r=29, s= 9)
A[0]=fe2f0e5f  B[0]=c3420c73  C[0]=a477cb42  D[0]=1822c96c
A[1]=75d67fc4  B[1]=0d2c0350  C[1]=60c6cd1a  D[1]=8bae45df
A[2]=5108afab  B[2]=9a91dc34  C[2]=65b42b5f  D[2]=7eab1fb5
A[3]=062376c6  B[3]=6eadb72a  C[3]=1272bd4d  D[3]=948752aa

Step 31: (r= 9, s=15)
A[0]=012a64b5  B[0]=5e1cbffc  C[0]=c3420c73  D[0]=a477cb42
A[1]=31509afc  B[1]=acff88eb  C[1]=0d2c0350  D[1]=60c6cd1a
A[2]=2fcff0c9  B[2]=115f56a2  C[2]=9a91dc34  D[2]=65b42b5f
A[3]=858ea736  B[3]=46ed8c0c  C[3]=6eadb72a  D[3]=1272bd4d

Feed-Forward Step 0: (r=15, s= 5)
A[0]=60d92ce8  B[0]=325a8095  C[0]=5e1cbffc  D[0]=c3420c73
A[1]=1b55bf51  B[1]=4d7e18a8  C[1]=acff88eb  D[1]=0d2c0350
A[2]=6548138f  B[2]=f86497e7  C[2]=115f56a2  D[2]=9a91dc34
A[3]=331eb60d  B[3]=539b42c7  C[3]=46ed8c0c  D[3]=6eadb72a

Feed-Forward Step 1: (r= 5, s=29)
A[0]=a47ff906  B[0]=1b259d0c  C[0]=325a8095  D[0]=5e1cbffc
A[1]=75278f7d  B[1]=6ab7ea23  C[1]=4d7e18a8  D[1]=acff88eb
A[2]=a92e5ae6  B[2]=a90271ec  C[2]=f86497e7  D[2]=115f56a2
A[3]=28e0a6ba  B[3]=63d6c1a6  C[3]=539b42c7  D[3]=46ed8c0c

Feed-Forward Step 2: (r=29, s= 9)
A[0]=45acd4ca  B[0]=d48fff20  C[0]=1b259d0c  D[0]=325a8095
A[1]=61abfc9b  B[1]=aea4f1ef  C[1]=6ab7ea23  D[1]=4d7e18a8
A[2]=257ba1f9  B[2]=d525cb5c  C[2]=a90271ec  D[2]=f86497e7
A[3]=55fb8cb5  B[3]=451c14d7  C[3]=63d6c1a6  D[3]=539b42c7

Feed-Forward Step 3: (r= 9, s=15)
A[0]=359ab826  B[0]=59a9948b  C[0]=d48fff20  D[0]=1b259d0c
A[1]=f69c763b  B[1]=57f936c3  C[1]=aea4f1ef  D[1]=6ab7ea23
A[2]=f0088ba5  B[2]=f743f24a  C[2]=d525cb5c  D[2]=a90271ec
A[3]=6ae149af  B[3]=f7196aab  C[3]=451c14d7  D[3]=63d6c1a6
```

Compression Function Output

```
A[0]=359ab826  B[0]=59a9948b  C[0]=d48fff20  D[0]=1b259d0c
A[1]=f69c763b  B[1]=57f936c3  C[1]=aea4f1ef  D[1]=6ab7ea23
A[2]=f0088ba5  B[2]=f743f24a  C[2]=d525cb5c  D[2]=a90271ec
A[3]=6ae149af  B[3]=f7196aab  C[3]=451c14d7  D[3]=63d6c1a6
```

Final block

```
M[  0..  7] = 00 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    4  177  210   45  165  187  234   40
y[  8.. 15] =  101   34  138  136   32   51  140  236
y[ 16.. 23] =  197    5  107  213   42  239  210   91
y[ 24.. 31] =  112   87  126   65  121  118  204  159
y[ 32.. 39] =   32  210   63  149  138  147  181  215
y[ 40.. 47] =   58    4  174  220   32   36   73   94
y[ 48.. 55] =   60   67  181  117  175   93   92  129
y[ 56.. 63] =  246  229   94   37   17  151   88  210
y[ 64.. 71] =  253   80   47  212   92   70   23  217
y[ 72.. 79] =  156  223  119  121  225  206  117   21
y[ 80.. 87] =   60  252  150   44  215   18   47  166
y[ 88.. 95] =  145  170  131  192  136  139   53   98
y[ 96..103] =  225   47  194  108  119  110   76   42
y[104..111] =  199  253   83   37  225  221  184  163
y[112..119] =  197  190   76  140   82  164  165  128
y[120..127] =   11   28  163  220  240  106  169   47
```

Intermediate Expanded Message

```
Z[ 0] = c63002e4  2085de09  cd6abd84  1ce8ef61
Z[ 1] = 189248fd  a88faa01  24db1720  f0d3ab73
Z[ 2] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
Z[ 3] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
Z[ 4] = de091720  b1f42d87  b082aa01  e1a6c914
Z[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
Z[ 6] = 306b2b5c  548dc914  4335c4be  a380427c
Z[ 7] = ebc4f80d  1abd43ee  b3660c49  de093f98
Z[ 8] = 39d0fd1c  df7b21f7  3296427c  e318109f
Z[ 9] = e76eb703  577155ff  db25e8e0  0f2d548d
Z[10] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
Z[11] = c121af10  d107a4f2  aabaa88f  46d2264d
Z[12] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
Z[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
Z[14] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
Z[15] = 143c07f3  e543bc12  4c9af3b7  21f7c068
Z[16] = fc84037c  28f1d70f  5024afdc  1409ebf7
Z[17] = a80557fb  67a99857  e4201be0  65eb9a15
```

```
Z[18] = 3444cbbc  a2cb5d35  db6a2496  28f1d70f
Z[19] = 9e706190  923e6dc2  96996967  2e2bd1d5
Z[20] = e4201be0  c91f36e1  67a99857  4234bdcc
Z[21] = cd7a3286  484db7b3  e4201be0  c0693f97
Z[22] = cbbc3444  4234bdcc  476eb892  afdc5024
Z[23] = 0995f66b  ae1e51e2  f1310ecf  b3584ca8
Z[24] = 45b0ba50  d8cd2733  3cfac306  dd2822d8
Z[25] = e2621d9e  69679699  d3932c6d  124bedb5
Z[26] = fba5045b  2654d9ac  0faef052  b0bb4f45
Z[27] = b4374bc9  c761389f  993666ca  555eaaa2
Z[28] = 28f1d70f  5e14a1ec  5fd2a02e  2496db6a
Z[29] = fc84037c  203bdfc5  e0a41f5c  ae1e51e2
Z[30] = c5a33a5d  9a1565eb  aefd5103  6f809080
Z[31] = 1864e79c  dfc5203b  5c56a3aa  28f1d70f
```

Expanded Message

```
W[ 0] = de091720  b1f42d87  b082aa01  e1a6c914
W[ 1] = 306b2b5c  548dc914  4335c4be  a380427c
W[ 2] = c63002e4  2085de09  cd6abd84  1ce8ef61
W[ 3] = 039dd4a4  e0344d53  f2fe1e5a  41c3de09
W[ 4] = ebc4f80d  1abd43ee  b3660c49  de093f98
W[ 5] = 02e429ea  e543c405  1a041720  43ee34c1
W[ 6] = 3edf50f0  2ef95b0e  55465771  b92ed9b3
W[ 7] = 189248fd  a88faa01  24db1720  f0d3ab73
W[ 8] = 143c07f3  e543bc12  4c9af3b7  21f7c068
W[ 9] = c121af10  d107a4f2  aabaa88f  46d2264d
W[10] = 21f7e8e0  4e0cd279  4f7e55ff  1e5a36ec
W[11] = 39d0fd1c  df7b21f7  3296427c  e318109f
W[12] = e76eb703  577155ff  db25e8e0  0f2d548d
W[13] = fd1cd616  1abd3bfb  e5fce8e0  bc12cb3f
W[14] = fc632b5c  1fccb2ad  0d02e1a6  be3d21f7
W[15] = cf95d4a4  ab7336ec  bccb3b42  5c80bd84
W[16] = a80557fb  67a99857  e4201be0  65eb9a15
W[17] = 3444cbbc  a2cb5d35  db6a2496  28f1d70f
W[18] = 0995f66b  ae1e51e2  f1310ecf  b3584ca8
W[19] = e4201be0  c91f36e1  67a99857  4234bdcc
W[20] = cbbc3444  4234bdcc  476eb892  afdc5024
W[21] = cd7a3286  484db7b3  e4201be0  c0693f97
W[22] = fc84037c  28f1d70f  5024afdc  1409ebf7
W[23] = 9e706190  923e6dc2  96996967  2e2bd1d5
W[24] = c5a33a5d  9a1565eb  aefd5103  6f809080
W[25] = 45b0ba50  d8cd2733  3cfac306  dd2822d8
W[26] = e2621d9e  69679699  d3932c6d  124bedb5
W[27] = 1864e79c  dfc5203b  5c56a3aa  28f1d70f
W[28] = b4374bc9  c761389f  993666ca  555eaaa2
W[29] = fc84037c  203bdfc5  e0a41f5c  ae1e51e2
W[30] = 28f1d70f  5e14a1ec  5fd2a02e  2496db6a
W[31] = fba5045b  2654d9ac  0faef052  b0bb4f45
```

Feistel Steps

```
IV :
A[0]=359ab826  B[0]=59a9948b  C[0]=d48fff20  D[0]=1b259d0c
A[1]=f69c763b  B[1]=57f936c3  C[1]=aea4f1ef  D[1]=6ab7ea23
A[2]=f0088ba5  B[2]=f743f24a  C[2]=d525cb5c  D[2]=a90271ec
A[3]=6ae149af  B[3]=f7196aab  C[3]=451c14d7  D[3]=63d6c1a6

IV XOR M :
A[0]=359aba26  B[0]=59a9948b  C[0]=d48fff20  D[0]=1b259d0c
A[1]=f69c763b  B[1]=57f936c3  C[1]=aea4f1ef  D[1]=6ab7ea23
A[2]=f0088ba5  B[2]=f743f24a  C[2]=d525cb5c  D[2]=a90271ec
A[3]=6ae149af  B[3]=f7196aab  C[3]=451c14d7  D[3]=63d6c1a6

Step  0: (r= 3, s=20)
A[0]=47d05da7  B[0]=acd5d131  C[0]=59a9948b  D[0]=d48fff20
A[1]=775c137b  B[1]=b4e3b1df  C[1]=57f936c3  D[1]=aea4f1ef
A[2]=3b5f3828  B[2]=80445d2f  C[2]=f743f24a  D[2]=d525cb5c
A[3]=28309adf  B[3]=570a4d7b  C[3]=f7196aab  D[3]=451c14d7

Step  1: (r=20, s=14)
A[0]=c16cfe70  B[0]=da747d05  C[0]=acd5d131  D[0]=59a9948b
A[1]=aa2a110d  B[1]=37b775c1  C[1]=b4e3b1df  D[1]=57f936c3
A[2]=f515b42d  B[2]=8283b5f3  C[2]=80445d2f  D[2]=f743f24a
A[3]=a7ab25aa  B[3]=adf28309  C[3]=570a4d7b  D[3]=f7196aab

Step  2: (r=14, s=27)
A[0]=04a9e32d  B[0]=3f9c305b  C[0]=da747d05  D[0]=acd5d131
A[1]=6a869379  B[1]=84436a8a  C[1]=37b775c1  D[1]=b4e3b1df
A[2]=53922f51  B[2]=6d0b7d45  C[2]=8283b5f3  D[2]=80445d2f
A[3]=67e95576  B[3]=c96aa9ea  C[3]=adf28309  D[3]=570a4d7b

Step  3: (r=27, s= 3)
A[0]=051ba06e  B[0]=68254f19  C[0]=3f9c305b  D[0]=da747d05
A[1]=059a7880  B[1]=cb54349b  C[1]=84436a8a  D[1]=37b775c1
A[2]=0a571a7a  B[2]=8a9c917a  C[2]=6d0b7d45  D[2]=8283b5f3
A[3]=dd99ac16  B[3]=b33f4aab  C[3]=c96aa9ea  D[3]=adf28309

Step  4: (r= 3, s=20)
A[0]=83b2f969  B[0]=28dd0370  C[0]=68254f19  D[0]=3f9c305b
A[1]=76565043  B[1]=2cd3c400  C[1]=cb54349b  D[1]=84436a8a
A[2]=a8316143  B[2]=52b8d3d0  C[2]=8a9c917a  D[2]=6d0b7d45
A[3]=dd9356e6  B[3]=eccd60b6  C[3]=b33f4aab  D[3]=c96aa9ea

Step  5: (r=20, s=14)
A[0]=7daa1de3  B[0]=96983b2f  C[0]=28dd0370  D[0]=68254f19
A[1]=cf128f2c  B[1]=04376565  C[1]=2cd3c400  D[1]=cb54349b
A[2]=b005ffa1  B[2]=143a8316  C[2]=52b8d3d0  D[2]=8a9c917a
A[3]=0c8ba823  B[3]=6e6dd935  C[3]=eccd60b6  D[3]=b33f4aab
```

```
Step  6: (r=14, s=27)
A[0]=0ae8199f  B[0]=8778df6a  C[0]=96983b2f  D[0]=28dd0370
A[1]=e81b76a7  B[1]=a3cb33c4  C[1]=04376565  D[1]=2cd3c400
A[2]=c989a105  B[2]=7fe86c01  C[2]=143a8316  D[2]=52b8d3d0
A[3]=3642bfce  B[3]=ea08c322  C[3]=6e6dd935  D[3]=eccd60b6

Step  7: (r=27, s= 3)
A[0]=718789ee  B[0]=f85740cc  C[0]=8778df6a  D[0]=96983b2f
A[1]=1da94531  B[1]=3f40dbb5  C[1]=a3cb33c4  D[1]=04376565
A[2]=a23ba07a  B[2]=2e4c4d08  C[2]=7fe86c01  D[2]=143a8316
A[3]=9e90162f  B[3]=71b215fe  C[3]=ea08c322  D[3]=6e6dd935

Step  8: (r=26, s= 4)
A[0]=d9b043fe  B[0]=b9c61e27  C[0]=f85740cc  D[0]=8778df6a
A[1]=7662454b  B[1]=c476a514  C[1]=3f40dbb5  D[1]=a3cb33c4
A[2]=c8566dc6  B[2]=ea88ee81  C[2]=2e4c4d08  D[2]=7fe86c01
A[3]=c9ad0ad7  B[3]=be7a4058  C[3]=71b215fe  D[3]=ea08c322

Step  9: (r= 4, s=23)
A[0]=d5680d34  B[0]=9b043fed  C[0]=b9c61e27  D[0]=f85740cc
A[1]=d031c838  B[1]=662454b7  C[1]=c476a514  D[1]=3f40dbb5
A[2]=271095ad  B[2]=8566dc6c  C[2]=ea88ee81  D[2]=2e4c4d08
A[3]=da18df36  B[3]=9ad0ad7c  C[3]=be7a4058  D[3]=71b215fe

Step 10: (r=23, s=11)
A[0]=c6aeb782  B[0]=9a6ab406  C[0]=9b043fed  D[0]=b9c61e27
A[1]=772e9ed7  B[1]=1c6818e4  C[1]=662454b7  D[1]=c476a514
A[2]=3876a6c9  B[2]=d693884a  C[2]=8566dc6c  D[2]=ea88ee81
A[3]=913de679  B[3]=9b6d0c6f  C[3]=9ad0ad7c  D[3]=be7a4058

Step 11: (r=11, s=26)
A[0]=7f715121  B[0]=75bc1635  C[0]=9a6ab406  D[0]=9b043fed
A[1]=ae143508  B[1]=74f6bbb9  C[1]=1c6818e4  D[1]=662454b7
A[2]=1c84de5a  B[2]=b53649c3  C[2]=d693884a  D[2]=8566dc6c
A[3]=05ecb932  B[3]=ef33cc89  C[3]=9b6d0c6f  D[3]=9ad0ad7c

Step 12: (r=26, s= 4)
A[0]=41690224  B[0]=85fdc544  C[0]=75bc1635  D[0]=9a6ab406
A[1]=09105968  B[1]=22b850d4  C[1]=74f6bbb9  D[1]=1c6818e4
A[2]=1a508c53  B[2]=68721379  C[2]=b53649c3  D[2]=d693884a
A[3]=1cb6a887  B[3]=c817b2e4  C[3]=ef33cc89  D[3]=9b6d0c6f

Step 13: (r= 4, s=23)
A[0]=c5778779  B[0]=16902244  C[0]=85fdc544  D[0]=75bc1635
A[1]=37167348  B[1]=91059680  C[1]=22b850d4  D[1]=74f6bbb9
A[2]=558aa381  B[2]=a508c531  C[2]=68721379  D[2]=b53649c3
A[3]=aa977240  B[3]=cb6a8871  C[3]=c817b2e4  D[3]=ef33cc89

Step 14: (r=23, s=11)
```

```
A[0]=4a623af9  B[0]=bce2bbc3  C[0]=16902244  D[0]=85fdc544
A[1]=7eb3fb8f  B[1]=a41b8b39  C[1]=91059680  D[1]=22b850d4
A[2]=3dca1cf3  B[2]=c0aac551  C[2]=a508c531  D[2]=68721379
A[3]=01e9bf7f  B[3]=20554bb9  C[3]=cb6a8871  D[3]=c817b2e4

Step 15: (r=11, s=26)
A[0]=f6b97140  B[0]=11d7ca53  C[0]=bce2bbc3  D[0]=16902244
A[1]=7404f49c  B[1]=9fdc7bf5  C[1]=a41b8b39  D[1]=91059680
A[2]=c502eaa3  B[2]=50e799ee  C[2]=c0aac551  D[2]=a508c531
A[3]=247483e4  B[3]=4dfbf80f  C[3]=20554bb9  D[3]=cb6a8871

Step 16: (r=19, s=28)
A[0]=d25a3477  B[0]=8a07b5cb  C[0]=11d7ca53  D[0]=bce2bbc3
A[1]=1deb12bf  B[1]=a4e3a027  C[1]=9fdc7bf5  D[1]=a41b8b39
A[2]=5bbe5a94  B[2]=551e2817  C[2]=50e799ee  D[2]=c0aac551
A[3]=bd643475  B[3]=1f2123a4  C[3]=4dfbf80f  D[3]=20554bb9

Step 17: (r=28, s= 7)
A[0]=9d7ec6e3  B[0]=7d25a347  C[0]=8a07b5cb  D[0]=11d7ca53
A[1]=4aff2e2d  B[1]=f1deb12b  C[1]=a4e3a027  D[1]=9fdc7bf5
A[2]=375f563d  B[2]=45bbe5a9  C[2]=551e2817  D[2]=50e799ee
A[3]=73642c7e  B[3]=5bd64347  C[3]=1f2123a4  D[3]=4dfbf80f

Step 18: (r= 7, s=22)
A[0]=81e5bb82  B[0]=bf6371ce  C[0]=7d25a347  D[0]=8a07b5cb
A[1]=3037d4f6  B[1]=7f9716a5  C[1]=f1deb12b  D[1]=a4e3a027
A[2]=ec380c3e  B[2]=afab1e9b  C[2]=45bbe5a9  D[2]=551e2817
A[3]=debb9820  B[3]=b2163f39  C[3]=5bd64347  D[3]=1f2123a4

Step 19: (r=22, s=19)
A[0]=2b4e6a4b  B[0]=e0a0796e  C[0]=bf6371ce  D[0]=7d25a347
A[1]=6de2adf6  B[1]=3d8c0df5  C[1]=7f9716a5  D[1]=f1deb12b
A[2]=50ebcd0b  B[2]=0fbb0e03  C[2]=afab1e9b  D[2]=45bbe5a9
A[3]=244bb356  B[3]=0837aee6  C[3]=b2163f39  D[3]=5bd64347

Step 20: (r=19, s=28)
A[0]=0ef7b422  B[0]=52595a73  C[0]=e0a0796e  D[0]=bf6371ce
A[1]=33741f2c  B[1]=6fb36f15  C[1]=3d8c0df5  D[1]=7f9716a5
A[2]=047e7d21  B[2]=685a875e  C[2]=0fbb0e03  D[2]=afab1e9b
A[3]=6515ffa1  B[3]=9ab1225d  C[3]=0837aee6  D[3]=b2163f39

Step 21: (r=28, s= 7)
A[0]=f7d64339  B[0]=20ef7b42  C[0]=52595a73  D[0]=e0a0796e
A[1]=e2c0267d  B[1]=c33741f2  C[1]=6fb36f15  D[1]=3d8c0df5
A[2]=43943a92  B[2]=1047e7d2  C[2]=685a875e  D[2]=0fbb0e03
A[3]=1dce1caf  B[3]=16515ffa  C[3]=9ab1225d  D[3]=0837aee6

Step 22: (r= 7, s=22)
A[0]=77673fe7  B[0]=eb219cfb  C[0]=20ef7b42  D[0]=52595a73
```

```
A[1]=e86fd574  B[1]=60133ef1  C[1]=c33741f2  D[1]=6fb36f15
A[2]=53766527  B[2]=ca1d4921  C[2]=1047e7d2  D[2]=685a875e
A[3]=623061a9  B[3]=e70e578e  C[3]=16515ffa  D[3]=9ab1225d

Step 23: (r=22, s=19)
A[0]=29077f20  B[0]=f9ddd9cf  C[0]=eb219cfb  D[0]=20ef7b42
A[1]=00979d61  B[1]=5d3a1bf5  C[1]=60133ef1  D[1]=c33741f2
A[2]=a9206429  B[2]=49d4dd99  C[2]=ca1d4921  D[2]=1047e7d2
A[3]=bc1b935f  B[3]=6a588c18  C[3]=e70e578e  D[3]=16515ffa

Step 24: (r=15, s= 5)
A[0]=05c26fa5  B[0]=bf901483  C[0]=f9ddd9cf  D[0]=eb219cfb
A[1]=ddf14e67  B[1]=ceb0804b  C[1]=5d3a1bf5  D[1]=60133ef1
A[2]=160099ce  B[2]=3214d490  C[2]=49d4dd99  D[2]=ca1d4921
A[3]=dd66b6e1  B[3]=c9afde0d  C[3]=6a588c18  D[3]=e70e578e

Step 25: (r= 5, s=29)
A[0]=85e13744  B[0]=b84df4a0  C[0]=bf901483  D[0]=f9ddd9cf
A[1]=8d8a2b39  B[1]=be29ccfb  C[1]=ceb0804b  D[1]=5d3a1bf5
A[2]=c4ab90b7  B[2]=c01339c2  C[2]=3214d490  D[2]=49d4dd99
A[3]=b418700a  B[3]=acd6dc3b  C[3]=c9afde0d  D[3]=6a588c18

Step 26: (r=29, s= 9)
A[0]=54092694  B[0]=90bc26e8  C[0]=b84df4a0  D[0]=bf901483
A[1]=ad0b853f  B[1]=31b14567  C[1]=be29ccfb  D[1]=ceb0804b
A[2]=55401e1f  B[2]=f8957216  C[2]=c01339c2  D[2]=3214d490
A[3]=496bdfbc  B[3]=56830e01  C[3]=acd6dc3b  D[3]=c9afde0d

Step 27: (r= 9, s=15)
A[0]=799c06ca  B[0]=124d28a8  C[0]=90bc26e8  D[0]=b84df4a0
A[1]=4ef6695d  B[1]=170a7f5a  C[1]=31b14567  D[1]=be29ccfb
A[2]=685557e7  B[2]=803c3eaa  C[2]=f8957216  D[2]=c01339c2
A[3]=789a6af6  B[3]=d7bf7892  C[3]=56830e01  D[3]=acd6dc3b

Step 28: (r=15, s= 5)
A[0]=d8db91aa  B[0]=03653cce  C[0]=124d28a8  D[0]=90bc26e8
A[1]=53a2135d  B[1]=34aea77b  C[1]=170a7f5a  D[1]=31b14567
A[2]=615e2295  B[2]=abf3b42a  C[2]=803c3eaa  D[2]=f8957216
A[3]=1d836ab9  B[3]=357b3c4d  C[3]=d7bf7892  D[3]=56830e01

Step 29: (r= 5, s=29)
A[0]=ffb5ff0d  B[0]=1b72355b  C[0]=03653cce  D[0]=124d28a8
A[1]=9da042b3  B[1]=74426baa  C[1]=34aea77b  D[1]=170a7f5a
A[2]=aac92e5e  B[2]=2bc452ac  C[2]=abf3b42a  D[2]=803c3eaa
A[3]=f78e06b9  B[3]=b06d5723  C[3]=357b3c4d  D[3]=d7bf7892

Step 30: (r=29, s= 9)
A[0]=dc2e1503  B[0]=bff6bfe1  C[0]=1b72355b  D[0]=03653cce
A[1]=5863291e  B[1]=73b40856  C[1]=74426baa  D[1]=34aea77b
```

```
A[2]=df1bcdee  B[2]=d55925cb  C[2]=2bc452ac  D[2]=abf3b42a
A[3]=4acb0b44  B[3]=3ef1c0d7  C[3]=b06d5723  D[3]=357b3c4d

Step 31: (r= 9, s=15)
A[0]=72d22cfe  B[0]=5c2a07b8  C[0]=bff6bfe1  D[0]=1b72355b
A[1]=6b396e47  B[1]=c6523cb0  C[1]=73b40856  D[1]=74426baa
A[2]=515f5535  B[2]=379bddbe  C[2]=d55925cb  D[2]=2bc452ac
A[3]=adbecd3f  B[3]=96168895  C[3]=3ef1c0d7  D[3]=b06d5723

Feed-Forward Step 0: (r=15, s= 5)
A[0]=7d945ce1  B[0]=167f3969  C[0]=5c2a07b8  D[0]=bff6bfe1
A[1]=58fc6766  B[1]=b723b59c  C[1]=c6523cb0  D[1]=73b40856
A[2]=83aa60d5  B[2]=aa9aa8af  C[2]=379bddbe  D[2]=d55925cb
A[3]=4b446e5f  B[3]=669fd6df  C[3]=96168895  D[3]=3ef1c0d7

Feed-Forward Step 1: (r= 5, s=29)
A[0]=1b07e8ac  B[0]=b28b9c2f  C[0]=167f3969  D[0]=5c2a07b8
A[1]=14c7bb7e  B[1]=1f8ceccb  C[1]=b723b59c  D[1]=c6523cb0
A[2]=42f2b6e7  B[2]=754c1ab0  C[2]=aa9aa8af  D[2]=379bddbe
A[3]=41112b17  B[3]=688dcbe9  C[3]=669fd6df  D[3]=96168895

Feed-Forward Step 2: (r=29, s= 9)
A[0]=2dd981fd  B[0]=8360fd15  C[0]=b28b9c2f  D[0]=167f3969
A[1]=20152935  B[1]=c298f76f  C[1]=1f8ceccb  D[1]=b723b59c
A[2]=fba9ab4c  B[2]=e85e56dc  C[2]=754c1ab0  D[2]=aa9aa8af
A[3]=085b6798  B[3]=e8222562  C[3]=688dcbe9  D[3]=669fd6df

Feed-Forward Step 3: (r= 9, s=15)
A[0]=0d1cfc6a  B[0]=b303fa5b  C[0]=8360fd15  D[0]=b28b9c2f
A[1]=f9a650ca  B[1]=2a526a40  C[1]=c298f76f  D[1]=1f8ceccb
A[2]=49cf9a4f  B[2]=535699f7  C[2]=e85e56dc  D[2]=754c1ab0
A[3]=cd4583be  B[3]=b6cf3010  C[3]=e8222562  D[3]=688dcbe9
```

Compression Function Output

```
A[0]=0d1cfc6a  B[0]=b303fa5b  C[0]=8360fd15  D[0]=b28b9c2f
A[1]=f9a650ca  B[1]=2a526a40  C[1]=c298f76f  D[1]=1f8ceccb
A[2]=49cf9a4f  B[2]=535699f7  C[2]=e85e56dc  D[2]=754c1ab0
A[3]=cd4583be  B[3]=b6cf3010  C[3]=e8222562  D[3]=688dcbe9
```

Hash Function Output

```
6a fc 1c 0d ca 50 a6 f9 4f 9a cf 49 be 83 45 cd
5b fa 03 b3 40 6a 52 2a f7 99 56 53 10 30 cf b6
```

6.2.3 Two blocks message

We use the message made of 700 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =  130  139   95   90   30    8   23   57
y[  8.. 15] =  129  152  176  135   15   86  140   53
y[ 16.. 23] =  193   34   88   34  136  231   70    7
y[ 24.. 31] =  225   75   44   72   68  127   35  120
y[ 32.. 39] =  241  151   22   70   34  193  146  163
y[ 40.. 47] =  249   20   11  219   17   74   73  235
y[ 48.. 55] =  253   50  134  235  137   79  165   92
y[ 56.. 63] =  255  194   67  159  197   44  211   92
y[ 64.. 71] =  256  181  162  182  227  122  234  179
y[ 72.. 79] =  128   91   81  207  242  115  117  226
y[ 80.. 87] =   64   80  169  160  121  120  187   42
y[ 88.. 95] =   32   58  213  108  189   44  222  244
y[ 96..103] =   16  248  235    8  223  133  111  210
y[104..111] =    8  180  246  193  240  238  184  157
y[112..119] =    4  177  123   70  120   85   92  171
y[120..127] =    2   76  190  217   60  190   46   94
```

Intermediate Expanded Message

```
Z[ 0] = aabaa439  410a44a7  05c815ae  2931109f
Z[ 1] = b41fa380  a7d6c577  3e260ad7  264dab73
Z[ 2] = 1892d1c0  18923f98  ed36a88f  050f3296
Z[ 3] = 3633e8e0  34081fcc  5bc73124  56b8194b
Z[ 4] = b366f470  32960fe6  d1c01892  bc12afc9
Z[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
Z[ 6] = 2422fd1c  f01aa71d  3917a948  427cbd84
Z[ 7] = d279fe8e  b92e306b  1fccd4a4  427cdec2
Z[ 8] = c914ff47  c9cdbb59  582aea52  c7a2ef61
Z[ 9] = 41c35c80  dbde3a89  531bf529  e999548d
Z[10] = 39d02e40  b9e7c068  56b85771  1e5acd6a
Z[11] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
Z[12] = f97f0b90  05c8f01a  a664e76e  de095037
Z[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
Z[14] = c63002e4  329658e3  3d6d56b8  c1da427c
Z[15] = 36ec0172  e318cf95  cf952b5c  43ee213e
Z[16] = ff21915f  ad3f52c1  e5de1a22  ebf71409
Z[17] = 6f809080  468fb971  f2ef0d11  65eb9a15
```

```
Z[18] = 37c0c840  b3584ca8  69679699  c3063cfa
Z[19] = 1be0e420  d9ac2654  c4c43b3c  e1831e7d
Z[20] = 0df0f210  ecd6132a  e2621d9e  60b19f4f
Z[21] = 06f8f908  f66b0995  f1310ecf  c0693f97
Z[22] = 037cfc84  6b2594db  68889778  5024afdc
Z[23] = 01befe42  c5a33a5d  3444cbbc  2812d7ee
Z[24] = bdcc9936  beab4e66  6a4606f8  bc0e31a7
Z[25] = 4f45a489  d47295ba  642d4aea  e4ff2e2b
Z[26] = 45b01d9e  ab811d9e  6888e95a  24960619
Z[27] = 32864155  5e143eb8  26546ea1  f4ad6888
Z[28] = f829a3aa  06f83cfa  93fcc840  d70fae1e
Z[29] = bced116c  c840dee6  ef734076  a8e4ecd6
Z[30] = ba502b8e  3cfaecd6  4a0b44d1  b5165024
Z[31] = 4234c91f  dd28aaa2  c5a32654  51e25024
```

Expanded Message

```
W[ 0] = b366f470  32960fe6  d1c01892  bc12afc9
W[ 1] = 2422fd1c  f01aa71d  3917a948  427cbd84
W[ 2] = aabaa439  410a44a7  05c815ae  2931109f
W[ 3] = 1892d1c0  18923f98  ed36a88f  050f3296
W[ 4] = d279fe8e  b92e306b  1fccd4a4  427cdec2
W[ 5] = 0e74fa38  e48a07f3  357a0c49  f01a34c1
W[ 6] = 3633e8e0  34081fcc  5bc73124  56b8194b
W[ 7] = b41fa380  a7d6c577  3e260ad7  264dab73
W[ 8] = 36ec0172  e318cf95  cf952b5c  43ee213e
W[ 9] = 29ea1720  4e0ce034  1fcccedc  f69be6b5
W[10] = f97f0b90  05c8f01a  a664e76e  de095037
W[11] = c914ff47  c9cdbb59  582aea52  c7a2ef61
W[12] = 41c35c80  dbde3a89  531bf529  e999548d
W[13] = c85b05c8  d1c0f80d  f245f3b7  b7bccb3f
W[14] = 39d02e40  b9e7c068  56b85771  1e5acd6a
W[15] = c63002e4  329658e3  3d6d56b8  c1da427c
W[16] = 6f809080  468fb971  f2ef0d11  65eb9a15
W[17] = 37c0c840  b3584ca8  69679699  c3063cfa
W[18] = 01befe42  c5a33a5d  3444cbbc  2812d7ee
W[19] = 0df0f210  ecd6132a  e2621d9e  60b19f4f
W[20] = 037cfc84  6b2594db  68889778  5024afdc
W[21] = 06f8f908  f66b0995  f1310ecf  c0693f97
W[22] = ff21915f  ad3f52c1  e5de1a22  ebf71409
W[23] = 1be0e420  d9ac2654  c4c43b3c  e1831e7d
W[24] = ba502b8e  3cfaecd6  4a0b44d1  b5165024
W[25] = bdcc9936  beab4e66  6a4606f8  bc0e31a7
W[26] = 4f45a489  d47295ba  642d4aea  e4ff2e2b
W[27] = 4234c91f  dd28aaa2  c5a32654  51e25024
W[28] = 32864155  5e143eb8  26546ea1  f4ad6888
W[29] = bced116c  c840dee6  ef734076  a8e4ecd6
W[30] = f829a3aa  06f83cfa  93fcc840  d70fae1e
W[31] = 45b01d9e  ab811d9e  6888e95a  24960619
```

Feistel Steps

```
IV :
A[0]=99dae06a  B[0]=da4d98d0  C[0]=fd892a60  D[0]=fad01f14
A[1]=c3d43239  B[1]=cf5c52be  C[1]=8a471f8c  D[1]=9eeef3b3
A[2]=4979de73  B[2]=655cbaf9  C[2]=86ce033f  D[2]=68aec37a
A[3]=3ee5d052  B[3]=2a9d238e  C[3]=0ff768d3  D[3]=6b209d72

IV XOR M :
A[0]=66251f95  B[0]=25b2672f  C[0]=0276d59f  D[0]=052fe0eb
A[1]=3c2bcdc6  B[1]=30a3ad41  C[1]=75b8e073  D[1]=61110c4c
A[2]=b686218c  B[2]=9aa34506  C[2]=7931fcc0  D[2]=97513c85
A[3]=c11a2fad  B[3]=d562dc71  C[3]=f008972c  D[3]=94df628d

Step  0: (r= 3, s=20)
A[0]=a80c3eca  B[0]=3128fcab  C[0]=25b2672f  D[0]=0276d59f
A[1]=4e616211  B[1]=e15e6e31  C[1]=30a3ad41  D[1]=75b8e073
A[2]=2e85c9c1  B[2]=b4310c65  C[2]=9aa34506  D[2]=7931fcc0
A[3]=189d1bf5  B[3]=08d17d6e  C[3]=d562dc71  D[3]=f008972c

Step  1: (r=20, s=14)
A[0]=b02d7b71  B[0]=ecaa80c3  C[0]=3128fcab  D[0]=25b2672f
A[1]=5d09ff76  B[1]=2114e616  C[1]=e15e6e31  D[1]=30a3ad41
A[2]=193e5a5e  B[2]=9c12e85c  C[2]=b4310c65  D[2]=9aa34506
A[3]=6d99e634  B[3]=bf5189d1  C[3]=08d17d6e  D[3]=d562dc71

Step  2: (r=14, s=27)
A[0]=1b6a43c3  B[0]=5edc6c0b  C[0]=ecaa80c3  D[0]=3128fcab
A[1]=8f2fad0e  B[1]=7fdd9742  C[1]=2114e616  D[1]=e15e6e31
A[2]=0471109f  B[2]=9697864f  C[2]=9c12e85c  D[2]=b4310c65
A[3]=b03b983e  B[3]=798d1b66  C[3]=bf5189d1  D[3]=08d17d6e

Step  3: (r=27, s= 3)
A[0]=3c47fbf6  B[0]=18db521e  C[0]=5edc6c0b  D[0]=ecaa80c3
A[1]=3df5839a  B[1]=74797d68  C[1]=7fdd9742  D[1]=2114e616
A[2]=04b83c37  B[2]=f8238884  C[2]=9697864f  D[2]=9c12e85c
A[3]=ddc7ccc2  B[3]=f581dcc1  C[3]=798d1b66  D[3]=bf5189d1

Step  4: (r= 3, s=20)
A[0]=86a9dd10  B[0]=e23fdfb1  C[0]=18db521e  D[0]=5edc6c0b
A[1]=027765c2  B[1]=efac1cd1  C[1]=74797d68  D[1]=7fdd9742
A[2]=7eb36f4a  B[2]=25c1e1b8  C[2]=f8238884  D[2]=9697864f
A[3]=379fd4f5  B[3]=ee3e6616  C[3]=f581dcc1  D[3]=798d1b66

Step  5: (r=20, s=14)
A[0]=45fce739  B[0]=d1086a9d  C[0]=e23fdfb1  D[0]=18db521e
A[1]=9690ecb6  B[1]=5c202776  C[1]=efac1cd1  D[1]=74797d68
A[2]=30107cca  B[2]=f4a7eb36  C[2]=25c1e1b8  D[2]=f8238884
A[3]=255f3fc7  B[3]=4f5379fd  C[3]=ee3e6616  D[3]=f581dcc1
```

```
Step  6: (r=14, s=27)
A[0]=f3b006f9  B[0]=39ce517f  C[0]=d1086a9d  D[0]=e23fdfb1
A[1]=736b9a55  B[1]=3b2da5a4  C[1]=5c202776  D[1]=efac1cd1
A[2]=e4352e72  B[2]=1f328c04  C[2]=f4a7eb36  D[2]=25c1e1b8
A[3]=57ab1d2e  B[3]=cff1c957  C[3]=4f5379fd  D[3]=ee3e6616

Step  7: (r=27, s= 3)
A[0]=d65fdae7  B[0]=cf9d8037  C[0]=39ce517f  D[0]=d1086a9d
A[1]=0821a6c9  B[1]=ab9b5cd2  C[1]=3b2da5a4  D[1]=5c202776
A[2]=909a5661  B[2]=9721a973  C[2]=1f328c04  D[2]=f4a7eb36
A[3]=cf96b515  B[3]=72bd58e9  C[3]=cff1c957  D[3]=4f5379fd

Step  8: (r=26, s= 4)
A[0]=9d3f5b8a  B[0]=9f597f6b  C[0]=cf9d8037  D[0]=39ce517f
A[1]=2aa23850  B[1]=2420869b  C[1]=ab9b5cd2  D[1]=3b2da5a4
A[2]=8d184a4a  B[2]=86426959  C[2]=9721a973  D[2]=1f328c04
A[3]=02c8b758  B[3]=573e5ad4  C[3]=72bd58e9  D[3]=cff1c957

Step  9: (r= 4, s=23)
A[0]=c0a64dc9  B[0]=d3f5b8a9  C[0]=9f597f6b  D[0]=cf9d8037
A[1]=61a0af65  B[1]=aa238502  C[1]=2420869b  D[1]=ab9b5cd2
A[2]=00e0494b  B[2]=d184a4a8  C[2]=86426959  D[2]=9721a973
A[3]=28bfea87  B[3]=2c8b7580  C[3]=573e5ad4  D[3]=72bd58e9

Step 10: (r=23, s=11)
A[0]=80e4659f  B[0]=e4e05326  C[0]=d3f5b8a9  D[0]=9f597f6b
A[1]=cc14a6d0  B[1]=b2b0d057  C[1]=aa238502  D[1]=2420869b
A[2]=891c2e15  B[2]=a5807024  C[2]=d184a4a8  D[2]=86426959
A[3]=75afd9a8  B[3]=43945ff5  C[3]=2c8b7580  D[3]=573e5ad4

Step 11: (r=11, s=26)
A[0]=42622da7  B[0]=232cfc07  C[0]=e4e05326  D[0]=d3f5b8a9
A[1]=990dcaba  B[1]=a5368660  C[1]=b2b0d057  D[1]=aa238502
A[2]=81ecb3d8  B[2]=e170ac48  C[2]=a5807024  D[2]=d184a4a8
A[3]=fad81d7f  B[3]=7ecd43ad  C[3]=43945ff5  D[3]=2c8b7580

Step 12: (r=26, s= 4)
A[0]=6bfd5c31  B[0]=9d0988b6  C[0]=232cfc07  D[0]=e4e05326
A[1]=d56fd2a2  B[1]=ea64372a  C[1]=a5368660  D[1]=b2b0d057
A[2]=68000211  B[2]=6207b2cf  C[2]=e170ac48  D[2]=a5807024
A[3]=ad1c295f  B[3]=ffeb6075  C[3]=7ecd43ad  D[3]=43945ff5

Step 13: (r= 4, s=23)
A[0]=12ec55b0  B[0]=bfd5c316  C[0]=9d0988b6  D[0]=232cfc07
A[1]=14f78229  B[1]=56fd2a2d  C[1]=ea64372a  D[1]=a5368660
A[2]=d251a699  B[2]=80002116  C[2]=6207b2cf  D[2]=e170ac48
A[3]=affab973  B[3]=d1c295fa  C[3]=ffeb6075  D[3]=7ecd43ad

Step 14: (r=23, s=11)
```

```
A[0]=6bea6ba7  B[0]=d809762a  C[0]=bfd5c316  D[0]=9d0988b6
A[1]=e830b683  B[1]=148a7bc1  C[1]=56fd2a2d  D[1]=ea64372a
A[2]=0f0ac52d  B[2]=4ce928d3  C[2]=80002116  D[2]=6207b2cf
A[3]=6e1dcb12  B[3]=b9d7fd5c  C[3]=d1c295fa  D[3]=ffeb6075

Step 15: (r=11, s=26)
A[0]=57a57433  B[0]=535d3b5f  C[0]=d809762a  D[0]=bfd5c316
A[1]=281f5e9a  B[1]=85b41f41  C[1]=148a7bc1  D[1]=56fd2a2d
A[2]=ce0b3009  B[2]=56296878  C[2]=4ce928d3  D[2]=80002116
A[3]=b4a29542  B[3]=ee589370  C[3]=b9d7fd5c  D[3]=d1c295fa

Step 16: (r=19, s=28)
A[0]=05777955  B[0]=a19abd2b  C[0]=535d3b5f  D[0]=d809762a
A[1]=7b708286  B[1]=f4d140fa  C[1]=85b41f41  D[1]=148a7bc1
A[2]=c5b32a84  B[2]=804e7059  C[2]=56296878  D[2]=4ce928d3
A[3]=5feaffc1  B[3]=aa15a514  C[3]=ee589370  D[3]=b9d7fd5c

Step 17: (r=28, s= 7)
A[0]=be97ed59  B[0]=50577795  C[0]=a19abd2b  D[0]=535d3b5f
A[1]=7171c65a  B[1]=67b70828  C[1]=f4d140fa  D[1]=85b41f41
A[2]=7de769b9  B[2]=4c5b32a8  C[2]=804e7059  D[2]=56296878
A[3]=df26cb3b  B[3]=15feaffc  C[3]=aa15a514  D[3]=ee589370

Step 18: (r= 7, s=22)
A[0]=6dfcbc23  B[0]=4bf6acdf  C[0]=50577795  D[0]=a19abd2b
A[1]=85411ed4  B[1]=b8e32d38  C[1]=67b70828  D[1]=f4d140fa
A[2]=da7b4c48  B[2]=f3b4dcbe  C[2]=4c5b32a8  D[2]=804e7059
A[3]=f28995a5  B[3]=93659def  C[3]=15feaffc  D[3]=aa15a514

Step 19: (r=22, s=19)
A[0]=08c6eaef  B[0]=08db7f2f  C[0]=4bf6acdf  D[0]=50577795
A[1]=6c62c758  B[1]=b5215047  C[1]=b8e32d38  D[1]=67b70828
A[2]=6dd54637  B[2]=12369ed3  C[2]=f3b4dcbe  D[2]=4c5b32a8
A[3]=d826623f  B[3]=697ca265  C[3]=93659def  D[3]=15feaffc

Step 20: (r=19, s=28)
A[0]=c08e1946  B[0]=57784637  C[0]=08db7f2f  D[0]=4bf6acdf
A[1]=eaaf6ccf  B[1]=3ac36316  C[1]=b5215047  D[1]=b8e32d38
A[2]=84884bc0  B[2]=31bb6eaa  C[2]=12369ed3  D[2]=f3b4dcbe
A[3]=cb70c65b  B[3]=11fec133  C[3]=697ca265  D[3]=93659def

Step 21: (r=28, s= 7)
A[0]=ed4b0c05  B[0]=6c08e194  C[0]=57784637  D[0]=08db7f2f
A[1]=b5829699  B[1]=feaaf6cc  C[1]=3ac36316  D[1]=b5215047
A[2]=3c26098e  B[2]=084884bc  C[2]=31bb6eaa  D[2]=12369ed3
A[3]=a47af39a  B[3]=bcb70c65  C[3]=11fec133  D[3]=697ca265

Step 22: (r= 7, s=22)
A[0]=ea289e2f  B[0]=a58602f6  C[0]=6c08e194  D[0]=57784637
```

```
A[1]=7c0d0004  B[1]=c14b4cda  C[1]=feaaf6cc  D[1]=3ac36316
A[2]=a645dd03  B[2]=1304c71e  C[2]=084884bc  D[2]=31bb6eaa
A[3]=8dc89f93  B[3]=3d79cd52  C[3]=bcb70c65  D[3]=11fec133

Step 23: (r=22, s=19)
A[0]=a9548c84  B[0]=8bfa8a27  C[0]=a58602f6  D[0]=6c08e194
A[1]=5693f5fd  B[1]=011f0340  C[1]=c14b4cda  D[1]=feaaf6cc
A[2]=0422504a  B[2]=40e99177  C[2]=1304c71e  D[2]=084884bc
A[3]=693c8f1b  B[3]=e4e37227  C[3]=3d79cd52  D[3]=bcb70c65

Step 24: (r=15, s= 5)
A[0]=80719e5f  B[0]=464254aa  C[0]=8bfa8a27  D[0]=a58602f6
A[1]=c8429ea8  B[1]=fafeab49  C[1]=011f0340  D[1]=c14b4cda
A[2]=f699d10a  B[2]=28250211  C[2]=40e99177  D[2]=1304c71e
A[3]=0c162e46  B[3]=478db49e  C[3]=e4e37227  D[3]=3d79cd52

Step 25: (r= 5, s=29)
A[0]=a11db768  B[0]=0e33cbf0  C[0]=464254aa  D[0]=8bfa8a27
A[1]=8bf08d92  B[1]=0853d519  C[1]=fafeab49  D[1]=011f0340
A[2]=81e945c1  B[2]=d33a215e  C[2]=28250211  D[2]=40e99177
A[3]=2421837d  B[3]=82c5c8c1  C[3]=478db49e  D[3]=e4e37227

Step 26: (r=29, s= 9)
A[0]=796335f5  B[0]=1423b6ed  C[0]=0e33cbf0  D[0]=464254aa
A[1]=10bdcf53  B[1]=517e11b2  C[1]=0853d519  D[1]=fafeab49
A[2]=2a43930b  B[2]=303d28b8  C[2]=d33a215e  D[2]=28250211
A[3]=f4cde107  B[3]=a484306f  C[3]=82c5c8c1  D[3]=478db49e

Step 27: (r= 9, s=15)
A[0]=157d65a9  B[0]=c66beaf2  C[0]=1423b6ed  D[0]=0e33cbf0
A[1]=4f45083b  B[1]=7b9ea621  C[1]=517e11b2  D[1]=0853d519
A[2]=6accda72  B[2]=87261654  C[2]=303d28b8  D[2]=d33a215e
A[3]=9263461b  B[3]=9bc20fe9  C[3]=a484306f  D[3]=82c5c8c1

Step 28: (r=15, s= 5)
A[0]=28dc2d6c  B[0]=b2d48abe  C[0]=c66beaf2  D[0]=1423b6ed
A[1]=a5fbb5fe  B[1]=841da7a2  C[1]=7b9ea621  D[1]=517e11b2
A[2]=1a631714  B[2]=6d393566  C[2]=87261654  D[2]=303d28b8
A[3]=f97b813f  B[3]=a30dc931  C[3]=9bc20fe9  D[3]=a484306f

Step 29: (r= 5, s=29)
A[0]=3ae090ed  B[0]=1b85ad85  C[0]=b2d48abe  D[0]=c66beaf2
A[1]=875bfb06  B[1]=bf76bfd4  C[1]=841da7a2  D[1]=7b9ea621
A[2]=61601d95  B[2]=4c62e283  C[2]=6d393566  D[2]=87261654
A[3]=808d54a3  B[3]=2f7027ff  C[3]=a30dc931  D[3]=9bc20fe9

Step 30: (r=29, s= 9)
A[0]=851a1352  B[0]=a75c121d  C[0]=1b85ad85  D[0]=b2d48abe
A[1]=997145c5  B[1]=d0eb7f60  C[1]=bf76bfd4  D[1]=841da7a2
```

```
A[2]=7639e1a5  B[2]=ac2c03b2  C[2]=4c62e283  D[2]=6d393566
A[3]=65638648  B[3]=7011aa94  C[3]=2f7027ff  D[3]=a30dc931

Step 31: (r= 9, s=15)
A[0]=d17c0abc  B[0]=3426a50a  C[0]=a75c121d  D[0]=1b85ad85
A[1]=e98ef553  B[1]=e28b8b32  C[1]=d0eb7f60  D[1]=bf76bfd4
A[2]=b55845ff  B[2]=73c34aec  C[2]=ac2c03b2  D[2]=4c62e283
A[3]=9d9ea1bc  B[3]=c70c90ca  C[3]=7011aa94  D[3]=2f7027ff

Feed-Forward Step 0: (r=15, s= 5)
A[0]=eb3db3e4  B[0]=055e68be  C[0]=3426a50a  D[0]=a75c121d
A[1]=a9cf829a  B[1]=7aa9f4c7  C[1]=e28b8b32  D[1]=d0eb7f60
A[2]=38fecb28  B[2]=22ffdaac  C[2]=73c34aec  D[2]=ac2c03b2
A[3]=71cec3e8  B[3]=50de4ecf  C[3]=c70c90ca  D[3]=7011aa94

Feed-Forward Step 1: (r= 5, s=29)
A[0]=92b25efa  B[0]=67b67c9d  C[0]=055e68be  D[0]=3426a50a
A[1]=3b32a886  B[1]=39f05355  C[1]=7aa9f4c7  D[1]=e28b8b32
A[2]=56678dcf  B[2]=1fd96507  C[2]=22ffdaac  D[2]=73c34aec
A[3]=c81ff772  B[3]=39d87d0e  C[3]=50de4ecf  D[3]=c70c90ca

Feed-Forward Step 2: (r=29, s= 9)
A[0]=23fe6183  B[0]=52564bdf  C[0]=67b67c9d  D[0]=055e68be
A[1]=02caf986  B[1]=c7665510  C[1]=39f05355  D[1]=7aa9f4c7
A[2]=2e4ea350  B[2]=eaccf1b9  C[2]=1fd96507  D[2]=22ffdaac
A[3]=0b44a5be  B[3]=5903feee  C[3]=39d87d0e  D[3]=50de4ecf

Feed-Forward Step 3: (r= 9, s=15)
A[0]=0fff439e  B[0]=fcc30647  C[0]=52564bdf  D[0]=67b67c9d
A[1]=2731269b  B[1]=95f30c05  C[1]=c7665510  D[1]=39f05355
A[2]=3e61ea0d  B[2]=9d46a05c  C[2]=eaccf1b9  D[2]=1fd96507
A[3]=8a6b06d0  B[3]=894b7c16  C[3]=5903feee  D[3]=39d87d0e
```

Compression Function Output

```
A[0]=0fff439e  B[0]=fcc30647  C[0]=52564bdf  D[0]=67b67c9d
A[1]=2731269b  B[1]=95f30c05  C[1]=c7665510  D[1]=39f05355
A[2]=3e61ea0d  B[2]=9d46a05c  C[2]=eaccf1b9  D[2]=1fd96507
A[3]=8a6b06d0  B[3]=894b7c16  C[3]=5903feee  D[3]=39d87d0e
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff f0
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  195  145  230   47   52  203  238  249
y[  8.. 15] =   12   96  215  134  192  149   97   86
y[ 16.. 23] =  125   71  253   29   78  108  111   14
y[ 24.. 31] =   76   62  254  175   50   20  235   16
y[ 32.. 39] =  224   33  108  228   44  109  107   42
y[ 40.. 47] =  154  246  148  136  113  117   81  174
y[ 48.. 55] =   56  126  148   62  151   51  153  212
y[ 56.. 63] =   51  141  153   14    7  209  219   46
y[ 64.. 71] =   14   20   75  104   16  215  142  205
y[ 72.. 79] =  162   98  256  209  240   66   86   20
y[ 80.. 87] =  132   44   30    5   90   44  223  126
y[ 88.. 95] =  226  151   51  249  247   44  154   79
y[ 96..103] =   33  241  111  146   19  101   97  216
y[104..111] =   50  140   61  172   65  117   52  126
y[112..119] =  201  236  251   10   65  247  201  209
y[120..127] =   24   46  196   55  113   95   83  196
```

Intermediate Expanded Message

```
Z[ 0] = af10d332  21f7ec7d  d8fa2594  fa38f245
Z[ 1] = 456008ac  a71de1a6  b1f4d107  3e264619
Z[ 2] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
Z[ 3] = 2cce36ec  c4befdd5  0e742422  0b90f01a
Z[ 4] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
Z[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
Z[ 6] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
Z[ 7] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
Z[ 8] = 0e740a1e  4b283633  e1a60b90  da6cace5
Z[ 9] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
Z[10] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
Z[11] = b366e999  fa3824db  1fccf8c6  3917b591
Z[12] = f47017d9  afc95037  48fd0dbb  e25f4619
Z[13] = ab732422  c2932c15  548d2ef9  5b0e2594
Z[14] = f0d3d788  073afbaa  f8c62ef9  dd50d788
Z[15] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
Z[16] = 0c32c9fe  4155e87b  0df02d4c  9bd3ef73
Z[17] = ad3f0a74  ff21db6a  f131c761  4aea547f
Z[18] = 931d6ce3  1a22fc84  4e6643f2  e26260b1
Z[19] = e4ff4234  2c6dfd63  f74a2b8e  a647ecd6
Z[20] = 1cbfe341  60b15e14  108d2654  547f5d35
Z[21] = 2b8ea647  3523a10d  389f626f  2d4c468f
Z[22] = cf3830c8  fac6a10d  389fa3aa  cf38a568
Z[23] = 14e82c6d  cadda568  626f0619  484ddee6
Z[24] = 116c9e70  5a9828f1  db6ad0f6  d2b4f908
Z[25] = 555e53a0  d63094db  397ea1ec  116c4aea
Z[26] = 26543dd9  045b1943  26545e14  6dc20c32
Z[27] = a3aa3602  f908b892  2654116c  44d10df0
Z[28] = f2101cbf  9f4fe6bd  57fb5ef3  dc492496
```

```
Z[29] = 9a15f66b  b5f59699  65eb65eb  6dc2b7b3
Z[30] = edb56dc2  08b63602  f74a2c6d  d630d8cd
Z[31] = 28129af4  2fe90c32  52c1d630  cadd2812
```

Expanded Message

```
W[ 0] = 17d9e827  eb0b4e0c  4ec51fcc  1e5a4d53
W[ 1] = 5b0e2878  2cceb13b  24dbb366  df7bb4d8
W[ 2] = af10d332  21f7ec7d  d8fa2594  fa38f245
W[ 3] = 334f5a55  14f5fd1c  4e0c385e  0a1e5037
W[ 4] = ac2c24db  0a1eb4d8  dd50050f  213ee48a
W[ 5] = f80db591  a88fb13b  548d51a9  c4053a89
W[ 6] = 2cce36ec  c4befdd5  0e742422  0b90f01a
W[ 7] = 456008ac  a71de1a6  b1f4d107  3e264619
W[ 8] = 213e1158  27bfd3eb  44a751a9  d3eb3bfb
W[ 9] = b366e999  fa3824db  1fccf8c6  3917b591
W[10] = f47017d9  afc95037  48fd0dbb  e25f4619
W[11] = 0e740a1e  4b283633  e1a60b90  da6cace5
W[12] = 46d2bb59  dd50ff47  2fb2f3b7  0e743e26
W[13] = ab732422  c2932c15  548d2ef9  5b0e2594
W[14] = 1fcca5ab  039d15ae  1fcc410a  5b0ee76e
W[15] = f0d3d788  073afbaa  f8c62ef9  dd50d788
W[16] = ad3f0a74  ff21db6a  f131c761  4aea547f
W[17] = 931d6ce3  1a22fc84  4e6643f2  e26260b1
W[18] = 14e82c6d  cadda568  626f0619  484ddee6
W[19] = 1cbfe341  60b15e14  108d2654  547f5d35
W[20] = cf3830c8  fac6a10d  389fa3aa  cf38a568
W[21] = 2b8ea647  3523a10d  389f626f  2d4c468f
W[22] = 0c32c9fe  4155e87b  0df02d4c  9bd3ef73
W[23] = e4ff4234  2c6dfd63  f74a2b8e  a647ecd6
W[24] = edb56dc2  08b63602  f74a2c6d  d630d8cd
W[25] = 116c9e70  5a9828f1  db6ad0f6  d2b4f908
W[26] = 555e53a0  d63094db  397ea1ec  116c4aea
W[27] = 28129af4  2fe90c32  52c1d630  cadd2812
W[28] = a3aa3602  f908b892  2654116c  44d10df0
W[29] = 9a15f66b  b5f59699  65eb65eb  6dc2b7b3
W[30] = f2101cbf  9f4fe6bd  57fb5ef3  dc492496
W[31] = 26543dd9  045b1943  26545e14  6dc20c32
```

Feistel Steps

```
IV :
A[0]=0fff439e  B[0]=fcc30647  C[0]=52564bdf  D[0]=67b67c9d
A[1]=2731269b  B[1]=95f30c05  C[1]=c7665510  D[1]=39f05355
A[2]=3e61ea0d  B[2]=9d46a05c  C[2]=eaccf1b9  D[2]=1fd96507
A[3]=8a6b06d0  B[3]=894b7c16  C[3]=5903feee  D[3]=39d87d0e

IV XOR M :
A[0]=f000bc61  B[0]=033cf9b8  C[0]=52564bdf  D[0]=67b67c9d
A[1]=d8ced964  B[1]=650cf3fa  C[1]=c7665510  D[1]=39f05355
```

```
A[2]=c19e15f2  B[2]=9d46a05c  C[2]=eaccf1b9  D[2]=1fd96507
A[3]=7594f92f  B[3]=894b7c16  C[3]=5903feee  D[3]=39d87d0e

Step  0: (r= 3, s=20)
A[0]=ce9ee99c  B[0]=8005e30f  C[0]=033cf9b8  D[0]=52564bdf
A[1]=7a07721d  B[1]=c676cb26  C[1]=650cf3fa  D[1]=c7665510
A[2]=ff6967d1  B[2]=0cf0af96  C[2]=9d46a05c  D[2]=eaccf1b9
A[3]=127bf673  B[3]=aca7c97b  C[3]=894b7c16  D[3]=5903feee

Step  1: (r=20, s=14)
A[0]=d680c238  B[0]=99cce9ee  C[0]=8005e30f  D[0]=033cf9b8
A[1]=59bd768f  B[1]=21d7a077  C[1]=c676cb26  D[1]=650cf3fa
A[2]=6cfbb0f1  B[2]=7d1ff696  C[2]=0cf0af96  D[2]=9d46a05c
A[3]=00e710df  B[3]=673127bf  C[3]=aca7c97b  D[3]=894b7c16

Step  2: (r=14, s=27)
A[0]=27ba73df  B[0]=308e35a0  C[0]=99cce9ee  D[0]=8005e30f
A[1]=dcb33f8a  B[1]=5da3d66f  C[1]=21d7a077  D[1]=c676cb26
A[2]=fb4aa465  B[2]=ec3c5b3e  C[2]=7d1ff696  D[2]=0cf0af96
A[3]=020b6760  B[3]=c437c039  C[3]=673127bf  D[3]=aca7c97b

Step  3: (r=27, s= 3)
A[0]=90fa0d46  B[0]=f93dd39e  C[0]=308e35a0  D[0]=99cce9ee
A[1]=cab35145  B[1]=56e599fc  C[1]=5da3d66f  D[1]=21d7a077
A[2]=320fa8f0  B[2]=2fda5523  C[2]=ec3c5b3e  D[2]=7d1ff696
A[3]=36b06d84  B[3]=00105b3b  C[3]=c437c039  D[3]=673127bf

Step  4: (r= 3, s=20)
A[0]=9a99f5a0  B[0]=87d06a34  C[0]=f93dd39e  D[0]=308e35a0
A[1]=fc45f123  B[1]=559a8a2e  C[1]=56e599fc  D[1]=5da3d66f
A[2]=02fbf506  B[2]=907d4781  C[2]=2fda5523  D[2]=ec3c5b3e
A[3]=dff93439  B[3]=b5836c21  C[3]=00105b3b  D[3]=c437c039

Step  5: (r=20, s=14)
A[0]=c819a0cc  B[0]=5a09a99f  C[0]=87d06a34  D[0]=f93dd39e
A[1]=8bd41651  B[1]=123fc45f  C[1]=559a8a2e  D[1]=56e599fc
A[2]=9a843a90  B[2]=50602fbf  C[2]=907d4781  D[2]=2fda5523
A[3]=affe8bd2  B[3]=439dff93  C[3]=b5836c21  D[3]=00105b3b

Step  6: (r=14, s=27)
A[0]=3d15908e  B[0]=68333206  C[0]=5a09a99f  D[0]=87d06a34
A[1]=901e3f92  B[1]=059462f5  C[1]=123fc45f  D[1]=559a8a2e
A[2]=596a4145  B[2]=0ea426a1  C[2]=50602fbf  D[2]=907d4781
A[3]=adcd3bdd  B[3]=a2f4abff  C[3]=439dff93  D[3]=b5836c21

Step  7: (r=27, s= 3)
A[0]=54dc6d7c  B[0]=71e8ac84  C[0]=68333206  D[0]=5a09a99f
A[1]=5424ff36  B[1]=9480f1fc  C[1]=059462f5  D[1]=123fc45f
A[2]=487aadf0  B[2]=2acb520a  C[2]=0ea426a1  D[2]=50602fbf
```

```
A[3]=50bc62c8  B[3]=ed6e69de  C[3]=a2f4abff  D[3]=439dff93

Step  8: (r=26, s= 4)
A[0]=1c8023db  B[0]=f15371b5  C[0]=71e8ac84  D[0]=68333206
A[1]=ba2a8eab  B[1]=d95093fc  C[1]=9480f1fc  D[1]=059462f5
A[2]=5e9b2825  B[2]=c121eab7  C[2]=2acb520a  D[2]=0ea426a1
A[3]=90b5ca94  B[3]=2142f18b  C[3]=ed6e69de  D[3]=a2f4abff

Step  9: (r= 4, s=23)
A[0]=83f903b9  B[0]=c8023db1  C[0]=f15371b5  D[0]=71e8ac84
A[1]=f1aad006  B[1]=a2a8eabb  C[1]=d95093fc  D[1]=9480f1fc
A[2]=934996fd  B[2]=e9b28255  C[2]=c121eab7  D[2]=2acb520a
A[3]=4fcd965c  B[3]=0b5ca949  C[3]=2142f18b  D[3]=ed6e69de

Step 10: (r=23, s=11)
A[0]=dd29681a  B[0]=dcc1fc81  C[0]=c8023db1  D[0]=f15371b5
A[1]=96fb1435  B[1]=0378d568  C[1]=a2a8eabb  D[1]=d95093fc
A[2]=7878c872  B[2]=7ec9a4cb  C[2]=e9b28255  D[2]=c121eab7
A[3]=c1501459  B[3]=2e27e6cb  C[3]=0b5ca949  D[3]=2142f18b

Step 11: (r=11, s=26)
A[0]=99b2bfa8  B[0]=4b40d6e9  C[0]=dcc1fc81  D[0]=c8023db1
A[1]=e5be952d  B[1]=d8a1acb7  C[1]=0378d568  D[1]=a2a8eabb
A[2]=85b320cb  B[2]=c64393c3  C[2]=7ec9a4cb  D[2]=e9b28255
A[3]=bcb89de5  B[3]=80a2ce0a  C[3]=2e27e6cb  D[3]=0b5ca949

Step 12: (r=26, s= 4)
A[0]=40f67592  B[0]=a266cafe  C[0]=4b40d6e9  D[0]=dcc1fc81
A[1]=493ebf77  B[1]=b796fa54  C[1]=d8a1acb7  D[1]=0378d568
A[2]=99844ff5  B[2]=2e16cc83  C[2]=c64393c3  D[2]=7ec9a4cb
A[3]=09a22eaa  B[3]=96f2e277  C[3]=80a2ce0a  D[3]=2e27e6cb

Step 13: (r= 4, s=23)
A[0]=672a4d54  B[0]=0f675924  C[0]=a266cafe  D[0]=4b40d6e9
A[1]=9472cbff  B[1]=93ebf774  C[1]=b796fa54  D[1]=d8a1acb7
A[2]=d31807f5  B[2]=9844ff59  C[2]=2e16cc83  D[2]=c64393c3
A[3]=d870e3f1  B[3]=9a22eaa0  C[3]=96f2e277  D[3]=80a2ce0a

Step 14: (r=23, s=11)
A[0]=9dfa7df8  B[0]=aa339526  C[0]=0f675924  D[0]=a266cafe
A[1]=88d857a4  B[1]=ffca3965  C[1]=93ebf774  D[1]=b796fa54
A[2]=1e112c72  B[2]=fae98c03  C[2]=9844ff59  D[2]=2e16cc83
A[3]=cef6e0d7  B[3]=f8ec3871  C[3]=9a22eaa0  D[3]=96f2e277

Step 15: (r=11, s=26)
A[0]=31ee48ee  B[0]=d3efc4ef  C[0]=aa339526  D[0]=0f675924
A[1]=4071302c  B[1]=c2bd2446  C[1]=ffca3965  D[1]=93ebf774
A[2]=12f43f8e  B[2]=896390f0  C[2]=fae98c03  D[2]=9844ff59
A[3]=83f9ced1  B[3]=b706be77  C[3]=f8ec3871  D[3]=9a22eaa0
```

```
Step 16: (r=19, s=28)
A[0]=e6ec6721  B[0]=47718f72  C[0]=d3efc4ef  D[0]=aa339526
A[1]=359d2763  B[1]=81620389  C[1]=c2bd2446  D[1]=ffca3965
A[2]=2daa2541  B[2]=fc7097a1  C[2]=896390f0  D[2]=fae98c03
A[3]=5572af4b  B[3]=768c1fce  C[3]=b706be77  D[3]=f8ec3871

Step 17: (r=28, s= 7)
A[0]=6d1f9e1e  B[0]=1e6ec672  C[0]=47718f72  D[0]=d3efc4ef
A[1]=3bf3a262  B[1]=3359d276  C[1]=81620389  D[1]=c2bd2446
A[2]=f72199ec  B[2]=12daa254  C[2]=fc7097a1  D[2]=896390f0
A[3]=dcb622de  B[3]=b5572af4  C[3]=768c1fce  D[3]=b706be77

Step 18: (r= 7, s=22)
A[0]=2d8f02bb  B[0]=8fcf0f36  C[0]=1e6ec672  D[0]=47718f72
A[1]=f71d318e  B[1]=f9d1311d  C[1]=3359d276  D[1]=81620389
A[2]=ae92f835  B[2]=90ccf67b  C[2]=12daa254  D[2]=fc7097a1
A[3]=dc3c6bed  B[3]=5b116f6e  C[3]=b5572af4  D[3]=768c1fce

Step 19: (r=22, s=19)
A[0]=d697c5c7  B[0]=aecb63c0  C[0]=8fcf0f36  D[0]=1e6ec672
A[1]=a445aa44  B[1]=63bdc74c  C[1]=f9d1311d  D[1]=3359d276
A[2]=320051f5  B[2]=0d6ba4be  C[2]=90ccf67b  D[2]=12daa254
A[3]=a7b7ea43  B[3]=fb770f1a  C[3]=5b116f6e  D[3]=b5572af4

Step 20: (r=19, s=28)
A[0]=59ec861d  B[0]=2e3eb4be  C[0]=aecb63c0  D[0]=8fcf0f36
A[1]=80a8f16e  B[1]=5225222d  C[1]=63bdc74c  D[1]=f9d1311d
A[2]=27d9716e  B[2]=8fa99002  C[2]=0d6ba4be  D[2]=90ccf67b
A[3]=963b28b8  B[3]=521d3dbf  C[3]=fb770f1a  D[3]=5b116f6e

Step 21: (r=28, s= 7)
A[0]=08aba40b  B[0]=d59ec861  C[0]=2e3eb4be  D[0]=aecb63c0
A[1]=5abe7dc3  B[1]=e80a8f16  C[1]=5225222d  D[1]=63bdc74c
A[2]=80a354cd  B[2]=e27d9716  C[2]=8fa99002  D[2]=0d6ba4be
A[3]=367c6ac3  B[3]=8963b28b  C[3]=521d3dbf  D[3]=fb770f1a

Step 22: (r= 7, s=22)
A[0]=d9b0d0e1  B[0]=55d20584  C[0]=d59ec861  D[0]=2e3eb4be
A[1]=056a3737  B[1]=5f3ee1ad  C[1]=e80a8f16  D[1]=5225222d
A[2]=c25ce2f4  B[2]=51aa66c0  C[2]=e27d9716  D[2]=8fa99002
A[3]=9bfc7792  B[3]=3e35619b  C[3]=8963b28b  D[3]=521d3dbf

Step 23: (r=22, s=19)
A[0]=7bcfddbd  B[0]=38766c34  C[0]=55d20584  D[0]=d59ec861
A[1]=1ae55d0b  B[1]=cdc15a8d  C[1]=5f3ee1ad  D[1]=e80a8f16
A[2]=4b98b7b9  B[2]=bd309738  C[2]=51aa66c0  D[2]=e27d9716
A[3]=bf45f961  B[3]=e4a6ff1d  C[3]=3e35619b  D[3]=8963b28b
```

```
Step 24: (r=15, s= 5)
A[0]=a3d5d871  B[0]=eedebde7  C[0]=38766c34  D[0]=55d20584
A[1]=2f745e73  B[1]=ae858d72  C[1]=cdc15a8d  D[1]=5f3ee1ad
A[2]=5c043f20  B[2]=5bdca5cc  C[2]=bd309738  D[2]=51aa66c0
A[3]=680f5c47  B[3]=fcb0dfa2  C[3]=e4a6ff1d  D[3]=3e35619b

Step 25: (r= 5, s=29)
A[0]=a4ce9016  B[0]=7abb0e34  C[0]=eedebde7  D[0]=38766c34
A[1]=96f70be0  B[1]=ee8bce65  C[1]=ae858d72  D[1]=cdc15a8d
A[2]=3f8449cd  B[2]=8087e40b  C[2]=5bdca5cc  D[2]=bd309738
A[3]=ae3d399c  B[3]=01eb88ed  C[3]=fcb0dfa2  D[3]=e4a6ff1d

Step 26: (r=29, s= 9)
A[0]=f0ba756c  B[0]=d499d202  C[0]=7abb0e34  D[0]=eedebde7
A[1]=92ec3ddd  B[1]=12dee17c  C[1]=ee8bce65  D[1]=ae858d72
A[2]=ae0201a2  B[2]=a7f08939  C[2]=8087e40b  D[2]=5bdca5cc
A[3]=4ecb3c8f  B[3]=95c7a733  C[3]=01eb88ed  D[3]=fcb0dfa2

Step 27: (r= 9, s=15)
A[0]=5d793e21  B[0]=74ead9e1  C[0]=d499d202  D[0]=7abb0e34
A[1]=d5094d3c  B[1]=d87bbb25  C[1]=12dee17c  D[1]=ee8bce65
A[2]=a57d8473  B[2]=0403455c  C[2]=a7f08939  D[2]=8087e40b
A[3]=ae87a1dd  B[3]=96791e9d  C[3]=95c7a733  D[3]=01eb88ed

Step 28: (r=15, s= 5)
A[0]=12823572  B[0]=9f10aebc  C[0]=74ead9e1  D[0]=d499d202
A[1]=c047d934  B[1]=a69e6a84  C[1]=d87bbb25  D[1]=12dee17c
A[2]=5a9e354c  B[2]=c239d2be  C[2]=0403455c  D[2]=a7f08939
A[3]=4f987e17  B[3]=d0eed743  C[3]=96791e9d  D[3]=95c7a733

Step 29: (r= 5, s=29)
A[0]=046cfa56  B[0]=5046ae42  C[0]=9f10aebc  D[0]=74ead9e1
A[1]=24365150  B[1]=08fb2698  C[1]=a69e6a84  D[1]=d87bbb25
A[2]=5a4596d2  B[2]=53c6a98b  C[2]=c239d2be  D[2]=0403455c
A[3]=c44b7e37  B[3]=f30fc2e9  C[3]=d0eed743  D[3]=96791e9d

Step 30: (r=29, s= 9)
A[0]=83d0b720  B[0]=c08d9f4a  C[0]=5046ae42  D[0]=9f10aebc
A[1]=5f519813  B[1]=0486ca2a  C[1]=08fb2698  D[1]=a69e6a84
A[2]=80f74322  B[2]=4b48b2da  C[2]=53c6a98b  D[2]=c239d2be
A[3]=e4c0cbd0  B[3]=f8896fc6  C[3]=f30fc2e9  D[3]=d0eed743

Step 31: (r= 9, s=15)
A[0]=c4720815  B[0]=a16e4107  C[0]=c08d9f4a  D[0]=5046ae42
A[1]=08887daf  B[1]=a33026be  C[1]=0486ca2a  D[1]=08fb2698
A[2]=0b9c5731  B[2]=ee864501  C[2]=4b48b2da  D[2]=53c6a98b
A[3]=facabe5b  B[3]=8197a1c9  C[3]=f8896fc6  D[3]=f30fc2e9

Feed-Forward Step 0: (r=15, s= 5)
```

```
A[0]=6588aa40  B[0]=040ae239  C[0]=a16e4107  D[0]=c08d9f4a
A[1]=b1f701f4  B[1]=3ed78444  C[1]=a33026be  D[1]=0486ca2a
A[2]=fcdd29e0  B[2]=2b9885ce  C[2]=ee864501  D[2]=4b48b2da
A[3]=c3e05318  B[3]=5f2dfd65  C[3]=8197a1c9  D[3]=f8896fc6

Feed-Forward Step 1: (r= 5, s=29)
A[0]=a3dd2d32  B[0]=b115480c  C[0]=040ae239  D[0]=a16e4107
A[1]=35b482a7  B[1]=3ee03e96  C[1]=3ed78444  D[1]=a33026be
A[2]=937a7b2a  B[2]=9ba53c1f  C[2]=2b9885ce  D[2]=ee864501
A[3]=f781da49  B[3]=7c0a6318  C[3]=5f2dfd65  D[3]=8197a1c9

Feed-Forward Step 2: (r=29, s= 9)
A[0]=9f646f85  B[0]=547ba5a6  C[0]=b115480c  D[0]=040ae239
A[1]=457478b7  B[1]=e6b69054  C[1]=3ee03e96  D[1]=3ed78444
A[2]=26d74c72  B[2]=526f4f65  C[2]=9ba53c1f  D[2]=2b9885ce
A[3]=e48b6c53  B[3]=3ef03b49  C[3]=7c0a6318  D[3]=5f2dfd65

Feed-Forward Step 3: (r= 9, s=15)
A[0]=f0ca3466  B[0]=c8df0b3e  C[0]=547ba5a6  D[0]=b115480c
A[1]=0dafa386  B[1]=e8f16e8a  C[1]=e6b69054  D[1]=3ee03e96
A[2]=7c807eaa  B[2]=ae98e44d  C[2]=526f4f65  D[2]=9ba53c1f
A[3]=3bcfd94d  B[3]=16d8a7c9  C[3]=3ef03b49  D[3]=7c0a6318
```

Compression Function Output

```
A[0]=f0ca3466  B[0]=c8df0b3e  C[0]=547ba5a6  D[0]=b115480c
A[1]=0dafa386  B[1]=e8f16e8a  C[1]=e6b69054  D[1]=3ee03e96
A[2]=7c807eaa  B[2]=ae98e44d  C[2]=526f4f65  D[2]=9ba53c1f
A[3]=3bcfd94d  B[3]=16d8a7c9  C[3]=3ef03b49  D[3]=7c0a6318
```

Final block

```
M[  0..  7] = bc 02 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  192  108  141  233   96  118  165  228
y[  8.. 15] =   32  222   69   67  220  239   71  167
y[ 16.. 23] =  128  193   38  144  230  170  141   22
y[ 24.. 31] =   43   18   57  253   52   49  135   90
y[ 32.. 39] =  220  141  251   80   69   78  112  146
y[ 40.. 47] =  246  192  105  151  220  224    4   25
y[ 48.. 55] =  248  255  112   48  106   24   23   60
```

```
y[ 56.. 63] =  177  160   25  225  205   82   19  141
y[ 64.. 71] =  184   11  235  143   23    1  211  148
y[ 72.. 79] =   87  154   50   52  156  137   48  209
y[ 80.. 87] =  248  183   81  232  146  206  235   97
y[ 88.. 95] =   76  101   62  123   67   70  241   29
y[ 96..103] =  156  235  125   39   50   41    7  230
y[104..111] =  130  184   14  225  156  152  115   94
y[112..119] =  128  121    7   71   13   95   96   59
y[120..127] =  199  216   94  151  171   37  100  235
```

Intermediate Expanded Message

```
Z[ 0] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
Z[ 1] = e6b51720  306b31dd  f2fee543  bef6334f
Z[ 2] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
Z[ 3] = 0d021f13  fd1c2931  23692594  410aa7d6
Z[ 4] = ac2ce543  39d0fbaa  385e31dd  afc950f0
Z[ 5] = d107f80d  b3664be1  e827e543  121102e4
Z[ 6] = fe8ef97f  22b050f0  11584c9a  2b5c109f
Z[ 7] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
Z[ 8] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
Z[ 9] = b5913edf  25942422  a948b703  dd5022b0
Z[10] = ca86f97f  edef3a89  db25afc9  4619f01a
Z[11] = 48fd36ec  58e32cce  3296306b  14f5f470
Z[12] = f01ab703  1c2f5a55  1da12422  ec7d050f
Z[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
Z[14] = 57715c80  334f050f  44a70965  2aa34560
Z[15] = e25fd616  b36643ee  1abdc1da  f01a4844
Z[16] = c069c761  ecd69af4  140953a0  d7eeafdc
Z[17] = 4bc91be0  2b8e3c1b  a805dfc5  29d03dd9
Z[18] = f8296f80  468f211a  9f4fe87b  ecd69af4
Z[19] = 42342575  360231a7  3a5d2d4c  f21095ba
Z[20] = a805dfc5  6ce3fac6  2b8e3c1b  06196190
Z[21] = 915ff66b  0c325b77  a805dfc5  642d037c
Z[22] = 6f80f829  06196190  0b535c56  53a01409
Z[23] = cd7aba50  51e215c7  b516d2b4  571c108d
Z[24] = 09955e14  9cb2eb18  00df66ca  a10de6bd
Z[25] = a647e183  2d4c3a5d  9778f052  d630b19a
Z[26] = bf8ac840  ea399d91  d393b437  547f132a
Z[27] = 57fb0fae  6b25fc84  3cfa2aaf  19434e66
Z[28] = ecd69af4  21f945b0  23b743f2  e87b9f4f
Z[29] = c069c761  e420a3aa  a489e341  51e215c7
Z[30] = 6967fe42  3dd929d0  52c114e8  33653444
Z[31] = dc49ab81  a3aae420  203b476e  ecd69af4
```

Expanded Message

```
W[ 0] = ac2ce543  39d0fbaa  385e31dd  afc950f0
W[ 1] = fe8ef97f  22b050f0  11584c9a  2b5c109f
W[ 2] = 4e0cd107  eea8ac2c  55464560  eb0bbd84
```

```
W[ 3] = d1c05c80  ae571b76  c121ec7d  0fe6ac2c
W[ 4] = b9e7c630  e8e01211  3b42da6c  ac2c0dbb
W[ 5] = d107f80d  b3664be1  e827e543  121102e4
W[ 6] = 0d021f13  fd1c2931  23692594  410aa7d6
W[ 7] = e6b51720  306b31dd  f2fee543  bef6334f
W[ 8] = e25fd616  b36643ee  1abdc1da  f01a4844
W[ 9] = 48fd36ec  58e32cce  3296306b  14f5f470
W[10] = f01ab703  1c2f5a55  1da12422  ec7d050f
W[11] = 07f3cb3f  ad9ef01a  00b9109f  b13bdec2
W[12] = b5913edf  25942422  a948b703  dd5022b0
W[13] = cb3fa439  e8e00a1e  b41fb703  43ee531b
W[14] = ca86f97f  edef3a89  db25afc9  4619f01a
W[15] = 57715c80  334f050f  44a70965  2aa34560
W[16] = 4bc91be0  2b8e3c1b  a805dfc5  29d03dd9
W[17] = f8296f80  468f211a  9f4fe87b  ecd69af4
W[18] = cd7aba50  51e215c7  b516d2b4  571c108d
W[19] = a805dfc5  6ce3fac6  2b8e3c1b  06196190
W[20] = 6f80f829  06196190  0b535c56  53a01409
W[21] = 915ff66b  0c325b77  a805dfc5  642d037c
W[22] = c069c761  ecd69af4  140953a0  d7eeafdc
W[23] = 42342575  360231a7  3a5d2d4c  f21095ba
W[24] = 6967fe42  3dd929d0  52c114e8  33653444
W[25] = 09955e14  9cb2eb18  00df66ca  a10de6bd
W[26] = a647e183  2d4c3a5d  9778f052  d630b19a
W[27] = dc49ab81  a3aae420  203b476e  ecd69af4
W[28] = 57fb0fae  6b25fc84  3cfa2aaf  19434e66
W[29] = c069c761  e420a3aa  a489e341  51e215c7
W[30] = ecd69af4  21f945b0  23b743f2  e87b9f4f
W[31] = bf8ac840  ea399d91  d393b437  547f132a
```

Feistel Steps

```
IV :
A[0]=f0ca3466  B[0]=c8df0b3e  C[0]=547ba5a6  D[0]=b115480c
A[1]=0dafa386  B[1]=e8f16e8a  C[1]=e6b69054  D[1]=3ee03e96
A[2]=7c807eaa  B[2]=ae98e44d  C[2]=526f4f65  D[2]=9ba53c1f
A[3]=3bcfd94d  B[3]=16d8a7c9  C[3]=3ef03b49  D[3]=7c0a6318

IV XOR M :
A[0]=f0ca36da  B[0]=c8df0b3e  C[0]=547ba5a6  D[0]=b115480c
A[1]=0dafa386  B[1]=e8f16e8a  C[1]=e6b69054  D[1]=3ee03e96
A[2]=7c807eaa  B[2]=ae98e44d  C[2]=526f4f65  D[2]=9ba53c1f
A[3]=3bcfd94d  B[3]=16d8a7c9  C[3]=3ef03b49  D[3]=7c0a6318

Step  0: (r= 3, s=20)
A[0]=764f400b  B[0]=8651b6d7  C[0]=c8df0b3e  D[0]=547ba5a6
A[1]=b52a2b79  B[1]=6d7d1c30  C[1]=e8f16e8a  D[1]=e6b69054
A[2]=130ef996  B[2]=e403f553  C[2]=ae98e44d  D[2]=526f4f65
A[3]=fb65e39c  B[3]=de7eca69  C[3]=16d8a7c9  D[3]=3ef03b49
```

```
Step  1: (r=20, s=14)
A[0]=83f86965  B[0]=00b764f4  C[0]=8651b6d7  D[0]=c8df0b3e
A[1]=454d5436  B[1]=b79b52a2  C[1]=6d7d1c30  D[1]=e8f16e8a
A[2]=a50de90a  B[2]=996130ef  C[2]=e403f553  D[2]=ae98e44d
A[3]=fc27a4f4  B[3]=39cfb65e  C[3]=de7eca69  D[3]=16d8a7c9

Step  2: (r=14, s=27)
A[0]=2dea7fec  B[0]=1a5960fe  C[0]=00b764f4  D[0]=8651b6d7
A[1]=3a6944d9  B[1]=550d9153  C[1]=b79b52a2  D[1]=6d7d1c30
A[2]=2f6451f9  B[2]=7a42a943  C[2]=996130ef  D[2]=e403f553
A[3]=6c3b839b  B[3]=e93d3f09  C[3]=39cfb65e  D[3]=de7eca69

Step  3: (r=27, s= 3)
A[0]=ccf6c52a  B[0]=616f53ff  C[0]=1a5960fe  D[0]=00b764f4
A[1]=66dc2ce9  B[1]=c9d34a26  C[1]=550d9153  D[1]=b79b52a2
A[2]=5ca76cb9  B[2]=c97b228f  C[2]=7a42a943  D[2]=996130ef
A[3]=0ce8b939  B[3]=db61dc1c  C[3]=e93d3f09  D[3]=39cfb65e

Step  4: (r= 3, s=20)
A[0]=09019931  B[0]=67b62956  C[0]=616f53ff  D[0]=1a5960fe
A[1]=b6a9cb50  B[1]=36e1674b  C[1]=c9d34a26  D[1]=550d9153
A[2]=a5a89a3b  B[2]=e53b65ca  C[2]=c97b228f  D[2]=7a42a943
A[3]=7ae11fae  B[3]=6745c9c8  C[3]=db61dc1c  D[3]=e93d3f09

Step  5: (r=20, s=14)
A[0]=c05aedab  B[0]=93109019  C[0]=67b62956  D[0]=616f53ff
A[1]=45055de6  B[1]=b50b6a9c  C[1]=36e1674b  D[1]=c9d34a26
A[2]=ff54e202  B[2]=a3ba5a89  C[2]=e53b65ca  D[2]=c97b228f
A[3]=bce9c848  B[3]=fae7ae11  C[3]=6745c9c8  D[3]=db61dc1c

Step  6: (r=14, s=27)
A[0]=c105b222  B[0]=bb6af016  C[0]=93109019  D[0]=67b62956
A[1]=686046ee  B[1]=57799141  C[1]=b50b6a9c  D[1]=36e1674b
A[2]=e0b3248f  B[2]=3880bfd5  C[2]=a3ba5a89  D[2]=e53b65ca
A[3]=8c458277  B[3]=72122f3a  C[3]=fae7ae11  D[3]=6745c9c8

Step  7: (r=27, s= 3)
A[0]=8a651d6b  B[0]=16082d91  C[0]=bb6af016  D[0]=93109019
A[1]=a2110bb9  B[1]=73430237  C[1]=57799141  D[1]=b50b6a9c
A[2]=dd6c7a64  B[2]=7f059924  C[2]=3880bfd5  D[2]=a3ba5a89
A[3]=77605c88  B[3]=bc622c13  C[3]=72122f3a  D[3]=fae7ae11

Step  8: (r=26, s= 4)
A[0]=6e3d7878  B[0]=ae299475  C[0]=16082d91  D[0]=bb6af016
A[1]=9129c1a6  B[1]=e688442e  C[1]=73430237  D[1]=57799141
A[2]=e1a922f5  B[2]=9375b1e9  C[2]=7f059924  D[2]=3880bfd5
A[3]=a56bece6  B[3]=21dd8172  C[3]=bc622c13  D[3]=72122f3a
```

```
Step  9: (r= 4, s=23)
A[0]=943377fc  B[0]=e3d78786  C[0]=ae299475  D[0]=16082d91
A[1]=7a0821ea  B[1]=129c1a69  C[1]=e688442e  D[1]=73430237
A[2]=f45ca5db  B[2]=1a922f5e  C[2]=9375b1e9  D[2]=7f059924
A[3]=217c433b  B[3]=56bece6a  C[3]=21dd8172  D[3]=bc622c13

Step 10: (r=23, s=11)
A[0]=e89dd191  B[0]=fe4a19bb  C[0]=e3d78786  D[0]=ae299475
A[1]=c301ef81  B[1]=f53d0410  C[1]=129c1a69  D[1]=e688442e
A[2]=5d26c39f  B[2]=edfa2e52  C[2]=1a922f5e  D[2]=9375b1e9
A[3]=e5e67f07  B[3]=9d90be21  C[3]=56bece6a  D[3]=21dd8172

Step 11: (r=11, s=26)
A[0]=64a298c6  B[0]=ee8c8f44  C[0]=fe4a19bb  D[0]=e3d78786
A[1]=f58f5051  B[1]=0f7c0e18  C[1]=f53d0410  D[1]=129c1a69
A[2]=5a1c1307  B[2]=361cfae9  C[2]=edfa2e52  D[2]=1a922f5e
A[3]=8526d692  B[3]=33f83f2f  C[3]=9d90be21  D[3]=56bece6a

Step 12: (r=26, s= 4)
A[0]=c70c3ff9  B[0]=19928a63  C[0]=ee8c8f44  D[0]=fe4a19bb
A[1]=f43c99fe  B[1]=47d63d41  C[1]=0f7c0e18  D[1]=f53d0410
A[2]=6986a59e  B[2]=1d68704c  C[2]=361cfae9  D[2]=edfa2e52
A[3]=b58d7e3f  B[3]=4a149b5a  C[3]=33f83f2f  D[3]=9d90be21

Step 13: (r= 4, s=23)
A[0]=4336e50c  B[0]=70c3ff9c  C[0]=19928a63  D[0]=ee8c8f44
A[1]=1beab090  B[1]=43c99fef  C[1]=47d63d41  D[1]=0f7c0e18
A[2]=81b39307  B[2]=986a59e6  C[2]=1d68704c  D[2]=361cfae9
A[3]=81542d97  B[3]=58d7e3fb  C[3]=4a149b5a  D[3]=33f83f2f

Step 14: (r=23, s=11)
A[0]=7bcc6dad  B[0]=86219b72  C[0]=70c3ff9c  D[0]=19928a63
A[1]=33f3ebd2  B[1]=480df558  C[1]=43c99fef  D[1]=47d63d41
A[2]=33a06f6b  B[2]=83c0d9c9  C[2]=986a59e6  D[2]=1d68704c
A[3]=bcfac185  B[3]=cbc0aa16  C[3]=58d7e3fb  D[3]=4a149b5a

Step 15: (r=11, s=26)
A[0]=830a7137  B[0]=636d6bde  C[0]=86219b72  D[0]=70c3ff9c
A[1]=8107eaef  B[1]=9f5e919f  C[1]=480df558  D[1]=43c99fef
A[2]=d7452b2c  B[2]=037b599d  C[2]=83c0d9c9  D[2]=986a59e6
A[3]=e494bcb0  B[3]=d60c2de7  C[3]=cbc0aa16  D[3]=58d7e3fb

Step 16: (r=19, s=28)
A[0]=83b778ac  B[0]=89bc1853  C[0]=636d6bde  D[0]=86219b72
A[1]=eced2143  B[1]=577c083f  C[1]=9f5e919f  D[1]=480df558
A[2]=69ca45dc  B[2]=5966ba29  C[2]=037b599d  D[2]=83c0d9c9
A[3]=2edadd5a  B[3]=e58724a5  C[3]=d60c2de7  D[3]=cbc0aa16

Step 17: (r=28, s= 7)
```

```
A[0]=ea2fc68d  B[0]=c83b778a  C[0]=89bc1853  D[0]=636d6bde
A[1]=b0c136c8  B[1]=3eced214  C[1]=577c083f  D[1]=9f5e919f
A[2]=0a289e41  B[2]=c69ca45d  C[2]=5966ba29  D[2]=037b599d
A[3]=cd83a9ea  B[3]=a2edadd5  C[3]=e58724a5  D[3]=d60c2de7

Step 18: (r= 7, s=22)
A[0]=a2da0d39  B[0]=17e346f5  C[0]=c83b778a  D[0]=89bc1853
A[1]=7ba96fb5  B[1]=609b6458  C[1]=3eced214  D[1]=577c083f
A[2]=f057ed9a  B[2]=144f2085  C[2]=c69ca45d  D[2]=5966ba29
A[3]=2656b270  B[3]=c1d4f566  C[3]=a2edadd5  D[3]=e58724a5

Step 19: (r=22, s=19)
A[0]=dd17fb26  B[0]=4e68b683  C[0]=17e346f5  D[0]=c83b778a
A[1]=54b2df2b  B[1]=ed5eea5b  C[1]=609b6458  D[1]=3eced214
A[2]=06b594a3  B[2]=66bc15fb  C[2]=144f2085  D[2]=c69ca45d
A[3]=0e324f4d  B[3]=9c0995ac  C[3]=c1d4f566  D[3]=a2edadd5

Step 20: (r=19, s=28)
A[0]=a2ccabfb  B[0]=d936e8bf  C[0]=4e68b683  D[0]=17e346f5
A[1]=9fb067cb  B[1]=f95aa596  C[1]=ed5eea5b  D[1]=609b6458
A[2]=e7f342e7  B[2]=a51835ac  C[2]=66bc15fb  D[2]=144f2085
A[3]=8160d233  B[3]=7a687192  C[3]=9c0995ac  D[3]=c1d4f566

Step 21: (r=28, s= 7)
A[0]=567341e7  B[0]=ba2ccabf  C[0]=d936e8bf  D[0]=4e68b683
A[1]=4c69e258  B[1]=b9fb067c  C[1]=f95aa596  D[1]=ed5eea5b
A[2]=c0b7e791  B[2]=7e7f342e  C[2]=a51835ac  D[2]=66bc15fb
A[3]=ef6050db  B[3]=38160d23  C[3]=7a687192  D[3]=9c0995ac

Step 22: (r= 7, s=22)
A[0]=ddeb6e77  B[0]=39a0f3ab  C[0]=ba2ccabf  D[0]=d936e8bf
A[1]=46e8b52a  B[1]=34f12c26  C[1]=b9fb067c  D[1]=f95aa596
A[2]=82002f1e  B[2]=5bf3c8e0  C[2]=7e7f342e  D[2]=a51835ac
A[3]=009c89d0  B[3]=b0286df7  C[3]=38160d23  D[3]=7a687192

Step 23: (r=22, s=19)
A[0]=8f3f28aa  B[0]=9df77adb  C[0]=39a0f3ab  D[0]=ba2ccabf
A[1]=4f5b49d1  B[1]=4a91ba2d  C[1]=34f12c26  D[1]=b9fb067c
A[2]=17294a1f  B[2]=c7a0800b  C[2]=5bf3c8e0  D[2]=7e7f342e
A[3]=f48e9ed5  B[3]=74002722  C[3]=b0286df7  D[3]=38160d23

Step 24: (r=15, s= 5)
A[0]=ce813949  B[0]=9455479f  C[0]=9df77adb  D[0]=39a0f3ab
A[1]=f5bb1a02  B[1]=a4e8a7ad  C[1]=4a91ba2d  D[1]=34f12c26
A[2]=75c43a6b  B[2]=a50f8b94  C[2]=c7a0800b  D[2]=5bf3c8e0
A[3]=87ca58da  B[3]=4f6afa47  C[3]=74002722  D[3]=b0286df7

Step 25: (r= 5, s=29)
A[0]=139d0019  B[0]=d0272939  C[0]=9455479f  D[0]=9df77adb
```

```
A[1]=6954b27d  B[1]=b763405e  C[1]=a4e8a7ad  D[1]=4a91ba2d
A[2]=10a6206e  B[2]=b8874d6e  C[2]=a50f8b94  D[2]=c7a0800b
A[3]=90735ae0  B[3]=f94b1b50  C[3]=4f6afa47  D[3]=74002722

Step 26: (r=29, s= 9)
A[0]=b6729200  B[0]=2273a003  C[0]=d0272939  D[0]=9455479f
A[1]=4e099048  B[1]=ad2a964f  C[1]=b763405e  D[1]=a4e8a7ad
A[2]=64072185  B[2]=c214c40d  C[2]=b8874d6e  D[2]=a50f8b94
A[3]=1b99a655  B[3]=120e6b5c  C[3]=f94b1b50  D[3]=4f6afa47

Step 27: (r= 9, s=15)
A[0]=5c6ff453  B[0]=e524016c  C[0]=2273a003  D[0]=d0272939
A[1]=61622d36  B[1]=1320909c  C[1]=ad2a964f  D[1]=b763405e
A[2]=74dcd053  B[2]=0e430ac8  C[2]=c214c40d  D[2]=b8874d6e
A[3]=fb6827e1  B[3]=334caa37  C[3]=120e6b5c  D[3]=f94b1b50

Step 28: (r=15, s= 5)
A[0]=a7d65602  B[0]=fa29ae37  C[0]=e524016c  D[0]=2273a003
A[1]=dda3da76  B[1]=169b30b1  C[1]=1320909c  D[1]=ad2a964f
A[2]=8eb80a7b  B[2]=6829ba6e  C[2]=0e430ac8  D[2]=c214c40d
A[3]=b57c539f  B[3]=13f0fdb4  C[3]=334caa37  D[3]=120e6b5c

Step 29: (r= 5, s=29)
A[0]=30417d22  B[0]=facac054  C[0]=fa29ae37  D[0]=e524016c
A[1]=64a84d4b  B[1]=b47b4edb  C[1]=169b30b1  D[1]=1320909c
A[2]=0963b68b  B[2]=d7014f71  C[2]=6829ba6e  D[2]=0e430ac8
A[3]=0768fe76  B[3]=af8a73f6  C[3]=13f0fdb4  D[3]=334caa37

Step 30: (r=29, s= 9)
A[0]=f5a63741  B[0]=46082fa4  C[0]=facac054  D[0]=fa29ae37
A[1]=0b72c5a4  B[1]=6c9509a9  C[1]=b47b4edb  D[1]=169b30b1
A[2]=f9076ac4  B[2]=612c76d1  C[2]=d7014f71  D[2]=6829ba6e
A[3]=a89b27eb  B[3]=c0ed1fce  C[3]=af8a73f6  D[3]=13f0fdb4

Step 31: (r= 9, s=15)
A[0]=5db36211  B[0]=4c6e83eb  C[0]=46082fa4  D[0]=facac054
A[1]=44456df5  B[1]=e58b4816  C[1]=6c9509a9  D[1]=b47b4edb
A[2]=bb299a4c  B[2]=0ed589f2  C[2]=612c76d1  D[2]=d7014f71
A[3]=89f15093  B[3]=364fd751  C[3]=c0ed1fce  D[3]=af8a73f6

Feed-Forward Step 0: (r=15, s= 5)
A[0]=eedb2e09  B[0]=b108aed9  C[0]=4c6e83eb  D[0]=46082fa4
A[1]=a4adad39  B[1]=b6faa222  C[1]=e58b4816  D[1]=6c9509a9
A[2]=5941228b  B[2]=cd265d94  C[2]=0ed589f2  D[2]=612c76d1
A[3]=25fe42de  B[3]=a849c4f8  C[3]=364fd751  D[3]=c0ed1fce

Feed-Forward Step 1: (r= 5, s=29)
A[0]=de06cec4  B[0]=db65c13d  C[0]=b108aed9  D[0]=4c6e83eb
A[1]=e72e86cf  B[1]=95b5a734  C[1]=b6faa222  D[1]=e58b4816
```

```
A[2]=a750fdde  B[2]=2824516b  C[2]=cd265d94  D[2]=0ed589f2
A[3]=96f79ae2  B[3]=bfc85bc4  C[3]=a849c4f8  D[3]=364fd751

Feed-Forward Step 2: (r=29, s= 9)
A[0]=eaf92e10  B[0]=9bc0d9d8  C[0]=db65c13d  D[0]=b108aed9
A[1]=41e73c7f  B[1]=fce5d0d9  C[1]=95b5a734  D[1]=b6faa222
A[2]=293436ee  B[2]=d4ea1fbb  C[2]=2824516b  D[2]=cd265d94
A[3]=aca3be40  B[3]=52def35c  C[3]=bfc85bc4  D[3]=a849c4f8

Feed-Forward Step 3: (r= 9, s=15)
A[0]=c87f5b43  B[0]=f25c21d5  C[0]=9bc0d9d8  D[0]=db65c13d
A[1]=818566c1  B[1]=ce78fe83  C[1]=fce5d0d9  D[1]=95b5a734
A[2]=eb0b564a  B[2]=686ddc52  C[2]=d4ea1fbb  D[2]=2824516b
A[3]=5c631a92  B[3]=477c8159  C[3]=52def35c  D[3]=bfc85bc4
```

Compression Function Output

```
A[0]=c87f5b43  B[0]=f25c21d5  C[0]=9bc0d9d8  D[0]=db65c13d
A[1]=818566c1  B[1]=ce78fe83  C[1]=fce5d0d9  D[1]=95b5a734
A[2]=eb0b564a  B[2]=686ddc52  C[2]=d4ea1fbb  D[2]=2824516b
A[3]=5c631a92  B[3]=477c8159  C[3]=52def35c  D[3]=bfc85bc4
```

Hash Function Output

```
43 5b 7f c8 c1 66 85 81 4a 56 0b eb 92 1a 63 5c
d5 21 5c f2 83 fe 78 ce 52 dc 6d 68 59 81 7c 47
```

6.3 SIMD-384

6.3.1 Empty message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
```

```
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   2 203 156  47 118 214 107 106
y[  8.. 15] =  45  93 212  20 111  73 162 251
y[ 16.. 23] =  97 215 249  53 211  19   3  89
y[ 24.. 31] =  49 207 101  67 151 130 223  23
y[ 32.. 39] = 189 202 178 239 253 127 204  49
y[ 40.. 47] =  76 236  82 137 232 157  65  79
y[ 48.. 55] =  96 161 176 130 161  30  47   9
y[ 56.. 63] = 189 247  61 226 248  90 107  64
y[ 64.. 71] =   0  88 131 243 133  59 113 115
y[ 72.. 79] =  17 236  33 213  12 191 111  19
y[ 80.. 87] = 251  61 103 208  57  35 148 248
y[ 88.. 95] =  47 116  65 119 249 178 143  40
y[ 96..103] = 189 129   8 163 204 227 230 196
y[104..111] = 205 122 151  45 187  19 227  72
y[112..119] = 247 125 111 121 140 220   6 107
y[120..127] =  77  69  10 101  21  65 149 171
y[128..135] = 255  54 101 210 139  43 150 151
y[136..143] = 212 164  45 237 146 184  95   6
y[144..151] = 160  42   8 204  46 238 254 168
y[152..159] = 208  50 156 190 106 127  34 234
y[160..167] =  68  55  79  18   4 130  53 208
y[168..175] = 181  21 175 120  25 100 192 178
y[176..183] = 161  96  81 127  96 227 210 248
y[184..191] =  68  10 196  31   9 167 150 193
y[192..199] =   0 169 126  14 124 198 144 142
y[200..207] = 240  21 224  44 245  66 146 238
y[208..215] =   6 196 154  49 200 222 109   9
y[216..223] = 210 141 192 138   8  79 114 217
y[224..231] =  68 128 249  94  53  30  27  61
y[232..239] =  52 135 106 212  70 238  30 185
y[240..247] =  10 132 146 136 117  37 251 150
y[248..255] = 180 188 247 156 236 192 108  86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
```

```
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe4201be  57fba805  993666ca  a2cb5d35
        d8cd2733  2733d8cd  9f4f60b1  52c1ad3f
Z[17] = ab81547f  06f8f908  2812d7ee  fd63029d
        d5512aaf  a80557fb  5c56a3aa  1d9ee262
Z[18] = 3b3cc4c4  44d1bb2f  037cfc84  2e2bd1d5
        bdcc4234  b892476e  15c7ea39  c761389f
Z[19] = ac6053a0  468fb971  53a0ac60  d70f28f1
        3b3cc4c4  cadd3523  07d7f829  a2cb5d35
Z[20] = 00000000  6dc2923e  6c0493fc  9d91626f
        f1310ecf  e3411cbf  f58c0a74  9f4f60b1
Z[21] = 053afac6  a64759b9  ce5931a7  5ef3a10d
        d70f28f1  c761389f  06f8f908  634e9cb2
Z[22] = 3b3cc4c4  f90806f8  2e2bd1d5  1785e87b
        2d4cd2b4  5c56a3aa  3cfac306  1a22e5de
Z[23] = 08b6f74a  9f4f60b1  65eb9a15  fac6053a
        bced4313  f74a08b6  edb5124b  5e14a1ec
Z[24] = 2f0ad0f6  d70f28f1  2575da8b  a3aa5c56
        aefd5103  ee94116c  c0693f97  053afac6
Z[25] = 2496db6a  d1d52e2b  ef73108d  b2794d87
        2b8ed472  c5a33a5d  6ea1915f  ebf71409
Z[26] = 2fe9d017  0faef052  915f6ea1  d5512aaf
        124bedb5  68889778  571ca8e4  bb2f44d1
Z[27] = 53a0ac60  6ea1915f  e5de1a22  f82907d7
        08b6f74a  1b01e4ff  b19a4e66  c84037c0
Z[28] = b3584ca8  0c32f3ce  cc9b3365  9bd3642d
        124bedb5  2654d9ac  397ec682  ef73108d
Z[29] = cadd3523  2aafd551  e1831e7d  07d7f829
```

```
          9af4650c  985767a9  44d1bb2f  dd2822d8
Z[30] = 6f809080  51e2ae1e  1a22e5de  3523cadd
          95ba6a46  d8cd2733  ef73108d  c1483eb8
Z[31] = 931d6ce3  96996967  203bdfc5  a2cb5d35
          c3e53c1b  a80557fb  c761389f  4aeab516
```

Expanded Message

```
W[ 0] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
          f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
          582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
          43352085  0e74df7b  34c15037  fbaabb59
W[ 3] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
          f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] = 5a55f8c6  57715037  e543ab73  4d530456
          31dd37a5  48fd073a  2ef90f2d  c1dab1f4
W[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
          53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] = baa04560  a439c577  15aebaa0  068121f7
          f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] = e1a64619  264dfa38  0dbbdec2  4051022b
          dbde2369  306b48fd  a439b366  109fe76e
W[ 8] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
          ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] = 4560baa0  5bc73a89  ea524560  f97fde09
          073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] = c0680000  0a1e5b0e  d55d599c  ace5ae57
          0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
          bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
          2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
          ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
          0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
          a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = ab81547f  06f8f908  2812d7ee  fd63029d
          d5512aaf  a80557fb  5c56a3aa  1d9ee262
W[17] = 3b3cc4c4  44d1bb2f  037cfc84  2e2bd1d5
          bdcc4234  b892476e  15c7ea39  c761389f
W[18] = 08b6f74a  9f4f60b1  65eb9a15  fac6053a
          bced4313  f74a08b6  edb5124b  5e14a1ec
W[19] = 00000000  6dc2923e  6c0493fc  9d91626f
          f1310ecf  e3411cbf  f58c0a74  9f4f60b1
W[20] = 3b3cc4c4  f90806f8  2e2bd1d5  1785e87b
```

```
        2d4cd2b4  5c56a3aa  3cfac306  1a22e5de
W[21] = 053afac6  a64759b9  ce5931a7  5ef3a10d
        d70f28f1  c761389f  06f8f908  634e9cb2
W[22] = fe4201be  57fba805  993666ca  a2cb5d35
        d8cd2733  2733d8cd  9f4f60b1  52c1ad3f
W[23] = ac6053a0  468fb971  53a0ac60  d70f28f1
        3b3cc4c4  cadd3523  07d7f829  a2cb5d35
W[24] = 6f809080  51e2ae1e  1a22e5de  3523cadd
        95ba6a46  d8cd2733  ef73108d  c1483eb8
W[25] = 2f0ad0f6  d70f28f1  2575da8b  a3aa5c56
        aefd5103  ee94116c  c0693f97  053afac6
W[26] = 2496db6a  d1d52e2b  ef73108d  b2794d87
        2b8ed472  c5a33a5d  6ea1915f  ebf71409
W[27] = 931d6ce3  96996967  203bdfc5  a2cb5d35
        c3e53c1b  a80557fb  c761389f  4aeab516
W[28] = 53a0ac60  6ea1915f  e5de1a22  f82907d7
        08b6f74a  1b01e4ff  b19a4e66  c84037c0
W[29] = cadd3523  2aafd551  e1831e7d  07d7f829
        9af4650c  985767a9  44d1bb2f  dd2822d8
W[30] = b3584ca8  0c32f3ce  cc9b3365  9bd3642d
        124bedb5  2654d9ac  397ec682  ef73108d
W[31] = 2fe9d017  0faef052  915f6ea1  d5512aaf
        124bedb5  68889778  571ca8e4  bb2f44d1
```

Feistel Steps

```
IV :
A[0]=3a8f3d6f  B[0]=f46f6c9b  C[0]=2da6fdc3  D[0]=91195b41
A[1]=756a1087  B[1]=9ab248ef  C[1]=fbafce00  D[1]=fcb9404e
A[2]=5d5318aa  B[2]=dbbfc9cc  C[2]=4c9a6954  D[2]=214e6c84
A[3]=bbca76f7  B[3]=cc8821fa  C[3]=b61f0faf  D[3]=88740b3a
A[4]=26a3a959  B[4]=354d3c2e  C[4]=f56099b5  D[4]=ba03a4b1
A[5]=aca1e37e  B[5]=da334fb1  C[5]=a3a5bdfb  D[5]=a82202fc
A[6]=b40c4642  B[6]=68ed79ce  C[6]=f83e0977  D[6]=994fddfb
A[7]=904085d9  B[7]=a5bc107d  C[7]=7eb15372  D[7]=b2e1a1de

IV XOR M :
A[0]=3a8f3d6f  B[0]=f46f6c9b  C[0]=2da6fdc3  D[0]=91195b41
A[1]=756a1087  B[1]=9ab248ef  C[1]=fbafce00  D[1]=fcb9404e
A[2]=5d5318aa  B[2]=dbbfc9cc  C[2]=4c9a6954  D[2]=214e6c84
A[3]=bbca76f7  B[3]=cc8821fa  C[3]=b61f0faf  D[3]=88740b3a
A[4]=26a3a959  B[4]=354d3c2e  C[4]=f56099b5  D[4]=ba03a4b1
A[5]=aca1e37e  B[5]=da334fb1  C[5]=a3a5bdfb  D[5]=a82202fc
A[6]=b40c4642  B[6]=68ed79ce  C[6]=f83e0977  D[6]=994fddfb
A[7]=904085d9  B[7]=a5bc107d  C[7]=7eb15372  D[7]=b2e1a1de

Step  0: (r= 3, s=20)
A[0]=2810e24f  B[0]=d479eb79  C[0]=f46f6c9b  D[0]=2da6fdc3
A[1]=10f2bfb4  B[1]=ab50843b  C[1]=9ab248ef  D[1]=fbafce00
```

```
A[2]=aa9e1094  B[2]=ea98c552  C[2]=dbbfc9cc  D[2]=4c9a6954
A[3]=586f481a  B[3]=de53b7bd  C[3]=cc8821fa  D[3]=b61f0faf
A[4]=ff791d73  B[4]=351d4ac9  C[4]=354d3c2e  D[4]=f56099b5
A[5]=dd7e8280  B[5]=650f1bf5  C[5]=da334fb1  D[5]=a3a5bdfb
A[6]=83f14c8f  B[6]=a0623215  C[6]=68ed79ce  D[6]=f83e0977
A[7]=e96d26f9  B[7]=82042ecc  C[7]=a5bc107d  D[7]=7eb15372

Step  1: (r=20, s=14)
A[0]=f828d34a  B[0]=24f2810e  C[0]=d479eb79  D[0]=f46f6c9b
A[1]=27b65778  B[1]=fb410f2b  C[1]=ab50843b  D[1]=9ab248ef
A[2]=e80a4db7  B[2]=094aa9e1  C[2]=ea98c552  D[2]=dbbfc9cc
A[3]=82ca28de  B[3]=81a586f4  C[3]=de53b7bd  D[3]=cc8821fa
A[4]=f013dfbe  B[4]=d73ff791  C[4]=351d4ac9  D[4]=354d3c2e
A[5]=1fe319a0  B[5]=280dd7e8  C[5]=650f1bf5  D[5]=da334fb1
A[6]=5949b32a  B[6]=c8f83f14  C[6]=a0623215  D[6]=68ed79ce
A[7]=c531e5bb  B[7]=6f9e96d2  C[7]=82042ecc  D[7]=a5bc107d

Step  2: (r=14, s=27)
A[0]=c0fdca06  B[0]=34d2be0a  C[0]=24f2810e  D[0]=d479eb79
A[1]=5809ea8a  B[1]=95de09ed  C[1]=fb410f2b  D[1]=ab50843b
A[2]=64a2453f  B[2]=936dfa02  C[2]=094aa9e1  D[2]=ea98c552
A[3]=0f9d5c3e  B[3]=8a37a0b2  C[3]=81a586f4  D[3]=de53b7bd
A[4]=aca4b256  B[4]=f7efbc04  C[4]=d73ff791  D[4]=351d4ac9
A[5]=9df3a41b  B[5]=c66807f8  C[5]=280dd7e8  D[5]=650f1bf5
A[6]=6a0ed1d5  B[6]=6cca9652  C[6]=c8f83f14  D[6]=a0623215
A[7]=9c1698df  B[7]=796ef14c  C[7]=6f9e96d2  D[7]=82042ecc

Step  3: (r=27, s= 3)
A[0]=41d75090  B[0]=3607ee50  C[0]=34d2be0a  D[0]=24f2810e
A[1]=69aa638a  B[1]=52c04f54  C[1]=95de09ed  D[1]=fb410f2b
A[2]=299dd010  B[2]=fb251229  C[2]=936dfa02  D[2]=094aa9e1
A[3]=5c7957da  B[3]=f07ceae1  C[3]=8a37a0b2  D[3]=81a586f4
A[4]=238ba820  B[4]=b5652592  C[4]=f7efbc04  D[4]=d73ff791
A[5]=e8ddc8d1  B[5]=dcef9d20  C[5]=c66807f8  D[5]=280dd7e8
A[6]=03f404cb  B[6]=ab50768e  C[6]=6cca9652  D[6]=c8f83f14
A[7]=a5cc8b6a  B[7]=fce0b4c6  C[7]=796ef14c  D[7]=6f9e96d2

Step  4: (r= 3, s=20)
A[0]=cb9e5e5a  B[0]=0eba8482  C[0]=3607ee50  D[0]=34d2be0a
A[1]=c1a4cc4c  B[1]=4d531c53  C[1]=52c04f54  D[1]=95de09ed
A[2]=59155a94  B[2]=4cee8081  C[2]=fb251229  D[2]=936dfa02
A[3]=30b8f7e7  B[3]=e3cabed2  C[3]=f07ceae1  D[3]=8a37a0b2
A[4]=fa5a575c  B[4]=1c5d4101  C[4]=b5652592  D[4]=f7efbc04
A[5]=ed812087  B[5]=46ee468f  C[5]=dcef9d20  D[5]=c66807f8
A[6]=7f16976b  B[6]=1fa02658  C[6]=ab50768e  D[6]=6cca9652
A[7]=c0e31cb7  B[7]=2e645b55  C[7]=fce0b4c6  D[7]=796ef14c

Step  5: (r=20, s=14)
A[0]=8b472d36  B[0]=e5acb9e5  C[0]=0eba8482  D[0]=3607ee50
```

```
A[1]=e69f389c  B[1]=c4cc1a4c  C[1]=4d531c53  D[1]=52c04f54
A[2]=7319bb5c  B[2]=a9459155  C[2]=4cee8081  D[2]=fb251229
A[3]=d9003778  B[3]=7e730b8f  C[3]=e3cabed2  D[3]=f07ceae1
A[4]=bf7ab371  B[4]=75cfa5a5  C[4]=1c5d4101  D[4]=b5652592
A[5]=5a5a4886  B[5]=087ed812  C[5]=46ee468f  D[5]=dcef9d20
A[6]=a784c256  B[6]=76b7f169  C[6]=1fa02658  D[6]=ab50768e
A[7]=f76f38df  B[7]=cb7c0e31  C[7]=2e645b55  D[7]=fce0b4c6

Step  6: (r=14, s=27)
A[0]=823ab4e5  B[0]=cb4da2d1  C[0]=e5acb9e5  D[0]=0eba8482
A[1]=6e74734a  B[1]=ce2739a7  C[1]=c4cc1a4c  D[1]=4d531c53
A[2]=85f2a186  B[2]=6ed71cc6  C[2]=a9459155  D[2]=4cee8081
A[3]=446e7243  B[3]=0dde3640  C[3]=7e730b8f  D[3]=e3cabed2
A[4]=8d3a92ec  B[4]=acdc6fde  C[4]=75cfa5a5  D[4]=1c5d4101
A[5]=475f5553  B[5]=92219696  C[5]=087ed812  D[5]=46ee468f
A[6]=f7473c3a  B[6]=3095a9e1  C[6]=76b7f169  D[6]=1fa02658
A[7]=3c220bb4  B[7]=ce37fddb  C[7]=cb7c0e31  D[7]=2e645b55

Step  7: (r=27, s= 3)
A[0]=00d5b09c  B[0]=2c11d5a7  C[0]=cb4da2d1  D[0]=e5acb9e5
A[1]=aa658974  B[1]=5373a39a  C[1]=ce2739a7  D[1]=c4cc1a4c
A[2]=1bc9c229  B[2]=342f950c  C[2]=6ed71cc6  D[2]=a9459155
A[3]=26b0aa60  B[3]=1a237392  C[3]=0dde3640  D[3]=7e730b8f
A[4]=5ce2385c  B[4]=6469d497  C[4]=acdc6fde  D[4]=75cfa5a5
A[5]=223ec08d  B[5]=9a3afaaa  C[5]=92219696  D[5]=087ed812
A[6]=07bc2e45  B[6]=d7ba39e1  C[6]=3095a9e1  D[6]=76b7f169
A[7]=83f60732  B[7]=a1e1105d  C[7]=ce37fddb  D[7]=cb7c0e31

Step  8: (r=26, s= 4)
A[0]=39bed46a  B[0]=700356c2  C[0]=2c11d5a7  D[0]=cb4da2d1
A[1]=abfb114d  B[1]=d2a99625  C[1]=5373a39a  D[1]=ce2739a7
A[2]=02c2edac  B[2]=a46f2708  C[2]=342f950c  D[2]=6ed71cc6
A[3]=6d62fa9b  B[3]=809ac2a9  C[3]=1a237392  D[3]=0dde3640
A[4]=bb855464  B[4]=717388e1  C[4]=6469d497  D[4]=acdc6fde
A[5]=8d5e0006  B[5]=3488fb02  C[5]=9a3afaaa  D[5]=92219696
A[6]=c1a899f3  B[6]=141ef0b9  C[6]=d7ba39e1  D[6]=3095a9e1
A[7]=8c644226  B[7]=ca0fd81c  C[7]=a1e1105d  D[7]=ce37fddb

Step  9: (r= 4, s=23)
A[0]=c8513399  B[0]=9bed46a3  C[0]=700356c2  D[0]=2c11d5a7
A[1]=3a2df5c9  B[1]=bfb114da  C[1]=d2a99625  D[1]=5373a39a
A[2]=333412ee  B[2]=2c2edac0  C[2]=a46f2708  D[2]=342f950c
A[3]=a8bdc5c5  B[3]=d62fa9b6  C[3]=809ac2a9  D[3]=1a237392
A[4]=151e5f4c  B[4]=b855464b  C[4]=717388e1  D[4]=6469d497
A[5]=5c237b9a  B[5]=d5e00068  C[5]=3488fb02  D[5]=9a3afaaa
A[6]=41d8197b  B[6]=1a899f3c  C[6]=141ef0b9  D[6]=d7ba39e1
A[7]=4884bf68  B[7]=c6442268  C[7]=ca0fd81c  D[7]=a1e1105d

Step 10: (r=23, s=11)
```

```
A[0]=9d079784  B[0]=cce42899  C[0]=9bed46a3  D[0]=700356c2
A[1]=564d8ecd  B[1]=e49d16fa  C[1]=bfb114da  D[1]=d2a99625
A[2]=ae61572c  B[2]=77199a09  C[2]=2c2edac0  D[2]=a46f2708
A[3]=6b373968  B[3]=e2d45ee2  C[3]=d62fa9b6  D[3]=809ac2a9
A[4]=4f4e1e02  B[4]=a60a8f2f  C[4]=b855464b  D[4]=717388e1
A[5]=fa30637e  B[5]=cd2e11bd  C[5]=d5e00068  D[5]=3488fb02
A[6]=c5f47fd9  B[6]=bda0ec0c  C[6]=1a899f3c  D[6]=141ef0b9
A[7]=7df93b4a  B[7]=b424425f  C[7]=c6442268  D[7]=ca0fd81c

Step 11: (r=11, s=26)
A[0]=3d87ecd1  B[0]=3cbc24e8  C[0]=cce42899  D[0]=9bed46a3
A[1]=7595b7a8  B[1]=6c766ab2  C[1]=e49d16fa  D[1]=bfb114da
A[2]=cfa517e1  B[2]=0ab96573  C[2]=77199a09  D[2]=2c2edac0
A[3]=fa82cc28  B[3]=b9cb4359  C[3]=e2d45ee2  D[3]=d62fa9b6
A[4]=dc4d8fc2  B[4]=70f0127a  C[4]=a60a8f2f  D[4]=b855464b
A[5]=7c463f25  B[5]=831bf7d1  C[5]=cd2e11bd  D[5]=d5e00068
A[6]=c4b587a5  B[6]=a3fece2f  C[6]=bda0ec0c  D[6]=1a899f3c
A[7]=6fdd6bd5  B[7]=c9da53ef  C[7]=b424425f  D[7]=c6442268

Step 12: (r=26, s= 4)
A[0]=10992d1d  B[0]=44f61fb3  C[0]=3cbc24e8  D[0]=cce42899
A[1]=248b3582  B[1]=a1d656de  C[1]=6c766ab2  D[1]=e49d16fa
A[2]=86bb4126  B[2]=873e945f  C[2]=0ab96573  D[2]=77199a09
A[3]=915df398  B[3]=a3ea0b30  C[3]=b9cb4359  D[3]=e2d45ee2
A[4]=a1fc3dc9  B[4]=0b71363f  C[4]=70f0127a  D[4]=a60a8f2f
A[5]=33b02846  B[5]=95f118fc  C[5]=831bf7d1  D[5]=cd2e11bd
A[6]=161b15e0  B[6]=9712d61e  C[6]=a3fece2f  D[6]=bda0ec0c
A[7]=cf2ac3b8  B[7]=55bf75af  C[7]=c9da53ef  D[7]=b424425f

Step 13: (r= 4, s=23)
A[0]=c00ed815  B[0]=0992d1d1  C[0]=44f61fb3  D[0]=3cbc24e8
A[1]=a475a82a  B[1]=48b35822  C[1]=a1d656de  D[1]=6c766ab2
A[2]=3185172c  B[2]=6bb41268  C[2]=873e945f  D[2]=0ab96573
A[3]=a880e89a  B[3]=15df3989  C[3]=a3ea0b30  D[3]=b9cb4359
A[4]=3b6b71d2  B[4]=1fc3dc9a  C[4]=0b71363f  D[4]=70f0127a
A[5]=beb1ac19  B[5]=3b028463  C[5]=95f118fc  D[5]=831bf7d1
A[6]=210ac5fe  B[6]=61b15e01  C[6]=9712d61e  D[6]=a3fece2f
A[7]=7334ffd7  B[7]=f2ac3b8c  C[7]=55bf75af  D[7]=c9da53ef

Step 14: (r=23, s=11)
A[0]=7d3687a7  B[0]=0ae0076c  C[0]=0992d1d1  D[0]=44f61fb3
A[1]=7ef01e35  B[1]=15523ad4  C[1]=48b35822  D[1]=a1d656de
A[2]=40d5776b  B[2]=9618c28b  C[2]=6bb41268  D[2]=873e945f
A[3]=4db7a779  B[3]=4d544074  C[3]=15df3989  D[3]=a3ea0b30
A[4]=57d58550  B[4]=e91db5b8  C[4]=1fc3dc9a  D[4]=0b71363f
A[5]=c8610757  B[5]=0cdf58d6  C[5]=3b028463  D[5]=95f118fc
A[6]=c3052b3e  B[6]=ff108562  C[6]=61b15e01  D[6]=9712d61e
A[7]=10042f90  B[7]=ebb99a7f  C[7]=f2ac3b8c  D[7]=55bf75af
```

```
Step 15: (r=11, s=26)
A[0]=9ed72620  B[0]=b43d3be9  C[0]=0ae0076c  D[0]=0992d1d1
A[1]=31459bf0  B[1]=80f1abf7  C[1]=15523ad4  D[1]=48b35822
A[2]=88d7fa4c  B[2]=abbb5a06  C[2]=9618c28b  D[2]=6bb41268
A[3]=d1f3d980  B[3]=bd3bca6d  C[3]=4d544074  D[3]=15df3989
A[4]=6089afae  B[4]=ac2a82be  C[4]=e91db5b8  D[4]=1fc3dc9a
A[5]=36e8699e  B[5]=083abe43  C[5]=0cdf58d6  D[5]=3b028463
A[6]=056cfe65  B[6]=2959f618  C[6]=ff108562  D[6]=61b15e01
A[7]=a18d5988  B[7]=217c8080  C[7]=ebb99a7f  D[7]=f2ac3b8c

Step 16: (r=19, s=28)
A[0]=a4161ec7  B[0]=3104f6b9  C[0]=b43d3be9  D[0]=0ae0076c
A[1]=1644f68a  B[1]=df818a2c  C[1]=80f1abf7  D[1]=15523ad4
A[2]=9f2cb3eb  B[2]=d26446bf  C[2]=abbb5a06  D[2]=9618c28b
A[3]=7d6be708  B[3]=cc068f9e  C[3]=bd3bca6d  D[3]=4d544074
A[4]=c6d4d0e3  B[4]=7d73044d  C[4]=ac2a82be  D[4]=e91db5b8
A[5]=8c277597  B[5]=4cf1b743  C[5]=083abe43  D[5]=0cdf58d6
A[6]=a7db1bf4  B[6]=f3282b67  C[6]=2959f618  D[6]=ff108562
A[7]=4ae0a575  B[7]=cc450c6a  C[7]=217c8080  D[7]=ebb99a7f

Step 17: (r=28, s= 7)
A[0]=def4b7f9  B[0]=7a4161ec  C[0]=3104f6b9  D[0]=b43d3be9
A[1]=f2977ee8  B[1]=a1644f68  C[1]=df818a2c  D[1]=80f1abf7
A[2]=a0c64112  B[2]=b9f2cb3e  C[2]=d26446bf  D[2]=abbb5a06
A[3]=6ab52a8b  B[3]=87d6be70  C[3]=cc068f9e  D[3]=bd3bca6d
A[4]=fc7ad648  B[4]=3c6d4d0e  C[4]=7d73044d  D[4]=ac2a82be
A[5]=2a5dce3f  B[5]=78c27759  C[5]=4cf1b743  D[5]=083abe43
A[6]=2d1cd0ed  B[6]=4a7db1bf  C[6]=f3282b67  D[6]=2959f618
A[7]=b42e7667  B[7]=54ae0a57  C[7]=cc450c6a  D[7]=217c8080

Step 18: (r= 7, s=22)
A[0]=5e0940ff  B[0]=7a5bfcef  C[0]=7a4161ec  D[0]=3104f6b9
A[1]=539bc80c  B[1]=4bbf7479  C[1]=a1644f68  D[1]=df818a2c
A[2]=256841e3  B[2]=63208950  C[2]=b9f2cb3e  D[2]=d26446bf
A[3]=ec3aca9d  B[3]=5a9545b5  C[3]=87d6be70  D[3]=cc068f9e
A[4]=d23ee5f7  B[4]=3d6b247e  C[4]=3c6d4d0e  D[4]=7d73044d
A[5]=f7bba29f  B[5]=2ee71f95  C[5]=78c27759  D[5]=4cf1b743
A[6]=507bc76a  B[6]=8e687696  C[6]=4a7db1bf  D[6]=f3282b67
A[7]=a952fcfa  B[7]=173b33da  C[7]=54ae0a57  D[7]=cc450c6a

Step 19: (r=22, s=19)
A[0]=4339ea2b  B[0]=3fd78250  C[0]=7a5bfcef  D[0]=7a4161ec
A[1]=c68f7903  B[1]=0314e6f2  C[1]=4bbf7479  D[1]=a1644f68
A[2]=0b53dfcc  B[2]=78c95a10  C[2]=63208950  D[2]=b9f2cb3e
A[3]=76c00022  B[3]=a77b0eb2  C[3]=5a9545b5  D[3]=87d6be70
A[4]=3cacdac9  B[4]=7df48fb9  C[4]=3d6b247e  D[4]=3c6d4d0e
A[5]=61cfdfa3  B[5]=a7fdeee8  C[5]=2ee71f95  D[5]=78c27759
A[6]=dc60f315  B[6]=da941ef1  C[6]=8e687696  D[6]=4a7db1bf
A[7]=a7511946  B[7]=3eaa54bf  C[7]=173b33da  D[7]=54ae0a57
```

```
Step 20: (r=19, s=28)
A[0]=7b2bd58c  B[0]=515a19cf  C[0]=3fd78250  D[0]=7a5bfcef
A[1]=8f3ad67c  B[1]=c81e347b  C[1]=0314e6f2  D[1]=4bbf7479
A[2]=3649bd86  B[2]=fe605a9e  C[2]=78c95a10  D[2]=63208950
A[3]=cfc33557  B[3]=0113b600  C[3]=a77b0eb2  D[3]=5a9545b5
A[4]=b7957969  B[4]=d649e566  C[4]=7df48fb9  D[4]=3d6b247e
A[5]=261a7510  B[5]=fd1b0e7e  C[5]=a7fdeee8  D[5]=2ee71f95
A[6]=7092c93d  B[6]=98aee307  C[6]=da941ef1  D[6]=8e687696
A[7]=d30fa328  B[7]=ca353a88  C[7]=3eaa54bf  D[7]=173b33da

Step 21: (r=28, s= 7)
A[0]=dca95cd5  B[0]=c7b2bd58  C[0]=515a19cf  D[0]=3fd78250
A[1]=0fde8993  B[1]=c8f3ad67  C[1]=c81e347b  D[1]=0314e6f2
A[2]=a93d842f  B[2]=63649bd8  C[2]=fe605a9e  D[2]=78c95a10
A[3]=37021787  B[3]=7cfc3355  C[3]=0113b600  D[3]=a77b0eb2
A[4]=ff269899  B[4]=9b795796  C[4]=d649e566  D[4]=7df48fb9
A[5]=3f145080  B[5]=0261a751  C[5]=fd1b0e7e  D[5]=a7fdeee8
A[6]=9796c14c  B[6]=d7092c93  C[6]=98aee307  D[6]=da941ef1
A[7]=5ee3417b  B[7]=8d30fa32  C[7]=ca353a88  D[7]=3eaa54bf

Step 22: (r= 7, s=22)
A[0]=ec65b297  B[0]=54ae6aee  C[0]=c7b2bd58  D[0]=515a19cf
A[1]=e5e9a21a  B[1]=ef44c987  C[1]=c8f3ad67  D[1]=c81e347b
A[2]=68679935  B[2]=9ec217d4  C[2]=63649bd8  D[2]=fe605a9e
A[3]=4e6c2327  B[3]=810bc39b  C[3]=7cfc3355  D[3]=0113b600
A[4]=a1994e7e  B[4]=934c4cff  C[4]=9b795796  D[4]=d649e566
A[5]=2005a887  B[5]=8a28401f  C[5]=0261a751  D[5]=fd1b0e7e
A[6]=1989261f  B[6]=cb60a64b  C[6]=d7092c93  D[6]=98aee307
A[7]=62c6524d  B[7]=71a0bdaf  C[7]=8d30fa32  D[7]=ca353a88

Step 23: (r=22, s=19)
A[0]=e216795c  B[0]=a5fb196c  C[0]=54ae6aee  D[0]=c7b2bd58
A[1]=d967e5e6  B[1]=86b97a68  C[1]=ef44c987  D[1]=c8f3ad67
A[2]=9e5c4586  B[2]=4d5a19e6  C[2]=9ec217d4  D[2]=63649bd8
A[3]=a399d60c  B[3]=c9d39b08  C[3]=810bc39b  D[3]=7cfc3355
A[4]=6f40406b  B[4]=9fa86653  C[4]=934c4cff  D[4]=9b795796
A[5]=a47fcb37  B[5]=21c8016a  C[5]=8a28401f  D[5]=0261a751
A[6]=57b5f666  B[6]=87c66249  C[6]=cb60a64b  D[6]=d7092c93
A[7]=593a1014  B[7]=9358b194  C[7]=71a0bdaf  D[7]=8d30fa32

Step 24: (r=15, s= 5)
A[0]=70a0a590  B[0]=3cae710b  C[0]=a5fb196c  D[0]=54ae6aee
A[1]=5ba6ede3  B[1]=f2f36cb3  C[1]=86b97a68  D[1]=ef44c987
A[2]=3739035d  B[2]=22c34f2e  C[2]=4d5a19e6  D[2]=9ec217d4
A[3]=993588d4  B[3]=eb0651cc  C[3]=c9d39b08  D[3]=810bc39b
A[4]=ed9da8b9  B[4]=2035b7a0  C[4]=9fa86653  D[4]=934c4cff
A[5]=cf0fad60  B[5]=e59bd23f  C[5]=21c8016a  D[5]=8a28401f
A[6]=d01e19c7  B[6]=fb332bda  C[6]=87c66249  D[6]=cb60a64b
```

```
A[7]=fd72010a  B[7]=080a2c9d  C[7]=9358b194  D[7]=71a0bdaf

Step 25: (r= 5, s=29)
A[0]=ee56fa50  B[0]=1414b20e  C[0]=3cae710b  D[0]=a5fb196c
A[1]=9a5308b7  B[1]=74ddbc6b  C[1]=f2f36cb3  D[1]=86b97a68
A[2]=b9e413cf  B[2]=e7206ba6  C[2]=22c34f2e  D[2]=4d5a19e6
A[3]=32ad42e2  B[3]=26b11a93  C[3]=eb0651cc  D[3]=c9d39b08
A[4]=92532996  B[4]=b3b5173d  C[4]=2035b7a0  D[4]=9fa86653
A[5]=5a111b95  B[5]=e1f5ac19  C[5]=e59bd23f  D[5]=21c8016a
A[6]=4028a172  B[6]=03c338fa  C[6]=fb332bda  D[6]=87c66249
A[7]=1212793b  B[7]=ae40215f  C[7]=080a2c9d  D[7]=9358b194

Step 26: (r=29, s= 9)
A[0]=ff9212e5  B[0]=1dcadf4a  C[0]=1414b20e  D[0]=3cae710b
A[1]=482e81c1  B[1]=f34a6116  C[1]=74ddbc6b  D[1]=f2f36cb3
A[2]=8c365731  B[2]=f73c8279  C[2]=e7206ba6  D[2]=22c34f2e
A[3]=b242a001  B[3]=4655a85c  C[3]=26b11a93  D[3]=eb0651cc
A[4]=1ff99b56  B[4]=d24a6532  C[4]=b3b5173d  D[4]=2035b7a0
A[5]=05448813  B[5]=ab422372  C[5]=e1f5ac19  D[5]=e59bd23f
A[6]=e987a678  B[6]=4805142e  C[6]=03c338fa  D[6]=fb332bda
A[7]=cda1585c  B[7]=62424f27  C[7]=ae40215f  D[7]=080a2c9d

Step 27: (r= 9, s=15)
A[0]=3b5322e8  B[0]=2425cbff  C[0]=1dcadf4a  D[0]=1414b20e
A[1]=92b2a53e  B[1]=5d038290  C[1]=f34a6116  D[1]=74ddbc6b
A[2]=bc2206ec  B[2]=6cae6318  C[2]=f73c8279  D[2]=e7206ba6
A[3]=f77a83fc  B[3]=85400364  C[3]=4655a85c  D[3]=26b11a93
A[4]=a0a11732  B[4]=f336ac3f  C[4]=d24a6532  D[4]=b3b5173d
A[5]=842dba59  B[5]=8910260a  C[5]=ab422372  D[5]=e1f5ac19
A[6]=2d3fe984  B[6]=0f4cf1d3  C[6]=4805142e  D[6]=03c338fa
A[7]=2a9d5dfe  B[7]=42b0b99b  C[7]=62424f27  D[7]=ae40215f

Step 28: (r=15, s= 5)
A[0]=f1c4946d  B[0]=91741da9  C[0]=2425cbff  D[0]=1dcadf4a
A[1]=61b1f9bf  B[1]=529f4959  C[1]=5d038290  D[1]=f34a6116
A[2]=678f83d6  B[2]=03765e11  C[2]=6cae6318  D[2]=f73c8279
A[3]=c8cb1aed  B[3]=41fe7bbd  C[3]=85400364  D[3]=4655a85c
A[4]=aef3394b  B[4]=8b995050  C[4]=f336ac3f  D[4]=d24a6532
A[5]=4a8fbea0  B[5]=dd2cc216  C[5]=8910260a  D[5]=ab422372
A[6]=fc6e3226  B[6]=f4c2169f  C[6]=0f4cf1d3  D[6]=4805142e
A[7]=16d8f27a  B[7]=aeff154e  C[7]=42b0b99b  D[7]=62424f27

Step 29: (r= 5, s=29)
A[0]=45321117  B[0]=38928dbe  C[0]=91741da9  D[0]=2425cbff
A[1]=27551db9  B[1]=363f37ec  C[1]=529f4959  D[1]=5d038290
A[2]=00a04a3e  B[2]=f1f07acc  C[2]=03765e11  D[2]=6cae6318
A[3]=783e2f7a  B[3]=19635db9  C[3]=41fe7bbd  D[3]=85400364
A[4]=b0e48532  B[4]=de672975  C[4]=8b995050  D[4]=f336ac3f
A[5]=7cb31565  B[5]=51f7d409  C[5]=dd2cc216  D[5]=8910260a
```

```
A[6]=6f8bc9b3  B[6]=8dc644df  C[6]=f4c2169f  D[6]=0f4cf1d3
A[7]=7ac43874  B[7]=db1e4f42  C[7]=aeff154e  D[7]=42b0b99b

Step 30: (r=29, s= 9)
A[0]=efc554df  B[0]=e8a64222  C[0]=38928dbe  D[0]=91741da9
A[1]=191a2874  B[1]=24eaa3b7  C[1]=363f37ec  D[1]=529f4959
A[2]=23779522  B[2]=c0140947  C[2]=f1f07acc  D[2]=03765e11
A[3]=79eb259b  B[3]=4f07c5ef  C[3]=19635db9  D[3]=41fe7bbd
A[4]=1e3e8f2f  B[4]=561c90a6  C[4]=de672975  D[4]=8b995050
A[5]=f9bb7f61  B[5]=af9662ac  C[5]=51f7d409  D[5]=dd2cc216
A[6]=40e48c24  B[6]=6df17936  C[6]=8dc644df  D[6]=f4c2169f
A[7]=ec751e7c  B[7]=8f58870e  C[7]=db1e4f42  D[7]=aeff154e

Step 31: (r= 9, s=15)
A[0]=965db32e  B[0]=8aa9bfdf  C[0]=e8a64222  D[0]=38928dbe
A[1]=a5ce8f37  B[1]=3450e832  C[1]=24eaa3b7  D[1]=363f37ec
A[2]=bc1483a5  B[2]=ef2a4446  C[2]=c0140947  D[2]=f1f07acc
A[3]=6050b231  B[3]=d64b36f3  C[3]=4f07c5ef  D[3]=19635db9
A[4]=6e403df0  B[4]=7d1e5e3c  C[4]=561c90a6  D[4]=de672975
A[5]=9c2c87e8  B[5]=76fec3f3  C[5]=af9662ac  D[5]=51f7d409
A[6]=75071127  B[6]=c9184881  C[6]=6df17936  D[6]=8dc644df
A[7]=0b01d3b8  B[7]=ea3cf9d8  C[7]=8f58870e  D[7]=db1e4f42

Feed-Forward Step 0: (r=15, s= 5)
A[0]=01539a52  B[0]=d9974b2e  C[0]=8aa9bfdf  D[0]=e8a64222
A[1]=dad56fe8  B[1]=479bd2e7  C[1]=3450e832  D[1]=24eaa3b7
A[2]=c18c27af  B[2]=41d2de0a  C[2]=ef2a4446  D[2]=c0140947
A[3]=d07c73ee  B[3]=5918b028  C[3]=d64b36f3  D[3]=4f07c5ef
A[4]=68e22ea6  B[4]=1ef83720  C[4]=7d1e5e3c  D[4]=561c90a6
A[5]=ea0ba486  B[5]=43f44e16  C[5]=76fec3f3  D[5]=af9662ac
A[6]=623a6bd1  B[6]=8893ba83  C[6]=c9184881  D[6]=6df17936
A[7]=bf8911c2  B[7]=e9dc0580  C[7]=ea3cf9d8  D[7]=8f58870e

Feed-Forward Step 1: (r= 5, s=29)
A[0]=be9f11c1  B[0]=2a734a40  C[0]=d9974b2e  D[0]=8aa9bfdf
A[1]=145453cd  B[1]=5aadfd1b  C[1]=479bd2e7  D[1]=3450e832
A[2]=cbe20d6b  B[2]=3184f5f8  C[2]=41d2de0a  D[2]=ef2a4446
A[3]=a8e3609f  B[3]=0f8e7dda  C[3]=5918b028  D[3]=d64b36f3
A[4]=dc7a428d  B[4]=1c45d4cd  C[4]=1ef83720  D[4]=7d1e5e3c
A[5]=8d39f791  B[5]=417490dd  C[5]=43f44e16  D[5]=76fec3f3
A[6]=c843f87d  B[6]=474d7a2c  C[6]=8893ba83  D[6]=c9184881
A[7]=a54ec101  B[7]=f1223857  C[7]=e9dc0580  D[7]=ea3cf9d8

Feed-Forward Step 2: (r=29, s= 9)
A[0]=fcb9f866  B[0]=37d3e238  C[0]=2a734a40  D[0]=d9974b2e
A[1]=da173a16  B[1]=a28a8a79  C[1]=5aadfd1b  D[1]=479bd2e7
A[2]=dcb1436c  B[2]=797c41ad  C[2]=3184f5f8  D[2]=41d2de0a
A[3]=c5fe021d  B[3]=f51c6c13  C[3]=0f8e7dda  D[3]=5918b028
A[4]=73f7a935  B[4]=bb8f4851  C[4]=1c45d4cd  D[4]=1ef83720
```

```
A[5]=abb14c6a  B[5]=31a73ef2  C[5]=417490dd  D[5]=43f44e16
A[6]=f223d67d  B[6]=b9087f0f  C[6]=474d7a2c  D[6]=8893ba83
A[7]=387778dd  B[7]=34a9d820  C[7]=f1223857  D[7]=e9dc0580

Feed-Forward Step 3: (r= 9, s=15)
A[0]=339a3ba9  B[0]=73f0cdf9  C[0]=37d3e238  D[0]=2a734a40
A[1]=53c038d6  B[1]=2e742db4  C[1]=a28a8a79  D[1]=5aadfd1b
A[2]=67d26a0f  B[2]=6286d9b9  C[2]=797c41ad  D[2]=3184f5f8
A[3]=8b8c92c4  B[3]=fc043b8b  C[3]=f51c6c13  D[3]=0f8e7dda
A[4]=1045da3a  B[4]=ef526ae7  C[4]=bb8f4851  D[4]=1c45d4cd
A[5]=2578d4b1  B[5]=6298d557  C[5]=31a73ef2  D[5]=417490dd
A[6]=6dccc551  B[6]=47acfbe4  C[6]=b9087f0f  D[6]=474d7a2c
A[7]=7bb4827a  B[7]=eef1ba70  C[7]=34a9d820  D[7]=f1223857
```

Compression Function Output

```
A[0]=339a3ba9  B[0]=73f0cdf9  C[0]=37d3e238  D[0]=2a734a40
A[1]=53c038d6  B[1]=2e742db4  C[1]=a28a8a79  D[1]=5aadfd1b
A[2]=67d26a0f  B[2]=6286d9b9  C[2]=797c41ad  D[2]=3184f5f8
A[3]=8b8c92c4  B[3]=fc043b8b  C[3]=f51c6c13  D[3]=0f8e7dda
A[4]=1045da3a  B[4]=ef526ae7  C[4]=bb8f4851  D[4]=1c45d4cd
A[5]=2578d4b1  B[5]=6298d557  C[5]=31a73ef2  D[5]=417490dd
A[6]=6dccc551  B[6]=47acfbe4  C[6]=b9087f0f  D[6]=474d7a2c
A[7]=7bb4827a  B[7]=eef1ba70  C[7]=34a9d820  D[7]=f1223857
```

Hash Function Output

```
a9 3b 9a 33 d6 38 c0 53 0f 6a d2 67 c4 92 8c 8b
3a da 45 10 b1 d4 78 25 51 c5 cc 6d 7a 82 b4 7b
f9 cd f0 73 b4 2d 74 2e b9 d9 86 62 8b 3b 04 fc
```

6.3.2 One block message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
```

```
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
y[104..111] =  129  171   92   61  218   92  254   87
y[112..119] =   84  189  205  152  233    8  203  182
y[120..127] =  168  207  190  143  124  129   57   30
y[128..135] =  192  141   92  168  121  110  169   28
y[136..143] =  128  161  211  146  197   45   44  249
y[144..151] =  171  249   62   82  157  156   70   32
y[152..159] =  122  202  163   42  174   32   21  256
y[160..167] =  244   93  107    0   28  137   44  134
y[168..175] =  129  255  154   17   97  197  180   68
y[176..183] =  132  107  244   30   65  163  147  190
y[184..191] =  115  193   79   65   69  180   30   67
y[192..199] =  205    3  191  238   12   69   15  256
y[200..207] =  106   66  122   90  108  168    4   39
y[208..215] =   82  251  217  159   43   47   16  138
y[216..223] =   62   41  152   21   23  239  124  246
y[224..231] =  176   51  194   43   74   68  188  100
y[232..239] =   19  207   16  134  197   67  195   38
y[240..247] =    3  145  211  141   79   12    7  226
y[248..255] =   91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
```

```
           12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] =  f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
           55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] =  17d9d841  5771a4f2  cedcdb25  12ca2d87
           c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] =  cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
           dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] =  ac2cd107  bfaf427c  4f7e5771  143cc068
           baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] =  fa38c1da  3b422cce  b703b7bc  17203296
           d841582a  1e5abc12  1720c405  ff470f2d
Z[10] =  4335f69b  00004d53  a948143c  a71d1fcc
           fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] =  4d53a5ab  15aef69b  bc122ef9  cf95b082
           d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] =  022bda6c  f245d04e  31dd08ac  ff470ad7
           2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] =  fbaa3b42  b92ee318  21f71f13  aa010b90
           1da12cce  0f2db41f  f2fe109f  f80d599c
Z[14] =  24dbc577  1f13d279  3124357a  4844ce23
           dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] =  af10022b  ac2cdec2  08ac3917  e999050f
           1da141c3  4ec549b6  c914d332  213ef470
Z[16] =  c761ad3f  50246ce3  69674155  b3582f0a
           6f806f80  d7ee51e2  cbbc053a  26542fe9
Z[17] =  b5160000  3602037c  a8e4ce59  3cfa45b0
           6a46f58c  ae1e57fb  b7b33523  124bb358
Z[18] =  f4ada2cb  5d35ce59  18646967  2654fc84
           9080c227  a6471785  547f9e70  bced59b9
Z[19] =  931d1409  f4ada8e4  389fb971  a02edc49
           642d31a7  44d1fc84  3c1b915f  1a222e2b
Z[20] =  d2b4bdcc  c682f210  0a7428f1  0d11b279
           5c56ee94  6a461a22  5e14b0bb  037c5fd2
Z[21] =  476e124b  dd280d11  2575e87b  0df03523
           36029857  a489397e  14094aea  6c04492c
Z[22] =  b971d017  c91f923e  4076d393  c3e536e1
           108d9080  0df05024  cbbcde07  c9fefd63
Z[23] =  029d492c  d7eed2b4  44d1eb18  0619d0f6
           4f45b279  58dac5a3  c9fe6c04  f21031a7
Z[24] =  9af44a0b  b279aaa2  5fd2dee6  1864132a
           ac60b516  9f4fc148  27333dd9  f90836e1
Z[25] =  f908d0f6  476ea489  a8052733  1be093fc
           d01765eb  2496a489  1be04313  ff21e87b
Z[26] =  5103571c  0000fd63  97781b01  94db132a
           fe42b516  0ecf3365  cbbc23b7  3b3cba50
Z[27] =  5d3508b6  1a22045b  ae1e492c  c5a34ca8
           c840116c  389f07d7  bcedfe42  3a5d492c
Z[28] =  029dab81  ef733523  3c1bfba5  ff210fae
           397e16a6  4e66108d  b2790fae  21f9626f
```

```
Z[29] = fac6f131  aaa259b9  28f13eb8  98579bd3
        23b767a9  124b2733  f0521943  f66bf3ce
Z[30] = 2c6d1cbf  25756967  3b3cc4c4  571c16a6
        d472b516  94db3523  3a5d5024  211a4bc9
Z[31] = 9e70c4c4  9af4a489  0a7406f8  e4ffbeab
        23b7d472  5ef39cb2  bdcc9080  28121a22
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b5160000  3602037c  a8e4ce59  3cfa45b0
        6a46f58c  ae1e57fb  b7b33523  124bb358
W[17] = f4ada2cb  5d35ce59  18646967  2654fc84
        9080c227  a6471785  547f9e70  bced59b9
W[18] = 029d492c  d7eed2b4  44d1eb18  0619d0f6
        4f45b279  58dac5a3  c9fe6c04  f21031a7
W[19] = d2b4bdcc  c682f210  0a7428f1  0d11b279
        5c56ee94  6a461a22  5e14b0bb  037c5fd2
```

```
W[20] = b971d017  c91f923e  4076d393  c3e536e1
        108d9080  0df05024  cbbcde07  c9fefd63
W[21] = 476e124b  dd280d11  2575e87b  0df03523
        36029857  a489397e  14094aea  6c04492c
W[22] = c761ad3f  50246ce3  69674155  b3582f0a
        6f806f80  d7ee51e2  cbbc053a  26542fe9
W[23] = 931d1409  f4ada8e4  389fb971  a02edc49
        642d31a7  44d1fc84  3c1b915f  1a222e2b
W[24] = 2c6d1cbf  25756967  3b3cc4c4  571c16a6
        d472b516  94db3523  3a5d5024  211a4bc9
W[25] = 9af44a0b  b279aaa2  5fd2dee6  1864132a
        ac60b516  9f4fc148  27333dd9  f90836e1
W[26] = f908d0f6  476ea489  a8052733  1be093fc
        d01765eb  2496a489  1be04313  ff21e87b
W[27] = 9e70c4c4  9af4a489  0a7406f8  e4ffbeab
        23b7d472  5ef39cb2  bdcc9080  28121a22
W[28] = 5d3508b6  1a22045b  ae1e492c  c5a34ca8
        c840116c  389f07d7  bcedfe42  3a5d492c
W[29] = fac6f131  aaa259b9  28f13eb8  98579bd3
        23b767a9  124b2733  f0521943  f66bf3ce
W[30] = 029dab81  ef733523  3c1bfba5  ff210fae
        397e16a6  4e66108d  b2790fae  21f9626f
W[31] = 5103571c  0000fd63  97781b01  94db132a
        fe42b516  0ecf3365  cbbc23b7  3b3cba50
```

Feistel Steps

```
IV :
A[0]=3a8f3d6f  B[0]=f46f6c9b  C[0]=2da6fdc3  D[0]=91195b41
A[1]=756a1087  B[1]=9ab248ef  C[1]=fbafce00  D[1]=fcb9404e
A[2]=5d5318aa  B[2]=dbbfc9cc  C[2]=4c9a6954  D[2]=214e6c84
A[3]=bbca76f7  B[3]=cc8821fa  C[3]=b61f0faf  D[3]=88740b3a
A[4]=26a3a959  B[4]=354d3c2e  C[4]=f56099b5  D[4]=ba03a4b1
A[5]=aca1e37e  B[5]=da334fb1  C[5]=a3a5bdfb  D[5]=a82202fc
A[6]=b40c4642  B[6]=68ed79ce  C[6]=f83e0977  D[6]=994fddfb
A[7]=904085d9  B[7]=a5bc107d  C[7]=7eb15372  D[7]=b2e1a1de

IV XOR M :
A[0]=398d3c6f  B[0]=d74d4dbb  C[0]=6ee4bc83  D[0]=f27b3a21
A[1]=726c1583  B[1]=bd946dcb  C[1]=bce98b44  D[1]=9bdf252a
A[2]=565911a2  B[2]=f095e0e4  C[2]=07d0201c  D[2]=4a2405ec
A[3]=b4c47bfb  B[3]=e3a60cd6  C[3]=f95142e3  D[3]=e71a6656
A[4]=35b1b849  B[4]=067f0d1e  C[4]=a632c8e5  D[4]=c971d5c1
A[5]=bbb7f66a  B[5]=ed057a85  C[5]=f4f3e8af  D[5]=df547788
A[6]=af165f5a  B[6]=53d740f6  C[6]=a364502f  D[6]=e235a483
A[7]=8f5e98c5  B[7]=9a822d41  C[7]=21ef0e2e  D[7]=cd9fdca2

Step  0: (r= 3, s=20)
A[0]=9160e923  B[0]=cc69e379  C[0]=d74d4dbb  D[0]=6ee4bc83
```

```
A[1]=62822b23  B[1]=9360ac1b  C[1]=bd946dcb  D[1]=bce98b44
A[2]=301d6161  B[2]=b2c88d12  C[2]=f095e0e4  D[2]=07d0201c
A[3]=a0466834  B[3]=a623dfdd  C[3]=e3a60cd6  D[3]=f95142e3
A[4]=dd55da55  B[4]=ad8dc249  C[4]=067f0d1e  D[4]=a632c8e5
A[5]=294b6799  B[5]=ddbfb355  C[5]=ed057a85  D[5]=f4f3e8af
A[6]=ae73f116  B[6]=78b2fad5  C[6]=53d740f6  D[6]=a364502f
A[7]=216f9998  B[7]=7af4c62c  C[7]=9a822d41  D[7]=21ef0e2e

Step  1: (r=20, s=14)
A[0]=34b25521  B[0]=9239160e  C[0]=cc69e379  D[0]=d74d4dbb
A[1]=6a8a7141  B[1]=b2362822  C[1]=9360ac1b  D[1]=bd946dcb
A[2]=f16a87db  B[2]=161301d6  C[2]=b2c88d12  D[2]=f095e0e4
A[3]=21866411  B[3]=834a0466  C[3]=a623dfdd  D[3]=e3a60cd6
A[4]=5e57250e  B[4]=a55dd55d  C[4]=ad8dc249  D[4]=067f0d1e
A[5]=b312527f  B[5]=799294b6  C[5]=ddbfb355  D[5]=ed057a85
A[6]=ae9aed43  B[6]=116ae73f  C[6]=78b2fad5  D[6]=53d740f6
A[7]=65a59ba2  B[7]=998216f9  C[7]=7af4c62c  D[7]=9a822d41

Step  2: (r=14, s=27)
A[0]=ce523f64  B[0]=95484d2c  C[0]=9239160e  D[0]=cc69e379
A[1]=8ca21747  B[1]=9c505aa2  C[1]=b2362822  D[1]=9360ac1b
A[2]=e3dcfdcb  B[2]=a1f6fc5a  C[2]=161301d6  D[2]=b2c88d12
A[3]=0d191632  B[3]=99044861  C[3]=834a0466  D[3]=a623dfdd
A[4]=f47601e8  B[4]=c9439795  C[4]=a55dd55d  D[4]=ad8dc249
A[5]=ebace7d7  B[5]=949fecc4  C[5]=799294b6  D[5]=ddbfb355
A[6]=bb0ae489  B[6]=bb50eba6  C[6]=116ae73f  D[6]=78b2fad5
A[7]=fc671a89  B[7]=66e89969  C[7]=998216f9  D[7]=7af4c62c

Step  3: (r=27, s= 3)
A[0]=9060cab4  B[0]=267291fb  C[0]=95484d2c  D[0]=9239160e
A[1]=39b34fa0  B[1]=3c6510ba  C[1]=9c505aa2  D[1]=b2362822
A[2]=46175e2f  B[2]=5f1ee7ee  C[2]=a1f6fc5a  D[2]=161301d6
A[3]=5a4a23be  B[3]=9068c8b1  C[3]=99044861  D[3]=834a0466
A[4]=ac15b674  B[4]=47a3b00f  C[4]=c9439795  D[4]=a55dd55d
A[5]=0472ee9e  B[5]=bf5d673e  C[5]=949fecc4  D[5]=799294b6
A[6]=eccb54c8  B[6]=4dd85724  C[6]=bb50eba6  D[6]=116ae73f
A[7]=c8923156  B[7]=4fe338d4  C[7]=66e89969  D[7]=998216f9

Step  4: (r= 3, s=20)
A[0]=9589d462  B[0]=830655a4  C[0]=267291fb  D[0]=95484d2c
A[1]=56108219  B[1]=cd9a7d01  C[1]=3c6510ba  D[1]=9c505aa2
A[2]=c1174d20  B[2]=30baf17a  C[2]=5f1ee7ee  D[2]=a1f6fc5a
A[3]=91d9477c  B[3]=d2511df2  C[3]=9068c8b1  D[3]=99044861
A[4]=d5ac58f4  B[4]=60adb3a5  C[4]=47a3b00f  D[4]=c9439795
A[5]=8f496cba  B[5]=239774f0  C[5]=bf5d673e  D[5]=949fecc4
A[6]=cc8bb6ef  B[6]=665aa647  C[6]=4dd85724  D[6]=bb50eba6
A[7]=fe4a876e  B[7]=44918ab6  C[7]=4fe338d4  D[7]=66e89969

Step  5: (r=20, s=14)
```

```
A[0]=5e9ad574  B[0]=4629589d  C[0]=830655a4  D[0]=267291fb
A[1]=552dae47  B[1]=21956108  C[1]=cd9a7d01  D[1]=3c6510ba
A[2]=f9b9a264  B[2]=d20c1174  C[2]=30baf17a  D[2]=5f1ee7ee
A[3]=d22f1698  B[3]=77c91d94  C[3]=d2511df2  D[3]=9068c8b1
A[4]=ab8ba1f7  B[4]=8f4d5ac5  C[4]=60adb3a5  D[4]=47a3b00f
A[5]=173bfdc8  B[5]=cba8f496  C[5]=239774f0  D[5]=bf5d673e
A[6]=c75a220d  B[6]=6efcc8bb  C[6]=665aa647  D[6]=4dd85724
A[7]=63eddf79  B[7]=76efe4a8  C[7]=44918ab6  D[7]=4fe338d4

Step  6: (r=14, s=27)
A[0]=eb7c10bd  B[0]=b55d17a6  C[0]=4629589d  D[0]=830655a4
A[1]=44b07381  B[1]=6b91d54b  C[1]=21956108  D[1]=cd9a7d01
A[2]=cbd668c4  B[2]=68993e6e  C[2]=d20c1174  D[2]=30baf17a
A[3]=ed904127  B[3]=c5a6348b  C[3]=77c91d94  D[3]=d2511df2
A[4]=edb360f4  B[4]=e87deae2  C[4]=8f4d5ac5  D[4]=60adb3a5
A[5]=bee61937  B[5]=ff7205ce  C[5]=cba8f496  D[5]=239774f0
A[6]=d127e236  B[6]=888371d6  C[6]=6efcc8bb  D[6]=665aa647
A[7]=84f94114  B[7]=77de58fb  C[7]=76efe4a8  D[7]=44918ab6

Step  7: (r=27, s= 3)
A[0]=c358ce11  B[0]=ef5be085  C[0]=b55d17a6  D[0]=4629589d
A[1]=d84eb840  B[1]=0a25839c  C[1]=6b91d54b  D[1]=21956108
A[2]=95714479  B[2]=265eb346  C[2]=68993e6e  D[2]=d20c1174
A[3]=95d33452  B[3]=3f6c8209  C[3]=c5a6348b  D[3]=77c91d94
A[4]=05248f72  B[4]=a76d9b07  C[4]=e87deae2  D[4]=8f4d5ac5
A[5]=c6ec1fba  B[5]=bdf730c9  C[5]=ff7205ce  D[5]=cba8f496
A[6]=5b9c4bd9  B[6]=b6893f11  C[6]=888371d6  D[6]=6efcc8bb
A[7]=7fe0e0be  B[7]=a427ca08  C[7]=77de58fb  D[7]=76efe4a8

Step  8: (r=26, s= 4)
A[0]=ccd401df  B[0]=470d6338  C[0]=ef5be085  D[0]=b55d17a6
A[1]=dc8db097  B[1]=03613ae1  C[1]=0a25839c  D[1]=6b91d54b
A[2]=c35f99e5  B[2]=e655c511  C[2]=265eb346  D[2]=68993e6e
A[3]=52b7f7dc  B[3]=4a574cd1  C[3]=3f6c8209  D[3]=c5a6348b
A[4]=91e43127  B[4]=c814923d  C[4]=a76d9b07  D[4]=e87deae2
A[5]=4e5983ca  B[5]=eb1bb07e  C[5]=bdf730c9  D[5]=ff7205ce
A[6]=a3ccf3ce  B[6]=656e712f  C[6]=b6893f11  D[6]=888371d6
A[7]=2c49874a  B[7]=f9ff8382  C[7]=a427ca08  D[7]=77de58fb

Step  9: (r= 4, s=23)
A[0]=6aae7eab  B[0]=cd401dfc  C[0]=470d6338  D[0]=ef5be085
A[1]=e3412ec4  B[1]=c8db097d  C[1]=03613ae1  D[1]=0a25839c
A[2]=02459e84  B[2]=35f99e5c  C[2]=e655c511  D[2]=265eb346
A[3]=b7dd5711  B[3]=2b7f7dc5  C[3]=4a574cd1  D[3]=3f6c8209
A[4]=4dff62d6  B[4]=1e431279  C[4]=c814923d  D[4]=a76d9b07
A[5]=5cad8a19  B[5]=e5983ca4  C[5]=eb1bb07e  D[5]=bdf730c9
A[6]=87862889  B[6]=3ccf3cea  C[6]=656e712f  D[6]=b6893f11
A[7]=bb409940  B[7]=c49874a2  C[7]=f9ff8382  D[7]=a427ca08
```

```
Step 10: (r=23, s=11)
A[0]=e722ea40  B[0]=55b5573f  C[0]=cd401dfc  D[0]=470d6338
A[1]=a82640fa  B[1]=6271a097  C[1]=c8db097d  D[1]=03613ae1
A[2]=798690a9  B[2]=420122cf  C[2]=35f99e5c  D[2]=e655c511
A[3]=027c0d01  B[3]=88dbeeab  C[3]=2b7f7dc5  D[3]=4a574cd1
A[4]=a4acc1c6  B[4]=6b26ffb1  C[4]=1e431279  D[4]=c814923d
A[5]=200bf203  B[5]=0cae56c5  C[5]=e5983ca4  D[5]=eb1bb07e
A[6]=9aa7ff70  B[6]=44c3c314  C[6]=3ccf3cea  D[6]=656e712f
A[7]=04b0cb47  B[7]=a05da04c  C[7]=c49874a2  D[7]=f9ff8382

Step 11: (r=11, s=26)
A[0]=53109f54  B[0]=17520739  C[0]=55b5573f  D[0]=cd401dfc
A[1]=30203f1b  B[1]=3207d541  C[1]=6271a097  D[1]=c8db097d
A[2]=bde4b982  B[2]=34854bcc  C[2]=420122cf  D[2]=35f99e5c
A[3]=8079f64c  B[3]=e0680813  C[3]=88dbeeab  D[3]=2b7f7dc5
A[4]=f2467a42  B[4]=660e3525  C[4]=6b26ffb1  D[4]=1e431279
A[5]=c789d4f8  B[5]=5f901900  C[5]=0cae56c5  D[5]=e5983ca4
A[6]=eb304bf1  B[6]=3ffb84d5  C[6]=44c3c314  D[6]=3ccf3cea
A[7]=ab394973  B[7]=865a3825  C[7]=a05da04c  D[7]=c49874a2

Step 12: (r=26, s= 4)
A[0]=554ff22d  B[0]=514c427d  C[0]=17520739  D[0]=55b5573f
A[1]=b53af860  B[1]=6cc080fc  C[1]=3207d541  D[1]=6271a097
A[2]=4a2a063b  B[2]=0af792e6  C[2]=34854bcc  D[2]=420122cf
A[3]=3c917952  B[3]=3201e7d9  C[3]=e0680813  D[3]=88dbeeab
A[4]=6bccc398  B[4]=0bc919e9  C[4]=660e3525  D[4]=6b26ffb1
A[5]=437df14e  B[5]=e31e2753  C[5]=5f901900  D[5]=0cae56c5
A[6]=0ce93171  B[6]=c7acc12f  C[6]=3ffb84d5  D[6]=44c3c314
A[7]=2b378475  B[7]=ceace525  C[7]=865a3825  D[7]=a05da04c

Step 13: (r= 4, s=23)
A[0]=01f3ba9e  B[0]=54ff22d5  C[0]=514c427d  D[0]=17520739
A[1]=d0bf66cd  B[1]=53af860b  C[1]=6cc080fc  D[1]=3207d541
A[2]=bd367277  B[2]=a2a063b4  C[2]=0af792e6  D[2]=34854bcc
A[3]=1ae0f53c  B[3]=c9179523  C[3]=3201e7d9  D[3]=e0680813
A[4]=e30d612f  B[4]=bccc3986  C[4]=0bc919e9  D[4]=660e3525
A[5]=c6a7c370  B[5]=37df14e4  C[5]=e31e2753  D[5]=5f901900
A[6]=50f00f30  B[6]=ce931710  C[6]=c7acc12f  D[6]=3ffb84d5
A[7]=3e7269b3  B[7]=b3784752  C[7]=ceace525  D[7]=865a3825

Step 14: (r=23, s=11)
A[0]=12a4c698  B[0]=4f00f9dd  C[0]=54ff22d5  D[0]=514c427d
A[1]=5573841c  B[1]=66e85fb3  C[1]=53af860b  D[1]=6cc080fc
A[2]=d6fb4825  B[2]=3bde9b39  C[2]=a2a063b4  D[2]=0af792e6
A[3]=d0da4bbc  B[3]=9e0d707a  C[3]=c9179523  D[3]=3201e7d9
A[4]=eea010fd  B[4]=97f186b0  C[4]=bccc3986  D[4]=0bc919e9
A[5]=028ea5d4  B[5]=b86353e1  C[5]=37df14e4  D[5]=e31e2753
A[6]=e579568d  B[6]=98287807  C[6]=ce931710  D[6]=c7acc12f
A[7]=0a2e958c  B[7]=d99f3934  C[7]=b3784752  D[7]=ceace525
```

```
Step 15: (r=11, s=26)
A[0]=47bb2320  B[0]=2634c095  C[0]=4f00f9dd  D[0]=54ff22d5
A[1]=b8bd9f7a  B[1]=9c20e2ab  C[1]=66e85fb3  D[1]=53af860b
A[2]=2270c779  B[2]=da412eb7  C[2]=3bde9b39  D[2]=a2a063b4
A[3]=4df5f86d  B[3]=d25de686  C[3]=9e0d707a  D[3]=c9179523
A[4]=88cedd76  B[4]=0087ef75  C[4]=97f186b0  D[4]=bccc3986
A[5]=bb150bce  B[5]=752ea014  C[5]=b86353e1  D[5]=37df14e4
A[6]=3d527666  B[6]=cab46f2b  C[6]=98287807  D[6]=ce931710
A[7]=80736dbb  B[7]=74ac6051  C[7]=d99f3934  D[7]=b3784752

Step 16: (r=19, s=28)
A[0]=1d5a25a7  B[0]=19023dd9  C[0]=2634c095  D[0]=4f00f9dd
A[1]=3f83629c  B[1]=fbd5c5ec  C[1]=9c20e2ab  D[1]=66e85fb3
A[2]=a9dfa4b2  B[2]=3bc91386  C[2]=da412eb7  D[2]=3bde9b39
A[3]=d9500f34  B[3]=c36a6faf  C[3]=d25de686  D[3]=9e0d707a
A[4]=c2628898  B[4]=ebb44676  C[4]=0087ef75  D[4]=97f186b0
A[5]=2d2a8246  B[5]=5e75d8a8  C[5]=752ea014  D[5]=b86353e1
A[6]=cec3ef40  B[6]=b331ea93  C[6]=cab46f2b  D[6]=98287807
A[7]=a528f13e  B[7]=6ddc039b  C[7]=74ac6051  D[7]=d99f3934

Step 17: (r=28, s= 7)
A[0]=955f170a  B[0]=71d5a25a  C[0]=19023dd9  D[0]=2634c095
A[1]=2d8c5eb2  B[1]=c3f83629  C[1]=fbd5c5ec  D[1]=9c20e2ab
A[2]=77dd3642  B[2]=2a9dfa4b  C[2]=3bc91386  D[2]=da412eb7
A[3]=9c26886c  B[3]=4d9500f3  C[3]=c36a6faf  D[3]=d25de686
A[4]=98c46569  B[4]=8c262889  C[4]=ebb44676  D[4]=0087ef75
A[5]=51d84a70  B[5]=62d2a824  C[5]=5e75d8a8  D[5]=752ea014
A[6]=fb2679c0  B[6]=0cec3ef4  C[6]=b331ea93  D[6]=cab46f2b
A[7]=6f1ccc2a  B[7]=ea528f13  C[7]=6ddc039b  D[7]=74ac6051

Step 18: (r= 7, s=22)
A[0]=b5769f04  B[0]=af8b854a  C[0]=71d5a25a  D[0]=19023dd9
A[1]=c60edad0  B[1]=c62f5916  C[1]=c3f83629  D[1]=fbd5c5ec
A[2]=5177a43b  B[2]=ee9b213b  C[2]=2a9dfa4b  D[2]=3bc91386
A[3]=39fca5d3  B[3]=1344364e  C[3]=4d9500f3  D[3]=c36a6faf
A[4]=1692f6bf  B[4]=6232b4cc  C[4]=8c262889  D[4]=ebb44676
A[5]=866260fa  B[5]=ec253828  C[5]=62d2a824  D[5]=5e75d8a8
A[6]=46d6933b  B[6]=933ce07d  C[6]=0cec3ef4  D[6]=b331ea93
A[7]=127fe892  B[7]=8e661537  C[7]=ea528f13  D[7]=6ddc039b

Step 19: (r=22, s=19)
A[0]=b7c42e92  B[0]=c12d5da7  C[0]=af8b854a  D[0]=71d5a25a
A[1]=e04deb51  B[1]=b43183b6  C[1]=c62f5916  D[1]=c3f83629
A[2]=86673c69  B[2]=0ed45de9  C[2]=ee9b213b  D[2]=2a9dfa4b
A[3]=58d5ce04  B[3]=74ce7f29  C[3]=1344364e  D[3]=4d9500f3
A[4]=4de3efb6  B[4]=afc5a4bd  C[4]=6232b4cc  D[4]=8c262889
A[5]=8be6ef1a  B[5]=3ea19898  C[5]=ec253828  D[5]=62d2a824
A[6]=512d3a03  B[6]=ced1b5a4  C[6]=933ce07d  D[6]=0cec3ef4
```

```
A[7]=c8d15d1c  B[7]=24849ffa  C[7]=8e661537  D[7]=ea528f13

Step 20: (r=19, s=28)
A[0]=97bc4a6e  B[0]=7495be21  C[0]=c12d5da7  D[0]=af8b854a
A[1]=4baa1758  B[1]=5a8f026f  C[1]=b43183b6  D[1]=c62f5916
A[2]=efc18762  B[2]=e34c3339  C[2]=0ed45de9  D[2]=ee9b213b
A[3]=e9701e97  B[3]=7022c6ae  C[3]=74ce7f29  D[3]=1344364e
A[4]=c99dd513  B[4]=7db26f1f  C[4]=afc5a4bd  D[4]=6232b4cc
A[5]=7fa8fa25  B[5]=78d45f37  C[5]=3ea19898  D[5]=ec253828
A[6]=f3a4b35c  B[6]=d01a8969  C[6]=ced1b5a4  D[6]=933ce07d
A[7]=142be404  B[7]=e8e6468a  C[7]=24849ffa  D[7]=8e661537

Step 21: (r=28, s= 7)
A[0]=8a76f6dc  B[0]=e97bc4a6  C[0]=7495be21  D[0]=c12d5da7
A[1]=7fcbd4e8  B[1]=84baa175  C[1]=5a8f026f  D[1]=b43183b6
A[2]=d40c5427  B[2]=2efc1876  C[2]=e34c3339  D[2]=0ed45de9
A[3]=501fb1bd  B[3]=7e9701e9  C[3]=7022c6ae  D[3]=74ce7f29
A[4]=b4d36c77  B[4]=3c99dd51  C[4]=7db26f1f  D[4]=afc5a4bd
A[5]=e8e8abc7  B[5]=57fa8fa2  C[5]=78d45f37  D[5]=3ea19898
A[6]=2808470d  B[6]=cf3a4b35  C[6]=d01a8969  D[6]=ced1b5a4
A[7]=e08d0631  B[7]=4142be40  C[7]=e8e6468a  D[7]=24849ffa

Step 22: (r= 7, s=22)
A[0]=a91f5ab0  B[0]=3b7b6e45  C[0]=e97bc4a6  D[0]=7495be21
A[1]=45bc3ef0  B[1]=e5ea743f  C[1]=84baa175  D[1]=5a8f026f
A[2]=51ad85df  B[2]=062a13ea  C[2]=2efc1876  D[2]=e34c3339
A[3]=61dc4b65  B[3]=0fd8dea8  C[3]=7e9701e9  D[3]=7022c6ae
A[4]=74efd508  B[4]=69b63bda  C[4]=3c99dd51  D[4]=7db26f1f
A[5]=8e8df608  B[5]=7455e3f4  C[5]=57fa8fa2  D[5]=78d45f37
A[6]=68c31e40  B[6]=04238694  C[6]=cf3a4b35  D[6]=d01a8969
A[7]=b44655fa  B[7]=468318f0  C[7]=4142be40  D[7]=e8e6468a

Step 23: (r=22, s=19)
A[0]=4892c566  B[0]=ac2a47d6  C[0]=3b7b6e45  D[0]=e97bc4a6
A[1]=80644b33  B[1]=bc116f0f  C[1]=e5ea743f  D[1]=84baa175
A[2]=855b4586  B[2]=77d46b61  C[2]=062a13ea  D[2]=2efc1876
A[3]=f5b11304  B[3]=d9587712  C[3]=0fd8dea8  D[3]=7e9701e9
A[4]=9d1d3cd1  B[4]=421d3bf5  C[4]=69b63bda  D[4]=3c99dd51
A[5]=d6ea1331  B[5]=8223a37d  C[5]=7455e3f4  D[5]=57fa8fa2
A[6]=beb72e2a  B[6]=901a30c7  C[6]=04238694  D[6]=cf3a4b35
A[7]=6682b166  B[7]=7ead1195  C[7]=468318f0  D[7]=4142be40

Step 24: (r=15, s= 5)
A[0]=5023d5bc  B[0]=62b32449  C[0]=ac2a47d6  D[0]=3b7b6e45
A[1]=5a0461ba  B[1]=2599c032  C[1]=bc116f0f  D[1]=e5ea743f
A[2]=bea88f26  B[2]=a2c342ad  C[2]=77d46b61  D[2]=062a13ea
A[3]=c44249a3  B[3]=89827ad8  C[3]=d9587712  D[3]=0fd8dea8
A[4]=4312b3c3  B[4]=9e68ce8e  C[4]=421d3bf5  D[4]=69b63bda
A[5]=801de5df  B[5]=0998eb75  C[5]=8223a37d  D[5]=7455e3f4
```

```
A[6]=8dfab134  B[6]=97155f5b  C[6]=901a30c7  D[6]=04238694
A[7]=b2d9d314  B[7]=58b33341  C[7]=7ead1195  D[7]=468318f0

Step 25: (r= 5, s=29)
A[0]=2d653caa  B[0]=047ab78a  C[0]=62b32449  D[0]=ac2a47d6
A[1]=8fd7e21b  B[1]=408c374b  C[1]=2599c032  D[1]=bc116f0f
A[2]=adb4e230  B[2]=d511e4d7  C[2]=a2c342ad  D[2]=77d46b61
A[3]=98b72557  B[3]=88493478  C[3]=89827ad8  D[3]=d9587712
A[4]=825ab605  B[4]=62567868  C[4]=9e68ce8e  D[4]=421d3bf5
A[5]=7df673ac  B[5]=03bcbbf0  C[5]=0998eb75  D[5]=8223a37d
A[6]=7a635330  B[6]=bf562691  C[6]=97155f5b  D[6]=901a30c7
A[7]=5744c85a  B[7]=5b3a6296  C[7]=58b33341  D[7]=7ead1195

Step 26: (r=29, s= 9)
A[0]=9583c8e3  B[0]=45aca795  C[0]=047ab78a  D[0]=62b32449
A[1]=27b7f0ae  B[1]=71fafc43  C[1]=408c374b  D[1]=2599c032
A[2]=eaa531c3  B[2]=15b69c46  C[2]=d511e4d7  D[2]=a2c342ad
A[3]=255f23bc  B[3]=f316e4aa  C[3]=88493478  D[3]=89827ad8
A[4]=414bb90b  B[4]=b04b56c0  C[4]=62567868  D[4]=9e68ce8e
A[5]=03be8b96  B[5]=8fbece75  C[5]=03bcbbf0  D[5]=0998eb75
A[6]=12ff6719  B[6]=0f4c6a66  C[6]=bf562691  D[6]=97155f5b
A[7]=4a86ef48  B[7]=4ae8990b  C[7]=5b3a6296  D[7]=58b33341

Step 27: (r= 9, s=15)
A[0]=e7bd1a10  B[0]=0791c72b  C[0]=45aca795  D[0]=047ab78a
A[1]=2b163d2b  B[1]=6fe15c4f  C[1]=71fafc43  D[1]=408c374b
A[2]=0dcc139b  B[2]=4a6387d5  C[2]=15b69c46  D[2]=d511e4d7
A[3]=45141c61  B[3]=be47784a  C[3]=f316e4aa  D[3]=88493478
A[4]=0142396a  B[4]=97721682  C[4]=b04b56c0  D[4]=62567868
A[5]=112f1274  B[5]=7d172c07  C[5]=8fbece75  D[5]=03bcbbf0
A[6]=739109ec  B[6]=fece3225  C[6]=0f4c6a66  D[6]=bf562691
A[7]=a9c86688  B[7]=0dde9095  C[7]=4ae8990b  D[7]=5b3a6296

Step 28: (r=15, s= 5)
A[0]=4c3e7fc0  B[0]=8d0873de  C[0]=0791c72b  D[0]=45aca795
A[1]=611f7216  B[1]=1e95958b  C[1]=6fe15c4f  D[1]=71fafc43
A[2]=31095ddc  B[2]=09cd86e6  C[2]=4a6387d5  D[2]=15b69c46
A[3]=aa2d382e  B[3]=0e30a28a  C[3]=be47784a  D[3]=f316e4aa
A[4]=044e1b6e  B[4]=1cb500a1  C[4]=97721682  D[4]=b04b56c0
A[5]=500f482c  B[5]=893a0897  C[5]=7d172c07  D[5]=8fbece75
A[6]=b54e3be3  B[6]=84f639c8  C[6]=fece3225  D[6]=0f4c6a66
A[7]=70fdc33b  B[7]=334454e4  C[7]=0dde9095  D[7]=4ae8990b

Step 29: (r= 5, s=29)
A[0]=2add3d98  B[0]=87cff809  C[0]=8d0873de  D[0]=0791c72b
A[1]=b72d5b16  B[1]=23ee42cc  C[1]=1e95958b  D[1]=6fe15c4f
A[2]=d0ce2463  B[2]=212bbb86  C[2]=09cd86e6  D[2]=4a6387d5
A[3]=0b20b9dc  B[3]=45a705d5  C[3]=0e30a28a  D[3]=be47784a
A[4]=26d69697  B[4]=89c36dc0  C[4]=1cb500a1  D[4]=97721682
```

```
A[5]=1f1d8723  B[5]=01e9058a  C[5]=893a0897  D[5]=7d172c07
A[6]=e05105b1  B[6]=a9c77c76  C[6]=84f639c8  D[6]=fece3225
A[7]=d04f313b  B[7]=1fb8676e  C[7]=334454e4  D[7]=0dde9095

Step 30: (r=29, s= 9)
A[0]=73e26f5a  B[0]=055ba7b3  C[0]=87cff809  D[0]=8d0873de
A[1]=3fd421e4  B[1]=d6e5ab62  C[1]=23ee42cc  D[1]=1e95958b
A[2]=023871f4  B[2]=7a19c48c  C[2]=212bbb86  D[2]=09cd86e6
A[3]=f72e7c6b  B[3]=8164173b  C[3]=45a705d5  D[3]=0e30a28a
A[4]=0fc76af6  B[4]=e4dad2d2  C[4]=89c36dc0  D[4]=1cb500a1
A[5]=e69df435  B[5]=63e3b0e4  C[5]=01e9058a  D[5]=893a0897
A[6]=13e53206  B[6]=3c0a20b6  C[6]=a9c77c76  D[6]=84f639c8
A[7]=4e2c8c39  B[7]=7a09e627  C[7]=1fb8676e  D[7]=334454e4

Step 31: (r= 9, s=15)
A[0]=6be0df0a  B[0]=c4deb4e7  C[0]=055ba7b3  D[0]=87cff809
A[1]=9751970a  B[1]=a843c87f  C[1]=d6e5ab62  D[1]=23ee42cc
A[2]=9419ede6  B[2]=70e3e804  C[2]=7a19c48c  D[2]=212bbb86
A[3]=3eb026b4  B[3]=5cf8d7ee  C[3]=8164173b  D[3]=45a705d5
A[4]=55238944  B[4]=8ed5ec1f  C[4]=e4dad2d2  D[4]=89c36dc0
A[5]=20944678  B[5]=3be86bcd  C[5]=63e3b0e4  D[5]=01e9058a
A[6]=37bead40  B[6]=ca640c27  C[6]=3c0a20b6  D[6]=a9c77c76
A[7]=57aabe42  B[7]=5918729c  C[7]=7a09e627  D[7]=1fb8676e

Feed-Forward Step 0: (r=15, s= 5)
A[0]=b2e29108  B[0]=6f8535f0  C[0]=c4deb4e7  D[0]=055ba7b3
A[1]=b744ad9b  B[1]=cb854ba8  C[1]=a843c87f  D[1]=d6e5ab62
A[2]=2371a6f7  B[2]=f6f34a0c  C[2]=70e3e804  D[2]=7a19c48c
A[3]=e3a5d97f  B[3]=135a1f58  C[3]=5cf8d7ee  D[3]=8164173b
A[4]=cb5a4634  B[4]=c4a22a91  C[4]=8ed5ec1f  D[4]=e4dad2d2
A[5]=127da513  B[5]=233c104a  C[5]=3be86bcd  D[5]=63e3b0e4
A[6]=5e1b19a1  B[6]=56a01bdf  C[6]=ca640c27  D[6]=3c0a20b6
A[7]=76ec0964  B[7]=5f212bd5  C[7]=5918729c  D[7]=7a09e627

Feed-Forward Step 1: (r= 5, s=29)
A[0]=1a41c82a  B[0]=5c522116  C[0]=6f8535f0  D[0]=c4deb4e7
A[1]=344f17c3  B[1]=e895b376  C[1]=cb854ba8  D[1]=a843c87f
A[2]=f56bbc21  B[2]=6e34dee4  C[2]=f6f34a0c  D[2]=70e3e804
A[3]=963e3e97  B[3]=74bb2ffc  C[3]=135a1f58  D[3]=5cf8d7ee
A[4]=3f392b4e  B[4]=6b48c699  C[4]=c4a22a91  D[4]=8ed5ec1f
A[5]=4abb95fa  B[5]=4fb4a262  C[5]=233c104a  D[5]=3be86bcd
A[6]=dab43d9a  B[6]=c363342b  C[6]=56a01bdf  D[6]=ca640c27
A[7]=5f9370b2  B[7]=dd812c8e  C[7]=5f212bd5  D[7]=5918729c

Feed-Forward Step 2: (r=29, s= 9)
A[0]=dfc366f6  B[0]=43483905  C[0]=5c522116  D[0]=6f8535f0
A[1]=4d3a5ad1  B[1]=6689e2f8  C[1]=e895b376  D[1]=cb854ba8
A[2]=a7b67b07  B[2]=3ead7784  C[2]=6e34dee4  D[2]=f6f34a0c
A[3]=ec1617ba  B[3]=f2c7c7d2  C[3]=74bb2ffc  D[3]=135a1f58
```

```
A[4]=73d8a2b1  B[4]=c7e72569  C[4]=6b48c699  D[4]=c4a22a91
A[5]=c401cc1a  B[5]=495772bf  C[5]=4fb4a262  D[5]=233c104a
A[6]=eb21be09  B[6]=5b5687b3  C[6]=c363342b  D[6]=56a01bdf
A[7]=192be36f  B[7]=4bf26e16  C[7]=dd812c8e  D[7]=5f212bd5

Feed-Forward Step 3: (r= 9, s=15)
A[0]=0a6004de  B[0]=86cdedbf  C[0]=43483905  D[0]=5c522116
A[1]=3b8e8bee  B[1]=74b5a29a  C[1]=6689e2f8  D[1]=e895b376
A[2]=9ab65749  B[2]=6cf60f4f  C[2]=3ead7784  D[2]=6e34dee4
A[3]=04fb2470  B[3]=2c2f75d8  C[3]=f2c7c7d2  D[3]=74bb2ffc
A[4]=a083d2f2  B[4]=b14562e7  C[4]=c7e72569  D[4]=6b48c699
A[5]=2f95ae23  B[5]=03983588  C[5]=495772bf  D[5]=4fb4a262
A[6]=acf4ace8  B[6]=437c13d6  C[6]=5b5687b3  D[6]=c363342b
A[7]=ca4c65aa  B[7]=57c6de32  C[7]=4bf26e16  D[7]=dd812c8e
```

Compression Function Output

```
A[0]=0a6004de  B[0]=86cdedbf  C[0]=43483905  D[0]=5c522116
A[1]=3b8e8bee  B[1]=74b5a29a  C[1]=6689e2f8  D[1]=e895b376
A[2]=9ab65749  B[2]=6cf60f4f  C[2]=3ead7784  D[2]=6e34dee4
A[3]=04fb2470  B[3]=2c2f75d8  C[3]=f2c7c7d2  D[3]=74bb2ffc
A[4]=a083d2f2  B[4]=b14562e7  C[4]=c7e72569  D[4]=6b48c699
A[5]=2f95ae23  B[5]=03983588  C[5]=495772bf  D[5]=4fb4a262
A[6]=acf4ace8  B[6]=437c13d6  C[6]=5b5687b3  D[6]=c363342b
A[7]=ca4c65aa  B[7]=57c6de32  C[7]=4bf26e16  D[7]=dd812c8e
```

Final block

```
M[  0..  7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
```

```
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
y[168..175] =  249  239  118   96   69  105  140  102
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
```

```
             410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9]  =  eb0bb41f  48fdc914  2878d107  2878f754
             b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10]  =  c1212594  31ddbfaf  109f1c2f  f470194b
             f2fefa38  45605546  4be131dd  49b6ab73
Z[11]  =  31dda380  ebc40172  0965be3d  2931c405
             cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12]  =  531bd1c0  e3d1e8e0  1383050f  0c493408
             582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13]  =  3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
             3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14]  =  c06831dd  aabaa4f2  548d478b  3633fd1c
             121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15]  =  e0ed08ac  e999bef6  dec2dd50  c6e9cedc
             e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16]  =  fac6053a  3365cc9b  d8cd2733  0ecff131
             e79c1864  52c1ad3f  a8e4571c  476eb892
Z[17]  =  a4895b77  bdcc4234  c761389f  f58c0a74
             f2ef0d11  ff2100df  6f809080  06f8f908
Z[18]  =  2d4cd2b4  b2794d87  21f9de07  1e7de183
             f90806f8  66ca9936  3c1bc3e5  9a1565eb
Z[19]  =  90806f80  01befe42  b0bb4f45  b7b3484d
             d1d52e2b  476eb892  547fab81  2812d7ee
Z[20]  =  c84037c0  e4201be0  0619f9e7  3eb8c148
             fe4201be  fc84037c  aefd5103  c9fe3602
Z[21]  =  95ba6a46  52c1ad3f  e2621d9e  e1831e7d
             f1310ecf  f9e70619  59b9a647  d8cd2733
Z[22]  =  3c1bc3e5  923e6dc2  563da9c3  fc84037c
             61909e70  e1831e7d  029dfd63  e4ff1b01
Z[23]  =  0a74f58c  b19a4e66  d63029d0  c4c43b3c
             2575da8b  e1831e7d  58daa726  f3ce0c32
Z[24]  =  a02e5fd2  1a22e5de  d63029d0  52c1ad3f
             4e66b19a  e95a16a6  69679699  f4ad0b53
Z[25]  =  e6bd1943  57fba805  30c8cf38  30c8cf38
             aaa2555e  bb2f44d1  00dfff21  cadd3523
Z[26]  =  b4374bc9  3c1bc3e5  1409ebf7  f2100df0
             f0520fae  53a0ac60  5b77a489  58daa726
Z[27]  =  3c1bc3e5  e79c1864  0b53f4ad  31a7ce59
             c4c43b3c  f1310ecf  ba5045b0  23b7dc49
Z[28]  =  642d9bd3  de0721f9  1785e87b  0ecff131
             6a4695ba  d2b42d4c  4aeab516  c682397e
Z[29]  =  4ca8b358  ce5931a7  97786888  0df0f210
             4aeab516  d0f62f0a  67a99857  6b2594db
Z[30]  =  b3584ca8  993666ca  65eb9a15  4155beab
             15c7ea39  4a0bb5f5  3523cadd  fd63029d
Z[31]  =  da8b2575  e4ff1b01  d7ee2812  bb2f44d1
             e4201be0  aaa2555e  52c1ad3f  e3411cbf
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a4895b77  bdcc4234  c761389f  f58c0a74
        f2ef0d11  ff2100df  6f809080  06f8f908
W[17] = 2d4cd2b4  b2794d87  21f9de07  1e7de183
        f90806f8  66ca9936  3c1bc3e5  9a1565eb
W[18] = 0a74f58c  b19a4e66  d63029d0  c4c43b3c
        2575da8b  e1831e7d  58daa726  f3ce0c32
W[19] = c84037c0  e4201be0  0619f9e7  3eb8c148
        fe4201be  fc84037c  aefd5103  c9fe3602
W[20] = 3c1bc3e5  923e6dc2  563da9c3  fc84037c
        61909e70  e1831e7d  029dfd63  e4ff1b01
W[21] = 95ba6a46  52c1ad3f  e2621d9e  e1831e7d
        f1310ecf  f9e70619  59b9a647  d8cd2733
W[22] = fac6053a  3365cc9b  d8cd2733  0ecff131
        e79c1864  52c1ad3f  a8e4571c  476eb892
W[23] = 90806f80  01befe42  b0bb4f45  b7b3484d
        d1d52e2b  476eb892  547fab81  2812d7ee
W[24] = b3584ca8  993666ca  65eb9a15  4155beab
```

```
        15c7ea39  4a0bb5f5  3523cadd  fd63029d
W[25] = a02e5fd2  1a22e5de  d63029d0  52c1ad3f
        4e66b19a  e95a16a6  69679699  f4ad0b53
W[26] = e6bd1943  57fba805  30c8cf38  30c8cf38
        aaa2555e  bb2f44d1  00dfff21  cadd3523
W[27] = da8b2575  e4ff1b01  d7ee2812  bb2f44d1
        e4201be0  aaa2555e  52c1ad3f  e3411cbf
W[28] = 3c1bc3e5  e79c1864  0b53f4ad  31a7ce59
        c4c43b3c  f1310ecf  ba5045b0  23b7dc49
W[29] = 4ca8b358  ce5931a7  97786888  0df0f210
        4aeab516  d0f62f0a  67a99857  6b2594db
W[30] = 642d9bd3  de0721f9  1785e87b  0ecff131
        6a4695ba  d2b42d4c  4aeab516  c682397e
W[31] = b4374bc9  3c1bc3e5  1409ebf7  f2100df0
        f0520fae  53a0ac60  5b77a489  58daa726
```

Feistel Steps

```
IV :
A[0]=0a6004de  B[0]=86cdedbf  C[0]=43483905  D[0]=5c522116
A[1]=3b8e8bee  B[1]=74b5a29a  C[1]=6689e2f8  D[1]=e895b376
A[2]=9ab65749  B[2]=6cf60f4f  C[2]=3ead7784  D[2]=6e34dee4
A[3]=04fb2470  B[3]=2c2f75d8  C[3]=f2c7c7d2  D[3]=74bb2ffc
A[4]=a083d2f2  B[4]=b14562e7  C[4]=c7e72569  D[4]=6b48c699
A[5]=2f95ae23  B[5]=03983588  C[5]=495772bf  D[5]=4fb4a262
A[6]=acf4ace8  B[6]=437c13d6  C[6]=5b5687b3  D[6]=c363342b
A[7]=ca4c65aa  B[7]=57c6de32  C[7]=4bf26e16  D[7]=dd812c8e

IV XOR M :
A[0]=0a6000de  B[0]=86cdedbf  C[0]=43483905  D[0]=5c522116
A[1]=3b8e8bee  B[1]=74b5a29a  C[1]=6689e2f8  D[1]=e895b376
A[2]=9ab65749  B[2]=6cf60f4f  C[2]=3ead7784  D[2]=6e34dee4
A[3]=04fb2470  B[3]=2c2f75d8  C[3]=f2c7c7d2  D[3]=74bb2ffc
A[4]=a083d2f2  B[4]=b14562e7  C[4]=c7e72569  D[4]=6b48c699
A[5]=2f95ae23  B[5]=03983588  C[5]=495772bf  D[5]=4fb4a262
A[6]=acf4ace8  B[6]=437c13d6  C[6]=5b5687b3  D[6]=c363342b
A[7]=ca4c65aa  B[7]=57c6de32  C[7]=4bf26e16  D[7]=dd812c8e

Step  0: (r= 3, s=20)
A[0]=6bc92769  B[0]=530006f0  C[0]=86cdedbf  D[0]=43483905
A[1]=26079b9a  B[1]=dc745f71  C[1]=74b5a29a  D[1]=6689e2f8
A[2]=42019aa0  B[2]=d5b2ba4c  C[2]=6cf60f4f  D[2]=3ead7784
A[3]=1218a47a  B[3]=27d92380  C[3]=2c2f75d8  D[3]=f2c7c7d2
A[4]=7c1d195b  B[4]=041e9795  C[4]=b14562e7  D[4]=c7e72569
A[5]=a24a2946  B[5]=7cad7119  C[5]=03983588  D[5]=495772bf
A[6]=05a0b88d  B[6]=67a56745  C[6]=437c13d6  D[6]=5b5687b3
A[7]=e0ca79df  B[7]=52632d56  C[7]=57c6de32  D[7]=4bf26e16

Step  1: (r=20, s=14)
```

```
A[0]=1f8bb292  B[0]=7696bc92  C[0]=530006f0  D[0]=86cdedbf
A[1]=65e6a5ab  B[1]=b9a26079  C[1]=dc745f71  D[1]=74b5a29a
A[2]=6a68d257  B[2]=aa042019  C[2]=d5b2ba4c  D[2]=6cf60f4f
A[3]=c8b01b2e  B[3]=47a1218a  C[3]=27d92380  D[3]=2c2f75d8
A[4]=5adbe8d7  B[4]=95b7c1d1  C[4]=041e9795  D[4]=b14562e7
A[5]=4e629807  B[5]=946a24a2  C[5]=7cad7119  D[5]=03983588
A[6]=3fef9fa0  B[6]=88d05a0b  C[6]=67a56745  D[6]=437c13d6
A[7]=a1670dfb  B[7]=9dfe0ca7  C[7]=52632d56  D[7]=57c6de32

Step  2: (r=14, s=27)
A[0]=fce55d91  B[0]=eca487e2  C[0]=7696bc92  D[0]=530006f0
A[1]=68ade78e  B[1]=a96ad979  C[1]=b9a26079  D[1]=dc745f71
A[2]=107b9657  B[2]=3495da9a  C[2]=aa042019  D[2]=d5b2ba4c
A[3]=c4b16b0e  B[3]=06cbb22c  C[3]=47a1218a  D[3]=27d92380
A[4]=aaf24ca3  B[4]=fa35d6b6  C[4]=95b7c1d1  D[4]=041e9795
A[5]=0ef06d29  B[5]=a601d398  C[5]=946a24a2  D[5]=7cad7119
A[6]=a311382b  B[6]=e7e80ffb  C[6]=88d05a0b  D[6]=67a56745
A[7]=a6491e5e  B[7]=c37ee859  C[7]=9dfe0ca7  D[7]=52632d56

Step  3: (r=27, s= 3)
A[0]=220bc959  B[0]=8fe72aec  C[0]=eca487e2  D[0]=7696bc92
A[1]=668a8d44  B[1]=73456f3c  C[1]=a96ad979  D[1]=b9a26079
A[2]=566b0b7c  B[2]=b883dcb2  C[2]=3495da9a  D[2]=aa042019
A[3]=cc8baefb  B[3]=76258b58  C[3]=06cbb22c  D[3]=47a1218a
A[4]=129a456a  B[4]=1d579265  C[4]=fa35d6b6  D[4]=95b7c1d1
A[5]=de085a2a  B[5]=48778369  C[5]=a601d398  D[5]=946a24a2
A[6]=f4afd950  B[6]=5d1889c1  C[6]=e7e80ffb  D[6]=88d05a0b
A[7]=9b81e23d  B[7]=f53248f2  C[7]=c37ee859  D[7]=9dfe0ca7

Step  4: (r= 3, s=20)
A[0]=3138af46  B[0]=105e4ac9  C[0]=8fe72aec  D[0]=eca487e2
A[1]=0051800f  B[1]=34546a23  C[1]=73456f3c  D[1]=a96ad979
A[2]=3c9d743f  B[2]=b3585be2  C[2]=b883dcb2  D[2]=3495da9a
A[3]=85c4d021  B[3]=645d77de  C[3]=76258b58  D[3]=06cbb22c
A[4]=828f405d  B[4]=94d22b50  C[4]=1d579265  D[4]=fa35d6b6
A[5]=a62cbf31  B[5]=f042d156  C[5]=48778369  D[5]=a601d398
A[6]=7e72af15  B[6]=a57eca87  C[6]=5d1889c1  D[6]=e7e80ffb
A[7]=99675b26  B[7]=dc0f11ec  C[7]=f53248f2  D[7]=c37ee859

Step  5: (r=20, s=14)
A[0]=06a9f979  B[0]=f463138a  C[0]=105e4ac9  D[0]=8fe72aec
A[1]=81d89d09  B[1]=00f00518  C[1]=34546a23  D[1]=73456f3c
A[2]=c85aa483  B[2]=43f3c9d7  C[2]=b3585be2  D[2]=b883dcb2
A[3]=68a3dcf8  B[3]=02185c4d  C[3]=645d77de  D[3]=76258b58
A[4]=aaacfb63  B[4]=05d828f4  C[4]=94d22b50  D[4]=1d579265
A[5]=4d6fc1d0  B[5]=f31a62cb  C[5]=f042d156  D[5]=48778369
A[6]=1a1c6ccd  B[6]=f157e72a  C[6]=a57eca87  D[6]=5d1889c1
A[7]=cbcb74bb  B[7]=b2699675  C[7]=dc0f11ec  D[7]=f53248f2
```

```
Step  6: (r=14, s=27)
A[0]=88c2a20b  B[0]=7e5e41aa  C[0]=f463138a  D[0]=105e4ac9
A[1]=b775da5d  B[1]=27426076  C[1]=00f00518  D[1]=34546a23
A[2]=b407e29c  B[2]=a920f216  C[2]=43f3c9d7  D[2]=b3585be2
A[3]=bc415bcc  B[3]=f73e1a28  C[3]=02185c4d  D[3]=645d77de
A[4]=0dd8b949  B[4]=3ed8eaab  C[4]=05d828f4  D[4]=94d22b50
A[5]=73515265  B[5]=f074135b  C[5]=f31a62cb  D[5]=f042d156
A[6]=e184a207  B[6]=1b334687  C[6]=f157e72a  D[6]=a57eca87
A[7]=0bed2b8f  B[7]=dd2ef2f2  C[7]=b2699675  D[7]=dc0f11ec

Step  7: (r=27, s= 3)
A[0]=551b976b  B[0]=5c461510  C[0]=7e5e41aa  D[0]=f463138a
A[1]=c1d995eb  B[1]=edbbaed2  C[1]=27426076  D[1]=00f00518
A[2]=9f2f9099  B[2]=e5a03f14  C[2]=a920f216  D[2]=43f3c9d7
A[3]=084e4013  B[3]=65e20ade  C[3]=f73e1a28  D[3]=02185c4d
A[4]=a82d0d97  B[4]=486ec5ca  C[4]=3ed8eaab  D[4]=05d828f4
A[5]=d30cd1a2  B[5]=2b9a8a93  C[5]=f074135b  D[5]=f31a62cb
A[6]=9492df88  B[6]=3f0c2510  C[6]=1b334687  D[6]=f157e72a
A[7]=827803bb  B[7]=785f695c  C[7]=dd2ef2f2  D[7]=b2699675

Step  8: (r=26, s= 4)
A[0]=e86e81bc  B[0]=ad546e5d  C[0]=5c461510  D[0]=7e5e41aa
A[1]=cfaefcaa  B[1]=af076657  C[1]=edbbaed2  D[1]=27426076
A[2]=c992ccdc  B[2]=667cbe42  C[2]=e5a03f14  D[2]=a920f216
A[3]=6dc1147e  B[3]=4c213900  C[3]=65e20ade  D[3]=f73e1a28
A[4]=669f2e56  B[4]=5ea0b436  C[4]=486ec5ca  D[4]=3ed8eaab
A[5]=5abd79f2  B[5]=8b4c3346  C[5]=2b9a8a93  D[5]=f074135b
A[6]=400d3e83  B[6]=22524b7e  C[6]=3f0c2510  D[6]=1b334687
A[7]=a15a267d  B[7]=ee09e00e  C[7]=785f695c  D[7]=dd2ef2f2

Step  9: (r= 4, s=23)
A[0]=3c630dc8  B[0]=86e81bce  C[0]=ad546e5d  D[0]=5c461510
A[1]=f97256ca  B[1]=faefcaac  C[1]=af076657  D[1]=edbbaed2
A[2]=50737785  B[2]=992ccdcc  C[2]=667cbe42  D[2]=e5a03f14
A[3]=51a61428  B[3]=dc1147e6  C[3]=4c213900  D[3]=65e20ade
A[4]=ff023388  B[4]=69f2e566  C[4]=5ea0b436  D[4]=486ec5ca
A[5]=05aa04da  B[5]=abd79f25  C[5]=8b4c3346  D[5]=2b9a8a93
A[6]=43031731  B[6]=00d3e834  C[6]=22524b7e  D[6]=3f0c2510
A[7]=4a510de3  B[7]=15a267da  C[7]=ee09e00e  D[7]=785f695c

Step 10: (r=23, s=11)
A[0]=a43a922c  B[0]=e41e3186  C[0]=86e81bce  D[0]=ad546e5d
A[1]=4074000a  B[1]=657cb92b  C[1]=faefcaac  D[1]=af076657
A[2]=ed921e7c  B[2]=c2a839bb  C[2]=992ccdcc  D[2]=667cbe42
A[3]=27dfb78a  B[3]=1428d30a  C[3]=dc1147e6  D[3]=4c213900
A[4]=f775435b  B[4]=c47f8119  C[4]=69f2e566  D[4]=5ea0b436
A[5]=309dd649  B[5]=6d02d502  C[5]=abd79f25  D[5]=8b4c3346
A[6]=96cf8617  B[6]=98a1818b  C[6]=00d3e834  D[6]=22524b7e
A[7]=9d3118eb  B[7]=f1a52886  C[7]=15a267da  D[7]=ee09e00e
```

```
Step 11: (r=11, s=26)
A[0]=de2da5ca  B[0]=d4916521  C[0]=e41e3186  D[0]=86e81bce
A[1]=91b11ef2  B[1]=a0005203  C[1]=657cb92b  D[1]=faefcaac
A[2]=5082a693  B[2]=90f3e76c  C[2]=c2a839bb  D[2]=992ccdcc
A[3]=667aa14b  B[3]=fdbc513e  C[3]=1428d30a  D[3]=dc1147e6
A[4]=b243f235  B[4]=aa1adfbb  C[4]=c47f8119  D[4]=69f2e566
A[5]=e48f6757  B[5]=eeb24984  C[5]=6d02d502  D[5]=abd79f25
A[6]=051d3f19  B[6]=7c30bcb6  C[6]=98a1818b  D[6]=00d3e834
A[7]=87957369  B[7]=88c75ce9  C[7]=f1a52886  D[7]=15a267da

Step 12: (r=26, s= 4)
A[0]=2b561b6f  B[0]=2b78b697  C[0]=d4916521  D[0]=e41e3186
A[1]=7d5394d5  B[1]=ca46c47b  C[1]=a0005203  D[1]=657cb92b
A[2]=521e536e  B[2]=4d420a9a  C[2]=90f3e76c  D[2]=c2a839bb
A[3]=d9730ee1  B[3]=2d99ea85  C[3]=fdbc513e  D[3]=1428d30a
A[4]=b76d1a29  B[4]=d6c90fc8  C[4]=aa1adfbb  D[4]=c47f8119
A[5]=cb0746ed  B[5]=5f923d9d  C[5]=eeb24984  D[5]=6d02d502
A[6]=820e7abe  B[6]=641474fc  C[6]=7c30bcb6  D[6]=98a1818b
A[7]=1542ddb2  B[7]=a61e55cd  C[7]=88c75ce9  D[7]=f1a52886

Step 13: (r= 4, s=23)
A[0]=638cba6d  B[0]=b561b6f2  C[0]=2b78b697  D[0]=d4916521
A[1]=a9c33586  B[1]=d5394d57  C[1]=ca46c47b  D[1]=a0005203
A[2]=013fd8a4  B[2]=21e536e5  C[2]=4d420a9a  D[2]=90f3e76c
A[3]=074806d9  B[3]=9730ee1d  C[3]=2d99ea85  D[3]=fdbc513e
A[4]=5dc423b2  B[4]=76d1a29b  C[4]=d6c90fc8  D[4]=aa1adfbb
A[5]=1438a32f  B[5]=b0746edc  C[5]=5f923d9d  D[5]=eeb24984
A[6]=d2fafd3f  B[6]=20e7abe8  C[6]=641474fc  D[6]=7c30bcb6
A[7]=a5dbd68e  B[7]=542ddb21  C[7]=a61e55cd  D[7]=88c75ce9

Step 14: (r=23, s=11)
A[0]=216053b3  B[0]=36b1c65d  C[0]=b561b6f2  D[0]=2b78b697
A[1]=aaa1ca57  B[1]=c354e19a  C[1]=d5394d57  D[1]=ca46c47b
A[2]=687c1968  B[2]=52009fec  C[2]=21e536e5  D[2]=4d420a9a
A[3]=03f819db  B[3]=6c83a403  C[3]=9730ee1d  D[3]=2d99ea85
A[4]=447013a1  B[4]=d92ee211  C[4]=76d1a29b  D[4]=d6c90fc8
A[5]=6873da2e  B[5]=978a1c51  C[5]=b0746edc  D[5]=5f923d9d
A[6]=0ab95ae2  B[6]=9fe97d7e  C[6]=20e7abe8  D[6]=641474fc
A[7]=25b11211  B[7]=4752edeb  C[7]=542ddb21  D[7]=a61e55cd

Step 15: (r=11, s=26)
A[0]=1d221520  B[0]=029d990b  C[0]=36b1c65d  D[0]=b561b6f2
A[1]=afb2400e  B[1]=0e52bd55  C[1]=c354e19a  D[1]=d5394d57
A[2]=0edfde1d  B[2]=e0cb4343  C[2]=52009fec  D[2]=21e536e5
A[3]=7a3e837b  B[3]=c0ced81f  C[3]=6c83a403  D[3]=9730ee1d
A[4]=2792c518  B[4]=809d0a23  C[4]=d92ee211  D[4]=76d1a29b
A[5]=c788875f  B[5]=9ed17343  C[5]=978a1c51  D[5]=b0746edc
A[6]=27378f0f  B[6]=cad71055  C[6]=9fe97d7e  D[6]=20e7abe8
```

```
A[7]=e0737089  B[7]=8890892d  C[7]=4752edeb  D[7]=542ddb21

Step 16: (r=19, s=28)
A[0]=683d4bee  B[0]=a900e910  C[0]=029d990b  D[0]=36b1c65d
A[1]=a716ac21  B[1]=00757d92  C[1]=0e52bd55  D[1]=c354e19a
A[2]=6f7ced2a  B[2]=f0e876fe  C[2]=e0cb4343  D[2]=52009fec
A[3]=bdfd40c8  B[3]=1bdbd1f4  C[3]=c0ced81f  D[3]=6c83a403
A[4]=0f26095e  B[4]=28c13c96  C[4]=809d0a23  D[4]=d92ee211
A[5]=0d22b545  B[5]=3afe3c44  C[5]=9ed17343  D[5]=978a1c51
A[6]=57037e68  B[6]=787939bc  C[6]=cad71055  D[6]=9fe97d7e
A[7]=c69cafd5  B[7]=844f039b  C[7]=8890892d  D[7]=4752edeb

Step 17: (r=28, s= 7)
A[0]=e6b0d819  B[0]=e683d4be  C[0]=a900e910  D[0]=029d990b
A[1]=9d160ecb  B[1]=1a716ac2  C[1]=00757d92  D[1]=0e52bd55
A[2]=597603e8  B[2]=a6f7ced2  C[2]=f0e876fe  D[2]=e0cb4343
A[3]=892099b4  B[3]=8bdfd40c  C[3]=1bdbd1f4  D[3]=c0ced81f
A[4]=ed69d813  B[4]=e0f26095  C[4]=28c13c96  D[4]=809d0a23
A[5]=007fb1c9  B[5]=50d22b54  C[5]=3afe3c44  D[5]=9ed17343
A[6]=4e2f30ef  B[6]=857037e6  C[6]=787939bc  D[6]=cad71055
A[7]=0afdf30a  B[7]=5c69cafd  C[7]=844f039b  D[7]=8890892d

Step 18: (r= 7, s=22)
A[0]=6af8a9e4  B[0]=586c0cf3  C[0]=e683d4be  D[0]=a900e910
A[1]=fb0e8f48  B[1]=8b0765ce  C[1]=1a716ac2  D[1]=00757d92
A[2]=3a2ee2f8  B[2]=bb01f42c  C[2]=a6f7ced2  D[2]=f0e876fe
A[3]=9cb465ae  B[3]=904cda44  C[3]=8bdfd40c  D[3]=1bdbd1f4
A[4]=e12e9716  B[4]=b4ec09f6  C[4]=e0f26095  D[4]=28c13c96
A[5]=7c30bddb  B[5]=3fd8e480  C[5]=50d22b54  D[5]=3afe3c44
A[6]=e75d6e4a  B[6]=179877a7  C[6]=857037e6  D[6]=787939bc
A[7]=566e3f88  B[7]=7ef98505  C[7]=5c69cafd  D[7]=844f039b

Step 19: (r=22, s=19)
A[0]=b40a3908  B[0]=791abe2a  C[0]=586c0cf3  D[0]=e683d4be
A[1]=70c28c96  B[1]=d23ec3a3  C[1]=8b0765ce  D[1]=1a716ac2
A[2]=7b3785fd  B[2]=be0e8bb8  C[2]=bb01f42c  D[2]=a6f7ced2
A[3]=fc1d0ab2  B[3]=6ba72d19  C[3]=904cda44  D[3]=8bdfd40c
A[4]=7878fe26  B[4]=c5b84ba5  C[4]=b4ec09f6  D[4]=e0f26095
A[5]=0462664a  B[5]=76df0c2f  C[5]=3fd8e480  D[5]=50d22b54
A[6]=d1380130  B[6]=92b9d75b  C[6]=179877a7  D[6]=857037e6
A[7]=643c92d0  B[7]=e2159b8f  C[7]=7ef98505  D[7]=5c69cafd

Step 20: (r=19, s=28)
A[0]=3e5e2360  B[0]=c845a051  C[0]=791abe2a  D[0]=586c0cf3
A[1]=70310a31  B[1]=64b38614  C[1]=d23ec3a3  D[1]=8b0765ce
A[2]=711bb0cd  B[2]=2febd9bc  C[2]=be0e8bb8  D[2]=bb01f42c
A[3]=b7f2e7d5  B[3]=5597e0e8  C[3]=6ba72d19  D[3]=904cda44
A[4]=e5c7d7bd  B[4]=f133c3c7  C[4]=c5b84ba5  D[4]=b4ec09f6
A[5]=a7c6bea4  B[5]=32502313  C[5]=76df0c2f  D[5]=3fd8e480
```

```
A[6]=583f8aab  B[6]=098689c0  C[6]=92b9d75b  D[6]=179877a7
A[7]=4400f158  B[7]=968321e4  C[7]=e2159b8f  D[7]=7ef98505

Step 21: (r=28, s= 7)
A[0]=199e87bf  B[0]=03e5e236  C[0]=c845a051  D[0]=791abe2a
A[1]=59c9cda3  B[1]=170310a3  C[1]=64b38614  D[1]=d23ec3a3
A[2]=3bbba5a4  B[2]=d711bb0c  C[2]=2febd9bc  D[2]=be0e8bb8
A[3]=daf25e17  B[3]=5b7f2e7d  C[3]=5597e0e8  D[3]=6ba72d19
A[4]=9df22def  B[4]=de5c7d7b  C[4]=f133c3c7  D[4]=c5b84ba5
A[5]=cf4c6f4d  B[5]=4a7c6bea  C[5]=32502313  D[5]=76df0c2f
A[6]=e7315a40  B[6]=b583f8aa  C[6]=098689c0  D[6]=92b9d75b
A[7]=2eab6df8  B[7]=84400f15  C[7]=968321e4  D[7]=e2159b8f

Step 22: (r= 7, s=22)
A[0]=bc9665b0  B[0]=cf43df8c  C[0]=03e5e236  D[0]=c845a051
A[1]=d103ea78  B[1]=e4e6d1ac  C[1]=170310a3  D[1]=64b38614
A[2]=cc2d4cc2  B[2]=ddd2d21d  C[2]=d711bb0c  D[2]=2febd9bc
A[3]=2b0c9371  B[3]=792f0bed  C[3]=5b7f2e7d  D[3]=5597e0e8
A[4]=f751bda1  B[4]=f916f7ce  C[4]=de5c7d7b  D[4]=f133c3c7
A[5]=0c17d166  B[5]=a637a6e7  C[5]=4a7c6bea  D[5]=32502313
A[6]=b2df1a2d  B[6]=98ad2073  C[6]=b583f8aa  D[6]=098689c0
A[7]=54afe16c  B[7]=55b6fc17  C[7]=84400f15  D[7]=968321e4

Step 23: (r=22, s=19)
A[0]=24ad18de  B[0]=6c2f2599  C[0]=cf43df8c  D[0]=03e5e236
A[1]=0174e1a6  B[1]=9e3440fa  C[1]=e4e6d1ac  D[1]=170310a3
A[2]=a3daa58e  B[2]=30b30b53  C[2]=ddd2d21d  D[2]=d711bb0c
A[3]=00a96fc9  B[3]=dc4ac324  C[3]=792f0bed  D[3]=5b7f2e7d
A[4]=eb1d3888  B[4]=687dd46f  C[4]=f916f7ce  D[4]=de5c7d7b
A[5]=9a9080af  B[5]=598305f4  C[5]=a637a6e7  D[5]=4a7c6bea
A[6]=9c137ffe  B[6]=8b6cb7c6  C[6]=98ad2073  D[6]=b583f8aa
A[7]=13835d0b  B[7]=5b152bf8  C[7]=55b6fc17  D[7]=84400f15

Step 24: (r=15, s= 5)
A[0]=4691cf8e  B[0]=8c6f1256  C[0]=6c2f2599  D[0]=cf43df8c
A[1]=2a681548  B[1]=70d300ba  C[1]=9e3440fa  D[1]=e4e6d1ac
A[2]=e9d986eb  B[2]=52c751ed  C[2]=30b30b53  D[2]=ddd2d21d
A[3]=0f2d5b6f  B[3]=b7e48054  C[3]=dc4ac324  D[3]=792f0bed
A[4]=c8dfad95  B[4]=9c44758e  C[4]=687dd46f  D[4]=f916f7ce
A[5]=c22d8e08  B[5]=4057cd48  C[5]=598305f4  D[5]=a637a6e7
A[6]=1904f38f  B[6]=bfff4e09  C[6]=8b6cb7c6  D[6]=98ad2073
A[7]=db16a7e4  B[7]=ae8589c1  C[7]=5b152bf8  D[7]=55b6fc17

Step 25: (r= 5, s=29)
A[0]=eea509ab  B[0]=d239f1c8  C[0]=8c6f1256  D[0]=6c2f2599
A[1]=7c172ce9  B[1]=4d02a905  C[1]=70d300ba  D[1]=9e3440fa
A[2]=92d6b284  B[2]=3b30dd7d  C[2]=52c751ed  D[2]=30b30b53
A[3]=616d9033  B[3]=e5ab6de1  C[3]=b7e48054  D[3]=dc4ac324
A[4]=fe9ab5cd  B[4]=1bf5b2b9  C[4]=9c44758e  D[4]=687dd46f
```

```
A[5]=9ff8260c  B[5]=45b1c118  C[5]=4057cd48  D[5]=598305f4
A[6]=cfa5d263  B[6]=209e71e3  C[6]=bfff4e09  D[6]=8b6cb7c6
A[7]=a03ef340  B[7]=62d4fc9b  C[7]=ae8589c1  D[7]=5b152bf8

Step 26: (r=29, s= 9)
A[0]=c2ad4e92  B[0]=7dd4a135  C[0]=d239f1c8  D[0]=8c6f1256
A[1]=5e16ded1  B[1]=2f82e59d  C[1]=4d02a905  D[1]=70d300ba
A[2]=af56f628  B[2]=925ad650  C[2]=3b30dd7d  D[2]=52c751ed
A[3]=38f8d8c2  B[3]=6c2db206  C[3]=e5ab6de1  D[3]=b7e48054
A[4]=56626261  B[4]=bfd356b9  C[4]=1bf5b2b9  D[4]=9c44758e
A[5]=6682f104  B[5]=93ff04c1  C[5]=45b1c118  D[5]=4057cd48
A[6]=85a98b17  B[6]=79f4ba4c  C[6]=209e71e3  D[6]=bfff4e09
A[7]=8e87d9de  B[7]=1407de68  C[7]=62d4fc9b  D[7]=ae8589c1

Step 27: (r= 9, s=15)
A[0]=39569e73  B[0]=5a9d2585  C[0]=7dd4a135  D[0]=d239f1c8
A[1]=868a3b37  B[1]=2dbda2bc  C[1]=2f82e59d  D[1]=4d02a905
A[2]=7fc08d9f  B[2]=adec515e  C[2]=925ad650  D[2]=3b30dd7d
A[3]=ccd7ed3c  B[3]=f1b18471  C[3]=6c2db206  D[3]=e5ab6de1
A[4]=8cb0f5a3  B[4]=c4c4c2ac  C[4]=bfd356b9  D[4]=1bf5b2b9
A[5]=bf1d1a12  B[5]=05e208cd  C[5]=93ff04c1  D[5]=45b1c118
A[6]=a9026b99  B[6]=53162f0b  C[6]=79f4ba4c  D[6]=209e71e3
A[7]=43167f80  B[7]=0fb3bd1d  C[7]=1407de68  D[7]=62d4fc9b

Step 28: (r=15, s= 5)
A[0]=22e71f96  B[0]=4f399cab  C[0]=5a9d2585  D[0]=7dd4a135
A[1]=d4664177  B[1]=1d9bc345  C[1]=2dbda2bc  D[1]=2f82e59d
A[2]=c053576b  B[2]=46cfbfe0  C[2]=adec515e  D[2]=925ad650
A[3]=c7ebcda0  B[3]=f69e666b  C[3]=f1b18471  D[3]=6c2db206
A[4]=3e61f35b  B[4]=7ad1c658  C[4]=c4c4c2ac  D[4]=bfd356b9
A[5]=570cdb71  B[5]=8d095f8e  C[5]=05e208cd  D[5]=93ff04c1
A[6]=c05c7515  B[6]=35ccd481  C[6]=53162f0b  D[6]=79f4ba4c
A[7]=ea67d212  B[7]=3fc0218b  C[7]=0fb3bd1d  D[7]=1407de68

Step 29: (r= 5, s=29)
A[0]=8d123bba  B[0]=5ce3f2c4  C[0]=4f399cab  D[0]=5a9d2585
A[1]=20ed2f6f  B[1]=8cc82efa  C[1]=1d9bc345  D[1]=2dbda2bc
A[2]=bab8458c  B[2]=0a6aed78  C[2]=46cfbfe0  D[2]=adec515e
A[3]=7b037c08  B[3]=fd79b418  C[3]=f69e666b  D[3]=f1b18471
A[4]=fcbe9c7c  B[4]=cc3e6b67  C[4]=7ad1c658  D[4]=c4c4c2ac
A[5]=5a39f450  B[5]=e19b6e2a  C[5]=8d095f8e  D[5]=05e208cd
A[6]=529dc45b  B[6]=0b8ea2b8  C[6]=35ccd481  D[6]=53162f0b
A[7]=b77d92b5  B[7]=4cfa425d  C[7]=3fc0218b  D[7]=0fb3bd1d

Step 30: (r=29, s= 9)
A[0]=b3e7b66d  B[0]=51a24777  C[0]=5ce3f2c4  D[0]=4f399cab
A[1]=863c00bc  B[1]=e41da5ed  C[1]=8cc82efa  D[1]=1d9bc345
A[2]=c596c22a  B[2]=975708b1  C[2]=0a6aed78  D[2]=46cfbfe0
A[3]=d96b298e  B[3]=0f606f81  C[3]=fd79b418  D[3]=f69e666b
```

```
A[4]=a3ae33d8  B[4]=9f97d38f  C[4]=cc3e6b67  D[4]=7ad1c658
A[5]=f6bf4ff4  B[5]=0b473e8a  C[5]=e19b6e2a  D[5]=8d095f8e
A[6]=ff6f1b50  B[6]=6a53b88b  C[6]=0b8ea2b8  D[6]=35ccd481
A[7]=ad94b7a3  B[7]=b6efb256  C[7]=4cfa425d  D[7]=3fc0218b

Step 31: (r= 9, s=15)
A[0]=cbd45bf1  B[0]=cf6cdb67  C[0]=51a24777  D[0]=5ce3f2c4
A[1]=54b358d6  B[1]=7801790c  C[1]=e41da5ed  D[1]=8cc82efa
A[2]=183e9316  B[2]=2d84558b  C[2]=975708b1  D[2]=0a6aed78
A[3]=fa612a66  B[3]=d6531db2  C[3]=0f606f81  D[3]=fd79b418
A[4]=f457d8d8  B[4]=5c67b147  C[4]=9f97d38f  D[4]=cc3e6b67
A[5]=354ddb30  B[5]=7e9fe9ed  C[5]=0b473e8a  D[5]=e19b6e2a
A[6]=4755d3d5  B[6]=de36a1fe  C[6]=6a53b88b  D[6]=0b8ea2b8
A[7]=93d7407e  B[7]=296f475b  C[7]=b6efb256  D[7]=4cfa425d

Feed-Forward Step 0: (r=15, s= 5)
A[0]=01b60b81  B[0]=2df8e5ea  C[0]=cf6cdb67  D[0]=51a24777
A[1]=3a8fe8a1  B[1]=ac6b2a59  C[1]=7801790c  D[1]=e41da5ed
A[2]=21ff49b6  B[2]=498b0c1f  C[2]=2d84558b  D[2]=975708b1
A[3]=804fd19a  B[3]=95337d30  C[3]=d6531db2  D[3]=0f606f81
A[4]=7ed24ebf  B[4]=ec6c7a2b  C[4]=5c67b147  D[4]=9f97d38f
A[5]=d48db914  B[5]=ed981aa6  C[5]=7e9fe9ed  D[5]=0b473e8a
A[6]=737e79af  B[6]=e9eaa3aa  C[6]=de36a1fe  D[6]=6a53b88b
A[7]=80bdefd1  B[7]=a03f49eb  C[7]=296f475b  D[7]=b6efb256

Feed-Forward Step 1: (r= 5, s=29)
A[0]=d4f657a7  B[0]=36c17020  C[0]=2df8e5ea  D[0]=cf6cdb67
A[1]=a2160382  B[1]=51fd1427  C[1]=ac6b2a59  D[1]=7801790c
A[2]=18fc76a3  B[2]=3fe936c4  C[2]=498b0c1f  D[2]=2d84558b
A[3]=74317c78  B[3]=09fa3350  C[3]=95337d30  D[3]=d6531db2
A[4]=a7779c2a  B[4]=da49d7ef  C[4]=ec6c7a2b  D[4]=5c67b147
A[5]=176d33cf  B[5]=91b7229a  C[5]=ed981aa6  D[5]=7e9fe9ed
A[6]=4db125ba  B[6]=6fcf35ee  C[6]=e9eaa3aa  D[6]=de36a1fe
A[7]=08bddde4  B[7]=17bdfa30  C[7]=a03f49eb  D[7]=296f475b

Feed-Forward Step 2: (r=29, s= 9)
A[0]=7d21645c  B[0]=fa9ecaf4  C[0]=36c17020  D[0]=2df8e5ea
A[1]=5abee48d  B[1]=5442c070  C[1]=51fd1427  D[1]=ac6b2a59
A[2]=1d04fe05  B[2]=631f8ed4  C[2]=3fe936c4  D[2]=498b0c1f
A[3]=ef1c9c19  B[3]=0e862f8f  C[3]=09fa3350  D[3]=95337d30
A[4]=401fe76c  B[4]=54eef385  C[4]=da49d7ef  D[4]=ec6c7a2b
A[5]=bc2e3c57  B[5]=e2eda679  C[5]=91b7229a  D[5]=ed981aa6
A[6]=05e576be  B[6]=49b624b7  C[6]=6fcf35ee  D[6]=e9eaa3aa
A[7]=3dba0320  B[7]=8117bbbc  C[7]=17bdfa30  D[7]=a03f49eb

Feed-Forward Step 3: (r= 9, s=15)
A[0]=eb88db05  B[0]=42c8b8fa  C[0]=fa9ecaf4  D[0]=36c17020
A[1]=b371a29a  B[1]=7dc91ab5  C[1]=5442c070  D[1]=51fd1427
A[2]=87d169e1  B[2]=09fc0a3a  C[2]=631f8ed4  D[2]=3fe936c4
```

```
A[3]=e240cce5  B[3]=393833de  C[3]=0e862f8f  D[3]=09fa3350
A[4]=5cee51fc  B[4]=3fced880  C[4]=54eef385  D[4]=da49d7ef
A[5]=6fba0a39  B[5]=5c78af78  C[5]=e2eda679  D[5]=91b7229a
A[6]=08e196b7  B[6]=caed7c0b  C[6]=49b624b7  D[6]=6fcf35ee
A[7]=720cf44a  B[7]=7406407b  C[7]=8117bbbc  D[7]=17bdfa30
```

Compression Function Output

```
A[0]=eb88db05  B[0]=42c8b8fa  C[0]=fa9ecaf4  D[0]=36c17020
A[1]=b371a29a  B[1]=7dc91ab5  C[1]=5442c070  D[1]=51fd1427
A[2]=87d169e1  B[2]=09fc0a3a  C[2]=631f8ed4  D[2]=3fe936c4
A[3]=e240cce5  B[3]=393833de  C[3]=0e862f8f  D[3]=09fa3350
A[4]=5cee51fc  B[4]=3fced880  C[4]=54eef385  D[4]=da49d7ef
A[5]=6fba0a39  B[5]=5c78af78  C[5]=e2eda679  D[5]=91b7229a
A[6]=08e196b7  B[6]=caed7c0b  C[6]=49b624b7  D[6]=6fcf35ee
A[7]=720cf44a  B[7]=7406407b  C[7]=8117bbbc  D[7]=17bdfa30
```

Hash Function Output

```
05 db 88 eb 9a a2 71 b3 e1 69 d1 87 e5 cc 40 e2
fc 51 ee 5c 39 0a ba 6f b7 96 e1 08 4a f4 0c 72
fa b8 c8 42 b5 1a c9 7d 3a 0a fc 09 de 33 38 39
```

6.3.3 Two blocks message

We use the message made of 1079 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
```

```
y[ 16.. 23] =  129   99   49  124  176  112   29   25
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
```

```
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff2101be  aaa2555e  ad3f52c1  cd7a3286
        e5de1a22  9d91626f  ebf71409  3365cc9b
Z[17] = 6f809080  d5512aaf  468fb971  e6bd1943
        f2ef0d11  3eb8c148  65eb9a15  a9c3563d
Z[18] = 37c0c840  5a98a568  b3584ca8  634e9cb2
        69679699  1f5ce0a4  c3063cfa  44d1bb2f
Z[19] = 1be0e420  2d4cd2b4  d9ac2654  31a7ce59
        c4c43b3c  0faef052  e1831e7d  b2794d87
Z[20] = 0df0f210  16a6e95a  ecd6132a  a8e4571c
        e2621d9e  07d7f829  60b19f4f  492cb6d4
Z[21] = 06f8f908  0b53f4ad  f66b0995  d4722b8e
        f1310ecf  93fc6c04  c0693f97  2496db6a
Z[22] = 037cfc84  95ba6a46  6b2594db  ea3915c7
        68889778  c9fe3602  5024afdc  124bedb5
Z[23] = 01befe42  cadd3523  c5a33a5d  650c9af4
        3444cbbc  e4ff1b01  2812d7ee  993666ca
Z[24] = fc844aea  51e2e5de  e5de4313  4d879cb2
        66ca4ca8  1be0bced  dd28563d  a4890b53
Z[25] = ba50563d  b5f56c04  afdc6190  a02e15c7
        bc0e4155  b4374ca8  6f80ad3f  b9719cb2
Z[26] = 4a0b0a74  dfc5ebf7  642d1be0  634e6b25
        52c1e6bd  9a15cc9b  b516f3ce  bdcc650c
Z[27] = eb189778  ae1e0000  1b01029d  4d879778
        d2b43523  b0bb6ea1  6b25ab81  42349080
Z[28] = 116c14e8  0b53d70f  1b01beab  650c6c04
        c4c44f45  a3aa37c0  5a98f052  60b115c7
Z[29] = 908045b0  b892b7b3  5a9837c0  afdc0fae
        5e14ac60  061952c1  d630571c  fc84a805
Z[30] = c91ff9e7  cc9b0fae  fd63fac6  4e66ad3f
        571cebf7  dee608b6  f052e6bd  c4c423b7
Z[31] = cf389a15  6f803602  66cab971  3602ef73
        3c1bd2b4  3dd9923e  60b14076  634e2e2b
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
W[11] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
W[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
W[15] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] = 6f809080  d5512aaf  468fb971  e6bd1943
        f2ef0d11  3eb8c148  65eb9a15  a9c3563d
W[17] = 37c0c840  5a98a568  b3584ca8  634e9cb2
        69679699  1f5ce0a4  c3063cfa  44d1bb2f
W[18] = 01befe42  cadd3523  c5a33a5d  650c9af4
        3444cbbc  e4ff1b01  2812d7ee  993666ca
W[19] = 0df0f210  16a6e95a  ecd6132a  a8e4571c
        e2621d9e  07d7f829  60b19f4f  492cb6d4
W[20] = 037cfc84  95ba6a46  6b2594db  ea3915c7
        68889778  c9fe3602  5024afdc  124bedb5
W[21] = 06f8f908  0b53f4ad  f66b0995  d4722b8e
        f1310ecf  93fc6c04  c0693f97  2496db6a
W[22] = ff2101be  aaa2555e  ad3f52c1  cd7a3286
        e5de1a22  9d91626f  ebf71409  3365cc9b
W[23] = 1be0e420  2d4cd2b4  d9ac2654  31a7ce59
        c4c43b3c  0faef052  e1831e7d  b2794d87
```

```
W[24] = c91ff9e7  cc9b0fae  fd63fac6  4e66ad3f
        571cebf7  dee608b6  f052e6bd  c4c423b7
W[25] = fc844aea  51e2e5de  e5de4313  4d879cb2
        66ca4ca8  1be0bced  dd28563d  a4890b53
W[26] = ba50563d  b5f56c04  afdc6190  a02e15c7
        bc0e4155  b4374ca8  6f80ad3f  b9719cb2
W[27] = cf389a15  6f803602  66cab971  3602ef73
        3c1bd2b4  3dd9923e  60b14076  634e2e2b
W[28] = eb189778  ae1e0000  1b01029d  4d879778
        d2b43523  b0bb6ea1  6b25ab81  42349080
W[29] = 908045b0  b892b7b3  5a9837c0  afdc0fae
        5e14ac60  061952c1  d630571c  fc84a805
W[30] = 116c14e8  0b53d70f  1b01beab  650c6c04
        c4c44f45  a3aa37c0  5a98f052  60b115c7
W[31] = 4a0b0a74  dfc5ebf7  642d1be0  634e6b25
        52c1e6bd  9a15cc9b  b516f3ce  bdcc650c
```

Feistel Steps

```
IV :
A[0]=3a8f3d6f  B[0]=f46f6c9b  C[0]=2da6fdc3  D[0]=91195b41
A[1]=756a1087  B[1]=9ab248ef  C[1]=fbafce00  D[1]=fcb9404e
A[2]=5d5318aa  B[2]=dbbfc9cc  C[2]=4c9a6954  D[2]=214e6c84
A[3]=bbca76f7  B[3]=cc8821fa  C[3]=b61f0faf  D[3]=88740b3a
A[4]=26a3a959  B[4]=354d3c2e  C[4]=f56099b5  D[4]=ba03a4b1
A[5]=aca1e37e  B[5]=da334fb1  C[5]=a3a5bdfb  D[5]=a82202fc
A[6]=b40c4642  B[6]=68ed79ce  C[6]=f83e0977  D[6]=994fddfb
A[7]=904085d9  B[7]=a5bc107d  C[7]=7eb15372  D[7]=b2e1a1de

IV XOR M :
A[0]=c570c290  B[0]=0b909364  C[0]=d259023c  D[0]=6ee6a4be
A[1]=8a95ef78  B[1]=654db710  C[1]=045031ff  D[1]=0346bfb1
A[2]=a2ace755  B[2]=24403633  C[2]=b36596ab  D[2]=deb1937b
A[3]=44358908  B[3]=3377de05  C[3]=49e0f050  D[3]=778bf4c5
A[4]=d95c56a6  B[4]=cab2c3d1  C[4]=0a9f664a  D[4]=45fc5b4e
A[5]=535e1c81  B[5]=25ccb04e  C[5]=5c5a4204  D[5]=57ddfd03
A[6]=4bf3b9bd  B[6]=97128631  C[6]=07c1f688  D[6]=66b02204
A[7]=6fbf7a26  B[7]=5a43ef82  C[7]=814eac8d  D[7]=4d1e5e21

Step  0: (r= 3, s=20)
A[0]=0a58b155  B[0]=2b861486  C[0]=0b909364  D[0]=d259023c
A[1]=73746dec  B[1]=54af7bc4  C[1]=654db710  D[1]=045031ff
A[2]=c379e43f  B[2]=15673aad  C[2]=24403633  D[2]=b36596ab
A[3]=6b04ec90  B[3]=21ac4842  C[3]=3377de05  D[3]=49e0f050
A[4]=05760937  B[4]=cae2b536  C[4]=cab2c3d1  D[4]=0a9f664a
A[5]=534bebea  B[5]=9af0e40a  C[5]=25ccb04e  D[5]=5c5a4204
A[6]=fde1dd4c  B[6]=5f9dcdea  C[6]=97128631  D[6]=07c1f688
A[7]=5f20652a  B[7]=7dfbd133  C[7]=5a43ef82  D[7]=814eac8d
```

```
Step  1: (r=20, s=14)
A[0]=085b6dd0  B[0]=1550a58b  C[0]=2b861486  D[0]=0b909364
A[1]=ea8609ae  B[1]=dec73746  C[1]=54af7bc4  D[1]=654db710
A[2]=714e1aa7  B[2]=43fc379e  C[2]=15673aad  D[2]=24403633
A[3]=35e0c4f2  B[3]=c906b04e  C[3]=21ac4842  D[3]=3377de05
A[4]=c9b20f55  B[4]=93705760  C[4]=cae2b536  D[4]=cab2c3d1
A[5]=aa5e189c  B[5]=bea534be  C[5]=9af0e40a  D[5]=25ccb04e
A[6]=f451abf8  B[6]=d4cfde1d  C[6]=5f9dcdea  D[6]=97128631
A[7]=d8e5f3d3  B[7]=52a5f206  C[7]=7dfbd133  D[7]=5a43ef82

Step  2: (r=14, s=27)
A[0]=60614c8b  B[0]=db740216  C[0]=1550a58b  D[0]=2b861486
A[1]=ac70b89d  B[1]=826bbaa1  C[1]=dec73746  D[1]=54af7bc4
A[2]=cb31c002  B[2]=86a9dc53  C[2]=43fc379e  D[2]=15673aad
A[3]=12e686ed  B[3]=313c8d78  C[3]=c906b04e  D[3]=21ac4842
A[4]=3daa69ff  B[4]=83d5726c  C[4]=93705760  D[4]=cae2b536
A[5]=33f04407  B[5]=86272a97  C[5]=bea534be  D[5]=9af0e40a
A[6]=d85f15c8  B[6]=6afe3d14  C[6]=d4cfde1d  D[6]=5f9dcdea
A[7]=ea3f4fce  B[7]=7cf4f639  C[7]=52a5f206  D[7]=7dfbd133

Step  3: (r=27, s= 3)
A[0]=47098d93  B[0]=5b030a64  C[0]=db740216  D[0]=1550a58b
A[1]=f1670518  B[1]=ed6385c4  C[1]=826bbaa1  D[1]=dec73746
A[2]=c26e87cb  B[2]=16598e00  C[2]=86a9dc53  D[2]=43fc379e
A[3]=14f74cd0  B[3]=68973437  C[3]=313c8d78  D[3]=c906b04e
A[4]=28f9abed  B[4]=f9ed534f  C[4]=83d5726c  D[4]=93705760
A[5]=e1035bf3  B[5]=399f8220  C[5]=86272a97  D[5]=bea534be
A[6]=29508aad  B[6]=46c2f8ae  C[6]=6afe3d14  D[6]=d4cfde1d
A[7]=bcc3a559  B[7]=7751fa7e  C[7]=7cf4f639  D[7]=52a5f206

Step  4: (r= 3, s=20)
A[0]=6e29e521  B[0]=384c6c9a  C[0]=5b030a64  D[0]=db740216
A[1]=c60b3c28  B[1]=8b3828c7  C[1]=ed6385c4  D[1]=826bbaa1
A[2]=0c83644f  B[2]=13743e5e  C[2]=16598e00  D[2]=86a9dc53
A[3]=a222fe94  B[3]=a7ba6680  C[3]=68973437  D[3]=313c8d78
A[4]=ff2c5d48  B[4]=47cd5f69  C[4]=f9ed534f  D[4]=83d5726c
A[5]=a54da94e  B[5]=081adf9f  C[5]=399f8220  D[5]=86272a97
A[6]=3ed47ca4  B[6]=4a845569  C[6]=46c2f8ae  D[6]=6afe3d14
A[7]=26e3b1bc  B[7]=e61d2acd  C[7]=7751fa7e  D[7]=7cf4f639

Step  5: (r=20, s=14)
A[0]=df0c6c09  B[0]=5216e29e  C[0]=384c6c9a  D[0]=5b030a64
A[1]=20ca2796  B[1]=c28c60b3  C[1]=8b3828c7  D[1]=ed6385c4
A[2]=16bc156c  B[2]=44f0c836  C[2]=13743e5e  D[2]=16598e00
A[3]=0c9818ef  B[3]=e94a222f  C[3]=a7ba6680  D[3]=68973437
A[4]=81c37cdf  B[4]=d48ff2c5  C[4]=47cd5f69  D[4]=f9ed534f
A[5]=9f92eb36  B[5]=94ea54da  C[5]=081adf9f  D[5]=399f8220
A[6]=90303346  B[6]=ca43ed47  C[6]=4a845569  D[6]=46c2f8ae
A[7]=39a13b6c  B[7]=1bc26e3b  C[7]=e61d2acd  D[7]=7751fa7e
```

```
Step  6: (r=14, s=27)
A[0]=41cdd166  B[0]=1b0277c3  C[0]=5216e29e  D[0]=384c6c9a
A[1]=48510812  B[1]=89e58832  C[1]=c28c60b3  D[1]=8b3828c7
A[2]=0c496e36  B[2]=055b05af  C[2]=44f0c836  D[2]=13743e5e
A[3]=8d33b1dd  B[3]=063bc326  C[3]=e94a222f  D[3]=a7ba6680
A[4]=0d9a5340  B[4]=df37e070  C[4]=d48ff2c5  D[4]=47cd5f69
A[5]=e6eb1854  B[5]=bacda7e4  C[5]=94ea54da  D[5]=081adf9f
A[6]=903adc6c  B[6]=0cd1a40c  C[6]=ca43ed47  D[6]=4a845569
A[7]=fdb512ec  B[7]=4edb0e68  C[7]=1bc26e3b  D[7]=e61d2acd

Step  7: (r=27, s= 3)
A[0]=9764f1a0  B[0]=320e6e8b  C[0]=1b0277c3  D[0]=5216e29e
A[1]=1401fbd7  B[1]=92428840  C[1]=89e58832  D[1]=c28c60b3
A[2]=aa74573e  B[2]=b0624b71  C[2]=055b05af  D[2]=44f0c836
A[3]=a0269db9  B[3]=ec699d8e  C[3]=063bc326  D[3]=e94a222f
A[4]=0f11528d  B[4]=006cd29a  C[4]=df37e070  D[4]=d48ff2c5
A[5]=87388b9f  B[5]=a73758c2  C[5]=bacda7e4  D[5]=94ea54da
A[6]=21f1b4b5  B[6]=6481d6e3  C[6]=0cd1a40c  D[6]=ca43ed47
A[7]=88dda395  B[7]=67eda897  C[7]=4edb0e68  D[7]=1bc26e3b

Step  8: (r=26, s= 4)
A[0]=96a4b523  B[0]=825d93c6  C[0]=320e6e8b  D[0]=1b0277c3
A[1]=117963b1  B[1]=5c5007ef  C[1]=92428840  D[1]=89e58832
A[2]=e0ae5239  B[2]=faa9d15c  C[2]=b0624b71  D[2]=055b05af
A[3]=bfcf2a77  B[3]=e6809a76  C[3]=ec699d8e  D[3]=063bc326
A[4]=e75df3cb  B[4]=343c454a  C[4]=006cd29a  D[4]=df37e070
A[5]=b732faa2  B[5]=7e1ce22e  C[5]=a73758c2  D[5]=bacda7e4
A[6]=c5eda972  B[6]=d487c6d2  C[6]=6481d6e3  D[6]=0cd1a40c
A[7]=23d425fd  B[7]=5623768e  C[7]=67eda897  D[7]=4edb0e68

Step  9: (r= 4, s=23)
A[0]=41bb0053  B[0]=6a4b5239  C[0]=825d93c6  D[0]=320e6e8b
A[1]=d0decc97  B[1]=17963b11  C[1]=5c5007ef  D[1]=92428840
A[2]=07d1a7d8  B[2]=0ae5239e  C[2]=faa9d15c  D[2]=b0624b71
A[3]=422cd1d7  B[3]=fcf2a77b  C[3]=e6809a76  D[3]=ec699d8e
A[4]=b24987a4  B[4]=75df3cbe  C[4]=343c454a  D[4]=006cd29a
A[5]=e199f01d  B[5]=732faa2b  C[5]=7e1ce22e  D[5]=a73758c2
A[6]=40045a6e  B[6]=5eda972c  C[6]=d487c6d2  D[6]=6481d6e3
A[7]=c615a2e8  B[7]=3d425fd2  C[7]=5623768e  D[7]=67eda897

Step 10: (r=23, s=11)
A[0]=04d08ae7  B[0]=29a0dd80  C[0]=6a4b5239  D[0]=825d93c6
A[1]=24541fee  B[1]=4be86f66  C[1]=17963b11  D[1]=5c5007ef
A[2]=ac6a0b05  B[2]=ec03e8d3  C[2]=0ae5239e  D[2]=faa9d15c
A[3]=c95f0de9  B[3]=eba11668  C[3]=fcf2a77b  D[3]=e6809a76
A[4]=2398c686  B[4]=d25924c3  C[4]=75df3cbe  D[4]=343c454a
A[5]=440f5fa0  B[5]=0ef0ccf8  C[5]=732faa2b  D[5]=7e1ce22e
A[6]=b9d72387  B[6]=3720022d  C[6]=5eda972c  D[6]=d487c6d2
```

```
A[7]=63816be2  B[7]=74630ad1  C[7]=3d425fd2  D[7]=5623768e

Step 11: (r=11, s=26)
A[0]=5ddc4aca  B[0]=84573826  C[0]=29a0dd80  D[0]=6a4b5239
A[1]=cdcd05e2  B[1]=a0ff7122  C[1]=4be86f66  D[1]=17963b11
A[2]=fb6a4ca3  B[2]=50582d63  C[2]=ec03e8d3  D[2]=0ae5239e
A[3]=23f0e378  B[3]=f86f4e4a  C[3]=eba11668  D[3]=fcf2a77b
A[4]=dfd6c1d7  B[4]=c634311c  C[4]=d25924c3  D[4]=75df3cbe
A[5]=6430eb16  B[5]=7afd0220  C[5]=0ef0ccf8  D[5]=732faa2b
A[6]=d112d294  B[6]=b91c3dce  C[6]=3720022d  D[6]=5eda972c
A[7]=fe89654a  B[7]=0b5f131c  C[7]=74630ad1  D[7]=3d425fd2

Step 12: (r=26, s= 4)
A[0]=7037a7ca  B[0]=2977712b  C[0]=84573826  D[0]=29a0dd80
A[1]=6aef41d5  B[1]=8b373417  C[1]=a0ff7122  D[1]=4be86f66
A[2]=ebcc7439  B[2]=8feda932  C[2]=50582d63  D[2]=ec03e8d3
A[3]=255b381b  B[3]=e08fc38d  C[3]=f86f4e4a  D[3]=eba11668
A[4]=96f5ff8d  B[4]=5f7f5b07  C[4]=c634311c  D[4]=d25924c3
A[5]=9399e141  B[5]=5990c3ac  C[5]=7afd0220  D[5]=0ef0ccf8
A[6]=f2aa09eb  B[6]=53444b4a  C[6]=b91c3dce  D[6]=3720022d
A[7]=63960542  B[7]=2bfa2595  C[7]=0b5f131c  D[7]=74630ad1

Step 13: (r= 4, s=23)
A[0]=f63e0fa8  B[0]=037a7ca7  C[0]=2977712b  D[0]=84573826
A[1]=471154a6  B[1]=aef41d56  C[1]=8b373417  D[1]=a0ff7122
A[2]=0cfbf92e  B[2]=bcc7439e  C[2]=8feda932  D[2]=50582d63
A[3]=d7b8d7f4  B[3]=55b381b2  C[3]=e08fc38d  D[3]=f86f4e4a
A[4]=ee9c0c88  B[4]=6f5ff8d9  C[4]=5f7f5b07  D[4]=c634311c
A[5]=77982141  B[5]=399e1419  C[5]=5990c3ac  D[5]=7afd0220
A[6]=0a63b744  B[6]=2aa09ebf  C[6]=53444b4a  D[6]=b91c3dce
A[7]=596cc2b0  B[7]=39605426  C[7]=2bfa2595  D[7]=0b5f131c

Step 14: (r=23, s=11)
A[0]=6f4d458b  B[0]=d47b1f07  C[0]=037a7ca7  D[0]=2977712b
A[1]=60883286  B[1]=532388aa  C[1]=aef41d56  D[1]=8b373417
A[2]=bf741593  B[2]=97067dfc  C[2]=bcc7439e  D[2]=8feda932
A[3]=af9a4f0a  B[3]=fa6bdc6b  C[3]=55b381b2  D[3]=e08fc38d
A[4]=d174903c  B[4]=44774e06  C[4]=6f5ff8d9  D[4]=5f7f5b07
A[5]=d7efeafc  B[5]=a0bbcc10  C[5]=399e1419  D[5]=5990c3ac
A[6]=1077bcd4  B[6]=a20531db  C[6]=2aa09ebf  D[6]=53444b4a
A[7]=b1025775  B[7]=582cb661  C[7]=39605426  D[7]=2bfa2595

Step 15: (r=11, s=26)
A[0]=fd8f95d1  B[0]=6a2c5b7a  C[0]=d47b1f07  D[0]=037a7ca7
A[1]=4e64ba90  B[1]=41943304  C[1]=532388aa  D[1]=aef41d56
A[2]=8b1ac5e1  B[2]=a0ac9dfb  C[2]=97067dfc  D[2]=bcc7439e
A[3]=ab410782  B[3]=d278557c  C[3]=fa6bdc6b  D[3]=55b381b2
A[4]=d9e149a1  B[4]=a481e68b  C[4]=44774e06  D[4]=6f5ff8d9
A[5]=1d53a08f  B[5]=7f57e6bf  C[5]=a0bbcc10  D[5]=399e1419
```

```
A[6]=364e3f25  B[6]=bde6a083  C[6]=a20531db  D[6]=2aa09ebf
A[7]=6f482fa8  B[7]=12bbad88  C[7]=582cb661  D[7]=39605426

Step 16: (r=19, s=28)
A[0]=b239e5ac  B[0]=ae8fec7c  C[0]=6a2c5b7a  D[0]=d47b1f07
A[1]=abe4b41e  B[1]=d4827325  C[1]=41943304  D[1]=532388aa
A[2]=058b95b8  B[2]=2f0c58d6  C[2]=a0ac9dfb  D[2]=97067dfc
A[3]=0ffa105b  B[3]=3c155a08  C[3]=d278557c  D[3]=fa6bdc6b
A[4]=22e74f64  B[4]=4d0ecf0a  C[4]=a481e68b  D[4]=44774e06
A[5]=5073fb2a  B[5]=0478ea9d  C[5]=7f57e6bf  D[5]=a0bbcc10
A[6]=7190afdb  B[6]=f929b271  C[6]=bde6a083  D[6]=a20531db
A[7]=c87eb8f3  B[7]=7d437a41  C[7]=12bbad88  D[7]=582cb661

Step 17: (r=28, s= 7)
A[0]=a54b9c56  B[0]=cb239e5a  C[0]=ae8fec7c  D[0]=6a2c5b7a
A[1]=d7302c3c  B[1]=eabe4b41  C[1]=d4827325  D[1]=41943304
A[2]=90955a51  B[2]=8058b95b  C[2]=2f0c58d6  D[2]=a0ac9dfb
A[3]=d0256fdd  B[3]=b0ffa105  C[3]=3c155a08  D[3]=d278557c
A[4]=aa032015  B[4]=422e74f6  C[4]=4d0ecf0a  D[4]=a481e68b
A[5]=03559486  B[5]=a5073fb2  C[5]=0478ea9d  D[5]=7f57e6bf
A[6]=7b370827  B[6]=b7190afd  C[6]=f929b271  D[6]=bde6a083
A[7]=85deacad  B[7]=3c87eb8f  C[7]=7d437a41  D[7]=12bbad88

Step 18: (r= 7, s=22)
A[0]=7d143397  B[0]=a5ce2b52  C[0]=cb239e5a  D[0]=ae8fec7c
A[1]=65b7dcad  B[1]=98161e6b  C[1]=eabe4b41  D[1]=d4827325
A[2]=f68f9cfd  B[2]=4aad28c8  C[2]=8058b95b  D[2]=2f0c58d6
A[3]=5f0cf95d  B[3]=12b7eee8  C[3]=b0ffa105  D[3]=3c155a08
A[4]=6bffe450  B[4]=01900ad5  C[4]=422e74f6  D[4]=4d0ecf0a
A[5]=618789e8  B[5]=aaca4301  C[5]=a5073fb2  D[5]=0478ea9d
A[6]=51bc6337  B[6]=9b8413bd  C[6]=b7190afd  D[6]=f929b271
A[7]=6d9849d5  B[7]=ef5656c2  C[7]=3c87eb8f  D[7]=7d437a41

Step 19: (r=22, s=19)
A[0]=834e1d3d  B[0]=e5df450c  C[0]=a5ce2b52  D[0]=cb239e5a
A[1]=595c0c1d  B[1]=2b596df7  C[1]=98161e6b  D[1]=eabe4b41
A[2]=7c276514  B[2]=3f7da3e7  C[2]=4aad28c8  D[2]=8058b95b
A[3]=40c0259e  B[3]=5757c33e  C[3]=12b7eee8  D[3]=b0ffa105
A[4]=d2d0cd13  B[4]=141afff9  C[4]=01900ad5  D[4]=422e74f6
A[5]=fa1ef48f  B[5]=7a1861e2  C[5]=aaca4301  D[5]=a5073fb2
A[6]=2d662ee9  B[6]=cdd46f18  C[6]=9b8413bd  D[6]=b7190afd
A[7]=f651df7e  B[7]=755b6612  C[7]=ef5656c2  D[7]=3c87eb8f

Step 20: (r=19, s=28)
A[0]=0831b55f  B[0]=e9ec1a70  C[0]=e5df450c  D[0]=a5ce2b52
A[1]=53896690  B[1]=60eacae0  C[1]=2b596df7  D[1]=98161e6b
A[2]=d38cbd00  B[2]=28a3e13b  C[2]=3f7da3e7  D[2]=4aad28c8
A[3]=d784eb23  B[3]=2cf20601  C[3]=5757c33e  D[3]=12b7eee8
A[4]=a0344eba  B[4]=689e9686  C[4]=141afff9  D[4]=01900ad5
```

```
A[5]=df3093f9  B[5]=a47fd0f7  C[5]=7a1861e2  D[5]=aaca4301
A[6]=2547d137  B[6]=77496b31  C[6]=cdd46f18  D[6]=9b8413bd
A[7]=dbabde2a  B[7]=fbf7b28e  C[7]=755b6612  D[7]=ef5656c2

Step 21: (r=28, s= 7)
A[0]=6f55a71b  B[0]=f0831b55  C[0]=e9ec1a70  D[0]=e5df450c
A[1]=d73952b5  B[1]=05389669  C[1]=60eacae0  D[1]=2b596df7
A[2]=536cdb93  B[2]=0d38cbd0  C[2]=28a3e13b  D[2]=3f7da3e7
A[3]=85a76308  B[3]=3d784eb2  C[3]=2cf20601  D[3]=5757c33e
A[4]=e250ac1c  B[4]=aa0344eb  C[4]=689e9686  D[4]=141afff9
A[5]=2d7b3a00  B[5]=9df3093f  C[5]=a47fd0f7  D[5]=7a1861e2
A[6]=436287cb  B[6]=72547d13  C[6]=77496b31  D[6]=cdd46f18
A[7]=92872446  B[7]=adbabde2  C[7]=fbf7b28e  D[7]=755b6612

Step 22: (r= 7, s=22)
A[0]=ca85d4a1  B[0]=aad38db7  C[0]=f0831b55  D[0]=e9ec1a70
A[1]=3ecab2c6  B[1]=9ca95aeb  C[1]=05389669  D[1]=60eacae0
A[2]=4c9a7986  B[2]=b66dc9a9  C[2]=0d38cbd0  D[2]=28a3e13b
A[3]=196abf7f  B[3]=d3b18442  C[3]=3d784eb2  D[3]=2cf20601
A[4]=7e2a8729  B[4]=28560e71  C[4]=aa0344eb  D[4]=689e9686
A[5]=d89f12e0  B[5]=bd9d0016  C[5]=9df3093f  D[5]=a47fd0f7
A[6]=29b49de7  B[6]=b143e5a1  C[6]=72547d13  D[6]=77496b31
A[7]=87acabf0  B[7]=43922349  C[7]=adbabde2  D[7]=fbf7b28e

Step 23: (r=22, s=19)
A[0]=ac8f0d25  B[0]=2872a175  C[0]=aad38db7  D[0]=f0831b55
A[1]=3c337ec5  B[1]=b18fb2ac  C[1]=9ca95aeb  D[1]=05389669
A[2]=0242e16d  B[2]=6193269e  C[2]=b66dc9a9  D[2]=0d38cbd0
A[3]=1285abbd  B[3]=dfc65aaf  C[3]=d3b18442  D[3]=3d784eb2
A[4]=e9cd5c9b  B[4]=ca5f8aa1  C[4]=28560e71  D[4]=aa0344eb
A[5]=bd8a411a  B[5]=b83627c4  C[5]=bd9d0016  D[5]=9df3093f
A[6]=9c1f77aa  B[6]=79ca6d27  C[6]=b143e5a1  D[6]=72547d13
A[7]=3f700c0c  B[7]=fc21eb2a  C[7]=43922349  D[7]=adbabde2

Step 24: (r=15, s= 5)
A[0]=3e157c95  B[0]=8692d647  C[0]=2872a175  D[0]=aad38db7
A[1]=d26deef7  B[1]=bf629e19  C[1]=b18fb2ac  D[1]=9ca95aeb
A[2]=af5c6d99  B[2]=70b68121  C[2]=6193269e  D[2]=b66dc9a9
A[3]=6317dd2c  B[3]=d5de8942  C[3]=dfc65aaf  D[3]=d3b18442
A[4]=5074d73e  B[4]=ae4df4e6  C[4]=ca5f8aa1  D[4]=28560e71
A[5]=4c50540c  B[5]=208d5ec5  C[5]=b83627c4  D[5]=bd9d0016
A[6]=844f3e2b  B[6]=bbd54e0f  C[6]=79ca6d27  D[6]=b143e5a1
A[7]=9ff6ea6c  B[7]=06061fb8  C[7]=fc21eb2a  D[7]=43922349

Step 25: (r= 5, s=29)
A[0]=c14708f5  B[0]=c2af92a7  C[0]=8692d647  D[0]=2872a175
A[1]=b7498168  B[1]=4dbddefa  C[1]=bf629e19  D[1]=b18fb2ac
A[2]=424bf49f  B[2]=eb8db335  C[2]=70b68121  D[2]=6193269e
A[3]=4d9fd488  B[3]=62fba58c  C[3]=d5de8942  D[3]=dfc65aaf
```

```
A[4]=8d15cc68  B[4]=0e9ae7ca  C[4]=ae4df4e6  D[4]=ca5f8aa1
A[5]=f011d42b  B[5]=8a0a8189  C[5]=208d5ec5  D[5]=b83627c4
A[6]=bfa11927  B[6]=89e7c570  C[6]=bbd54e0f  D[6]=79ca6d27
A[7]=53cec8c1  B[7]=fedd4d93  C[7]=06061fb8  D[7]=fc21eb2a

Step 26: (r=29, s= 9)
A[0]=e0168c6a  B[0]=b828e11e  C[0]=c2af92a7  D[0]=8692d647
A[1]=596e760d  B[1]=16e9302d  C[1]=4dbddefa  D[1]=bf629e19
A[2]=d875018d  B[2]=e8497e93  C[2]=eb8db335  D[2]=70b68121
A[3]=b19f3a2e  B[3]=09b3fa91  C[3]=62fba58c  D[3]=d5de8942
A[4]=973583fa  B[4]=11a2b98d  C[4]=0e9ae7ca  D[4]=ae4df4e6
A[5]=dc47f26c  B[5]=7e023a85  C[5]=8a0a8189  D[5]=208d5ec5
A[6]=97ac4d13  B[6]=f7f42324  C[6]=89e7c570  D[6]=bbd54e0f
A[7]=77f80b36  B[7]=2a79d918  C[7]=fedd4d93  D[7]=06061fb8

Step 27: (r= 9, s=15)
A[0]=ec7df168  B[0]=2d18d5c0  C[0]=b828e11e  D[0]=c2af92a7
A[1]=d671fba6  B[1]=dcec1ab2  C[1]=16e9302d  D[1]=4dbddefa
A[2]=cf3c08d4  B[2]=ea031bb0  C[2]=e8497e93  D[2]=eb8db335
A[3]=8c3114d9  B[3]=3e745d63  C[3]=09b3fa91  D[3]=62fba58c
A[4]=83a9d7ca  B[4]=6b07f52e  C[4]=11a2b98d  D[4]=0e9ae7ca
A[5]=6f3078ea  B[5]=8fe4d9b8  C[5]=7e023a85  D[5]=8a0a8189
A[6]=f1f5f9e7  B[6]=589a272f  C[6]=f7f42324  D[6]=89e7c570
A[7]=0c2e674b  B[7]=f0166cef  C[7]=2a79d918  D[7]=fedd4d93

Step 28: (r=15, s= 5)
A[0]=3df6d823  B[0]=f8b4763e  C[0]=2d18d5c0  D[0]=b828e11e
A[1]=5157aa58  B[1]=fdd36b38  C[1]=dcec1ab2  D[1]=16e9302d
A[2]=9d66d276  B[2]=046a679e  C[2]=ea031bb0  D[2]=e8497e93
A[3]=9afda255  B[3]=8a6cc618  C[3]=3e745d63  D[3]=09b3fa91
A[4]=dad78714  B[4]=ebe541d4  C[4]=6b07f52e  D[4]=11a2b98d
A[5]=28b25c29  B[5]=3c753798  C[5]=8fe4d9b8  D[5]=7e023a85
A[6]=13d80933  B[6]=fcf3f8fa  C[6]=589a272f  D[6]=f7f42324
A[7]=26fd64c7  B[7]=33a58617  C[7]=f0166cef  D[7]=2a79d918

Step 29: (r= 5, s=29)
A[0]=bda60e31  B[0]=bedb0467  C[0]=f8b4763e  D[0]=2d18d5c0
A[1]=755eacf6  B[1]=2af54b0a  C[1]=fdd36b38  D[1]=dcec1ab2
A[2]=f8c385a8  B[2]=acda4ed3  C[2]=046a679e  D[2]=ea031bb0
A[3]=3576e51c  B[3]=5fb44ab3  C[3]=8a6cc618  D[3]=3e745d63
A[4]=a6710bc2  B[4]=5af0e29b  C[4]=ebe541d4  D[4]=6b07f52e
A[5]=b5ce9643  B[5]=164b8525  C[5]=3c753798  D[5]=8fe4d9b8
A[6]=bfd0b70a  B[6]=7b012662  C[6]=fcf3f8fa  D[6]=589a272f
A[7]=a18201e1  B[7]=dfac98e4  C[7]=33a58617  D[7]=f0166cef

Step 30: (r=29, s= 9)
A[0]=aa120032  B[0]=37b4c1c6  C[0]=bedb0467  D[0]=f8b4763e
A[1]=86b40dad  B[1]=ceabd59e  C[1]=2af54b0a  D[1]=fdd36b38
A[2]=14fdbe2b  B[2]=1f1870b5  C[2]=acda4ed3  D[2]=046a679e
```

```
A[3]=3fed20fd  B[3]=86aedca3  C[3]=5fb44ab3  D[3]=8a6cc618
A[4]=01bf66d8  B[4]=54ce2178  C[4]=5af0e29b  D[4]=ebe541d4
A[5]=dc696384  B[5]=76b9d2c8  C[5]=164b8525  D[5]=3c753798
A[6]=d847ad04  B[6]=57fa16e1  C[6]=7b012662  D[6]=fcf3f8fa
A[7]=0fbbf7ce  B[7]=3430403c  C[7]=dfac98e4  D[7]=33a58617

Step 31: (r= 9, s=15)
A[0]=3f59b0ab  B[0]=24006554  C[0]=37b4c1c6  D[0]=bedb0467
A[1]=2525bfdf  B[1]=681b5b0d  C[1]=ceabd59e  D[1]=2af54b0a
A[2]=9072cc68  B[2]=fb7c5629  C[2]=1f1870b5  D[2]=acda4ed3
A[3]=34e7a2d2  B[3]=da41fa7f  C[3]=86aedca3  D[3]=5fb44ab3
A[4]=e9b52d26  B[4]=7ecdb003  C[4]=54ce2178  D[4]=5af0e29b
A[5]=cbf6f187  B[5]=d2c709b8  C[5]=76b9d2c8  D[5]=164b8525
A[6]=05105cd0  B[6]=8f5a09b0  C[6]=57fa16e1  D[6]=7b012662
A[7]=38498314  B[7]=77ef9c1f  C[7]=3430403c  D[7]=dfac98e4

Feed-Forward Step 0: (r=15, s= 5)
A[0]=a1c3f5d5  B[0]=d8559fac  C[0]=24006554  D[0]=37b4c1c6
A[1]=35ac737d  B[1]=dfef9292  C[1]=681b5b0d  D[1]=ceabd59e
A[2]=0624a1c8  B[2]=66344839  C[2]=fb7c5629  D[2]=1f1870b5
A[3]=1f4c4bee  B[3]=d1691a73  C[3]=da41fa7f  D[3]=86aedca3
A[4]=45396fda  B[4]=969374da  C[4]=7ecdb003  D[4]=54ce2178
A[5]=ce210251  B[5]=78c3e5fb  C[5]=d2c709b8  D[5]=76b9d2c8
A[6]=a27906d4  B[6]=2e680288  C[6]=8f5a09b0  D[6]=57fa16e1
A[7]=bb43e1bc  B[7]=c18a1c24  C[7]=77ef9c1f  D[7]=3430403c

Feed-Forward Step 1: (r= 5, s=29)
A[0]=7aa0f17c  B[0]=387ebab4  C[0]=d8559fac  D[0]=24006554
A[1]=a26d24d6  B[1]=b58e6fa6  C[1]=dfef9292  D[1]=681b5b0d
A[2]=97c94cc9  B[2]=c4943900  C[2]=66344839  D[2]=fb7c5629
A[3]=ba1e86c8  B[3]=e9897dc3  C[3]=d1691a73  D[3]=da41fa7f
A[4]=883f04e4  B[4]=a72dfb48  C[4]=969374da  D[4]=7ecdb003
A[5]=bdb2bd25  B[5]=c4204a39  C[5]=78c3e5fb  D[5]=d2c709b8
A[6]=a5382ed1  B[6]=4f20da94  C[6]=2e680288  D[6]=8f5a09b0
A[7]=d81397d5  B[7]=687c3797  C[7]=c18a1c24  D[7]=77ef9c1f

Feed-Forward Step 2: (r=29, s= 9)
A[0]=f546090e  B[0]=8f541e2f  C[0]=387ebab4  D[0]=d8559fac
A[1]=e8662c9c  B[1]=d44da49a  C[1]=b58e6fa6  D[1]=dfef9292
A[2]=4d45b1fd  B[2]=32f92999  C[2]=c4943900  D[2]=66344839
A[3]=2556238f  B[3]=1743d0d9  C[3]=e9897dc3  D[3]=d1691a73
A[4]=ceb7f4ee  B[4]=9107e09c  C[4]=a72dfb48  D[4]=969374da
A[5]=cf1a860e  B[5]=b7b657a4  C[5]=c4204a39  D[5]=78c3e5fb
A[6]=c48923c7  B[6]=34a705da  C[6]=4f20da94  D[6]=2e680288
A[7]=0172aaaf  B[7]=bb0272fa  C[7]=687c3797  D[7]=c18a1c24

Feed-Forward Step 3: (r= 9, s=15)
A[0]=4abfd912  B[0]=8c121dea  C[0]=8f541e2f  D[0]=387ebab4
A[1]=d25976d8  B[1]=cc5939d0  C[1]=d44da49a  D[1]=b58e6fa6
```

```
A[2]=017293b2  B[2]=8b63fa9a  C[2]=32f92999  D[2]=c4943900
A[3]=269071d6  B[3]=ac471e4a  C[3]=1743d0d9  D[3]=e9897dc3
A[4]=0e9e16bd  B[4]=6fe9dd9d  C[4]=9107e09c  D[4]=a72dfb48
A[5]=e7ef8ddc  B[5]=350c1d9e  C[5]=b7b657a4  D[5]=c4204a39
A[6]=688ee646  B[6]=12478f89  C[6]=34a705da  D[6]=4f20da94
A[7]=a7258d06  B[7]=e5555e02  C[7]=bb0272fa  D[7]=687c3797
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
y[ 24.. 31] =   88   14   70  255  173  206  169   46
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
```

```
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc84f3ce  45b0a3aa  4155ef73  2812b971
        00dfbced  da8b6f80  626f1f5c  ab81a8e4
Z[17] = ecd63b3c  108d2fe9  ff2165eb  00df4ca8
        9f4f4ca8  14093cfa  650cb6d4  c306b358
```

```
Z[18] = d551468f  e95a9857  d47214e8  52c1e95a
        ea39ae1e  b5f5ee94  555e634e  3f9757fb
Z[19] = c76158da  6967e79c  de07b437  2d4c31a7
        b358a2cb  a6479e70  1f5cb279  69670df0
Z[20] = 2aafd70f  d630571c  3f975a98  ad3fc5a3
        4e66d0f6  bf8a65eb  923ead3f  a5682c6d
Z[21] = ecd6547f  aefd23b7  fba59936  6ea15103
        1f5cef73  23b7ecd6  045bdc49  397e3a5d
Z[22] = fc84e79c  c069b971  9af4a2cb  15c74bc9
        4a0b3286  484d95ba  52c1053a  4234f210
Z[23] = fac64d87  f90894db  4a0b1be0  5103f4ad
        b97107d7  f3ce57fb  6967ba50  2c6d43f2
Z[24] = ac602d4c  563dae1e  0a749af4  2654037c
        ee94b437  14091864  41551f5c  5d35211a
Z[25] = 563dd551  9f4fb279  44d1da8b  5c56642d
        4f450c32  a02efe42  59b9d393  9a152812
Z[26] = d8cdb892  b892d8cd  a3aa52c1  00df5b77
        4ca8aefd  116cf052  36e11a22  29d05e14
Z[27] = 5ef3650c  e3414d87  f4add0f6  08b601be
        36e1d393  0b533b3c  431353a0  b279c3e5
Z[28] = db6ae341  e95a1e7d  b19ae0a4  0995ebf7
        08b6aaa2  fac61e7d  a8e46967  9cb29778
Z[29] = 9857492c  01be1864  563dab81  108dcd7a
        468fa726  9e70476e  e341a8e4  d1d55b77
Z[30] = 6a465e14  f131634e  0000e420  a10dd551
        58da476e  9cb20df0  36e1d70f  06f8b0bb
Z[31] = 3444cc9b  336521f9  2812e341  b0bb9857
        f131ad3f  3444f2ef  626f1f5c  e6bdc5a3
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
```

```
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ecd63b3c  108d2fe9  ff2165eb  00df4ca8
        9f4f4ca8  14093cfa  650cb6d4  c306b358
W[17] = d551468f  e95a9857  d47214e8  52c1e95a
        ea39ae1e  b5f5ee94  555e634e  3f9757fb
W[18] = fac64d87  f90894db  4a0b1be0  5103f4ad
        b97107d7  f3ce57fb  6967ba50  2c6d43f2
W[19] = 2aafd70f  d630571c  3f975a98  ad3fc5a3
        4e66d0f6  bf8a65eb  923ead3f  a5682c6d
W[20] = fc84e79c  c069b971  9af4a2cb  15c74bc9
        4a0b3286  484d95ba  52c1053a  4234f210
W[21] = ecd6547f  aefd23b7  fba59936  6ea15103
        1f5cef73  23b7ecd6  045bdc49  397e3a5d
W[22] = fc84f3ce  45b0a3aa  4155ef73  2812b971
        00dfbced  da8b6f80  626f1f5c  ab81a8e4
W[23] = c76158da  6967e79c  de07b437  2d4c31a7
        b358a2cb  a6479e70  1f5cb279  69670df0
W[24] = 6a465e14  f131634e  0000e420  a10dd551
        58da476e  9cb20df0  36e1d70f  06f8b0bb
W[25] = ac602d4c  563dae1e  0a749af4  2654037c
        ee94b437  14091864  41551f5c  5d35211a
W[26] = 563dd551  9f4fb279  44d1da8b  5c56642d
        4f450c32  a02efe42  59b9d393  9a152812
W[27] = 3444cc9b  336521f9  2812e341  b0bb9857
        f131ad3f  3444f2ef  626f1f5c  e6bdc5a3
W[28] = 5ef3650c  e3414d87  f4add0f6  08b601be
        36e1d393  0b533b3c  431353a0  b279c3e5
W[29] = 9857492c  01be1864  563dab81  108dcd7a
        468fa726  9e70476e  e341a8e4  d1d55b77
W[30] = db6ae341  e95a1e7d  b19ae0a4  0995ebf7
        08b6aaa2  fac61e7d  a8e46967  9cb29778
W[31] = d8cdb892  b892d8cd  a3aa52c1  00df5b77
        4ca8aefd  116cf052  36e11a22  29d05e14
```

Feistel Steps

```
IV :
```

```
A[0]=4abfd912  B[0]=8c121dea  C[0]=8f541e2f  D[0]=387ebab4
A[1]=d25976d8  B[1]=cc5939d0  C[1]=d44da49a  D[1]=b58e6fa6
A[2]=017293b2  B[2]=8b63fa9a  C[2]=32f92999  D[2]=c4943900
A[3]=269071d6  B[3]=ac471e4a  C[3]=1743d0d9  D[3]=e9897dc3
A[4]=0e9e16bd  B[4]=6fe9dd9d  C[4]=9107e09c  D[4]=a72dfb48
A[5]=e7ef8ddc  B[5]=350c1d9e  C[5]=b7b657a4  D[5]=c4204a39
A[6]=688ee646  B[6]=12478f89  C[6]=34a705da  D[6]=4f20da94
A[7]=a7258d06  B[7]=e5555e02  C[7]=bb0272fa  D[7]=687c3797

IV XOR M :
A[0]=b54026ed  B[0]=8c121dea  C[0]=8f541e2f  D[0]=387ebab4
A[1]=d2a78927  B[1]=cc5939d0  C[1]=d44da49a  D[1]=b58e6fa6
A[2]=017293b2  B[2]=8b63fa9a  C[2]=32f92999  D[2]=c4943900
A[3]=269071d6  B[3]=ac471e4a  C[3]=1743d0d9  D[3]=e9897dc3
A[4]=0e9e16bd  B[4]=6fe9dd9d  C[4]=9107e09c  D[4]=a72dfb48
A[5]=e7ef8ddc  B[5]=350c1d9e  C[5]=b7b657a4  D[5]=c4204a39
A[6]=688ee646  B[6]=12478f89  C[6]=34a705da  D[6]=4f20da94
A[7]=a7258d06  B[7]=e5555e02  C[7]=bb0272fa  D[7]=687c3797

Step  0: (r= 3, s=20)
A[0]=efb734e9  B[0]=aa01376d  C[0]=8c121dea  D[0]=8f541e2f
A[1]=022a699b  B[1]=953c493e  C[1]=cc5939d0  D[1]=d44da49a
A[2]=20c17674  B[2]=0b949d90  C[2]=8b63fa9a  D[2]=32f92999
A[3]=e5c5807d  B[3]=34838eb1  C[3]=ac471e4a  D[3]=1743d0d9
A[4]=cd7c6d53  B[4]=74f0b5e8  C[4]=6fe9dd9d  D[4]=9107e09c
A[5]=5d11de67  B[5]=3f7c6ee7  C[5]=350c1d9e  D[5]=b7b657a4
A[6]=118813d6  B[6]=44773233  C[6]=12478f89  D[6]=34a705da
A[7]=fb441ef0  B[7]=392c6835  C[7]=e5555e02  D[7]=bb0272fa

Step  1: (r=20, s=14)
A[0]=f919adef  B[0]=4e9efb73  C[0]=aa01376d  D[0]=8c121dea
A[1]=78b95922  B[1]=99b022a6  C[1]=953c493e  D[1]=cc5939d0
A[2]=6cd72552  B[2]=67420c17  C[2]=0b949d90  D[2]=8b63fa9a
A[3]=452aeabd  B[3]=07de5c58  C[3]=34838eb1  D[3]=ac471e4a
A[4]=2d75a54f  B[4]=d53cd7c6  C[4]=74f0b5e8  D[4]=6fe9dd9d
A[5]=c2edf459  B[5]=e675d11d  C[5]=3f7c6ee7  D[5]=350c1d9e
A[6]=bf4f9d03  B[6]=3d611881  C[6]=44773233  D[6]=12478f89
A[7]=525cfeb2  B[7]=ef0fb441  C[7]=392c6835  D[7]=e5555e02

Step  2: (r=14, s=27)
A[0]=bf8a9310  B[0]=6b7bfe46  C[0]=4e9efb73  D[0]=aa01376d
A[1]=8871ef3e  B[1]=56489e2e  C[1]=99b022a6  D[1]=953c493e
A[2]=0a0d0d06  B[2]=c9549b35  C[2]=67420c17  D[2]=0b949d90
A[3]=387984db  B[3]=baaf514a  C[3]=07de5c58  D[3]=34838eb1
A[4]=aee55328  B[4]=6953cb5d  C[4]=d53cd7c6  D[4]=74f0b5e8
A[5]=b39a8ddb  B[5]=7d1670bb  C[5]=e675d11d  D[5]=3f7c6ee7
A[6]=4b96854b  B[6]=e740efd3  C[6]=3d611881  D[6]=44773233
A[7]=86dbc494  B[7]=3fac9497  C[7]=ef0fb441  D[7]=392c6835
```

```
Step  3: (r=27, s= 3)
A[0]=146a8d67  B[0]=85fc5498  C[0]=6b7bfe46  D[0]=4e9efb73
A[1]=1160e3da  B[1]=f4438f79  C[1]=56489e2e  D[1]=99b022a6
A[2]=466a7417  B[2]=30506868  C[2]=c9549b35  D[2]=67420c17
A[3]=a4dd7fb2  B[3]=d9c3cc26  C[3]=baaf514a  D[3]=07de5c58
A[4]=deae22dd  B[4]=45772a99  C[4]=6953cb5d  D[4]=d53cd7c6
A[5]=33d9180e  B[5]=dd9cd46e  C[5]=7d1670bb  D[5]=e675d11d
A[6]=bc897b2e  B[6]=5a5cb42a  C[6]=e740efd3  D[6]=3d611881
A[7]=8feefc65  B[7]=a436de24  C[7]=3fac9497  D[7]=ef0fb441

Step  4: (r= 3, s=20)
A[0]=0ba9b641  B[0]=a3546b38  C[0]=85fc5498  D[0]=6b7bfe46
A[1]=37250d3d  B[1]=8b071ed0  C[1]=f4438f79  D[1]=56489e2e
A[2]=ddb4f92e  B[2]=3353a0ba  C[2]=30506868  D[2]=c9549b35
A[3]=34aa4bb5  B[3]=26ebfd95  C[3]=d9c3cc26  D[3]=baaf514a
A[4]=3116a141  B[4]=f57116ee  C[4]=45772a99  D[4]=6953cb5d
A[5]=99f6aaa4  B[5]=9ec8c071  C[5]=dd9cd46e  D[5]=7d1670bb
A[6]=5d2d3e19  B[6]=e44bd975  C[6]=5a5cb42a  D[6]=e740efd3
A[7]=7092beb1  B[7]=7f77e32c  C[7]=a436de24  D[7]=3fac9497

Step  5: (r=20, s=14)
A[0]=c18ba65a  B[0]=6410ba9b  C[0]=a3546b38  D[0]=85fc5498
A[1]=ae255306  B[1]=d3d37250  C[1]=8b071ed0  D[1]=f4438f79
A[2]=af9727be  B[2]=92eddb4f  C[2]=3353a0ba  D[2]=30506868
A[3]=2c60a3bc  B[3]=bb534aa4  C[3]=26ebfd95  D[3]=d9c3cc26
A[4]=59b0b818  B[4]=1413116a  C[4]=f57116ee  D[4]=45772a99
A[5]=73655eb8  B[5]=aa499f6a  C[5]=9ec8c071  D[5]=dd9cd46e
A[6]=f7ae103c  B[6]=e195d2d3  C[6]=e44bd975  D[6]=5a5cb42a
A[7]=db135f5b  B[7]=eb17092b  C[7]=7f77e32c  D[7]=a436de24

Step  6: (r=14, s=27)
A[0]=1dae0107  B[0]=e996b062  C[0]=6410ba9b  D[0]=a3546b38
A[1]=f20c2457  B[1]=54c1ab89  C[1]=d3d37250  D[1]=8b071ed0
A[2]=95973343  B[2]=c9efabe5  C[2]=92eddb4f  D[2]=3353a0ba
A[3]=8652e574  B[3]=28ef0b18  C[3]=bb534aa4  D[3]=26ebfd95
A[4]=ac9d7a85  B[4]=2e06166c  C[4]=1413116a  D[4]=f57116ee
A[5]=803806f4  B[5]=57ae1cd9  C[5]=aa499f6a  D[5]=9ec8c071
A[6]=c8ec15ab  B[6]=840f3deb  C[6]=e195d2d3  D[6]=e44bd975
A[7]=e5023a08  B[7]=d7d6f6c4  C[7]=eb17092b  D[7]=7f77e32c

Step  7: (r=27, s= 3)
A[0]=99774ed3  B[0]=38ed7008  C[0]=e996b062  D[0]=6410ba9b
A[1]=8fbd0737  B[1]=bf906122  C[1]=54c1ab89  D[1]=d3d37250
A[2]=8fcce522  B[2]=1cacb99a  C[2]=c9efabe5  D[2]=92eddb4f
A[3]=69fc54d9  B[3]=a432972b  C[3]=28ef0b18  D[3]=bb534aa4
A[4]=9620b799  B[4]=2d64ebd4  C[4]=2e06166c  D[4]=1413116a
A[5]=bb88f11a  B[5]=a401c037  C[5]=57ae1cd9  D[5]=aa499f6a
A[6]=1ca24efd  B[6]=5e4760ad  C[6]=840f3deb  D[6]=e195d2d3
A[7]=e299840f  B[7]=472811d0  C[7]=d7d6f6c4  D[7]=eb17092b
```

```
Step  8: (r=26, s= 4)
A[0]=63795a6c  B[0]=4e65dd3b  C[0]=38ed7008  D[0]=e996b062
A[1]=32e74068  B[1]=de3ef41c  C[1]=bf906122  D[1]=54c1ab89
A[2]=73643983  B[2]=8a3f3394  C[2]=1cacb99a  D[2]=c9efabe5
A[3]=267a01bd  B[3]=65a7f153  C[3]=a432972b  D[3]=28ef0b18
A[4]=aa05d117  B[4]=665882de  C[4]=2d64ebd4  D[4]=2e06166c
A[5]=032ea4d9  B[5]=6aee23c4  C[5]=a401c037  D[5]=57ae1cd9
A[6]=3474254c  B[6]=f472893b  C[6]=5e4760ad  D[6]=840f3deb
A[7]=cb7c959d  B[7]=3f8a6610  C[7]=472811d0  D[7]=d7d6f6c4

Step  9: (r= 4, s=23)
A[0]=ff0d3933  B[0]=3795a6c6  C[0]=4e65dd3b  D[0]=38ed7008
A[1]=6a0e2b84  B[1]=2e740683  C[1]=de3ef41c  D[1]=bf906122
A[2]=defd42e6  B[2]=36439837  C[2]=8a3f3394  D[2]=1cacb99a
A[3]=0e5e2c66  B[3]=67a01bd2  C[3]=65a7f153  D[3]=a432972b
A[4]=1c83cc03  B[4]=a05d117a  C[4]=665882de  D[4]=2d64ebd4
A[5]=5fccfb75  B[5]=32ea4d90  C[5]=6aee23c4  D[5]=a401c037
A[6]=6c7a2546  B[6]=474254c3  C[6]=f472893b  D[6]=5e4760ad
A[7]=75bd94b9  B[7]=b7c959dc  C[7]=3f8a6610  D[7]=472811d0

Step 10: (r=23, s=11)
A[0]=2876b959  B[0]=99ff869c  C[0]=3795a6c6  D[0]=4e65dd3b
A[1]=83de9069  B[1]=c2350715  C[1]=2e740683  D[1]=de3ef41c
A[2]=ebac760c  B[2]=736f7ea1  C[2]=36439837  D[2]=8a3f3394
A[3]=42ecfa84  B[3]=33072f16  C[3]=67a01bd2  D[3]=65a7f153
A[4]=f48513cd  B[4]=018e41e6  C[4]=a05d117a  D[4]=665882de
A[5]=2a11ed35  B[5]=baafe67d  C[5]=32ea4d90  D[5]=6aee23c4
A[6]=f6c5de67  B[6]=a3363d12  C[6]=474254c3  D[6]=f472893b
A[7]=2bc9883e  B[7]=5cbadeca  C[7]=b7c959dc  D[7]=3f8a6610

Step 11: (r=11, s=26)
A[0]=fd426927  B[0]=b5cac943  C[0]=99ff869c  D[0]=3795a6c6
A[1]=4eb9a221  B[1]=f4834c1e  C[1]=c2350715  D[1]=2e740683
A[2]=171cad55  B[2]=63b0675d  C[2]=736f7ea1  D[2]=36439837
A[3]=eaf3d255  B[3]=67d42217  C[3]=33072f16  D[3]=67a01bd2
A[4]=eb2dcb59  B[4]=289e6fa4  C[4]=018e41e6  D[4]=a05d117a
A[5]=8f5d33c3  B[5]=8f69a950  C[5]=baafe67d  D[5]=32ea4d90
A[6]=fee7173a  B[6]=2ef33fb6  C[6]=a3363d12  D[6]=474254c3
A[7]=6c79bdfe  B[7]=4c41f15e  C[7]=5cbadeca  D[7]=b7c959dc

Step 12: (r=26, s= 4)
A[0]=5400e4fb  B[0]=9ff509a4  C[0]=b5cac943  D[0]=99ff869c
A[1]=eed6aede  B[1]=853ae688  C[1]=f4834c1e  D[1]=c2350715
A[2]=812c3c87  B[2]=545c72b5  C[2]=63b0675d  D[2]=736f7ea1
A[3]=d5705cd6  B[3]=57abcf49  C[3]=67d42217  D[3]=33072f16
A[4]=c92e473f  B[4]=67acb72d  C[4]=289e6fa4  D[4]=018e41e6
A[5]=954ccf34  B[5]=0e3d74cf  C[5]=8f69a950  D[5]=baafe67d
A[6]=0440638b  B[6]=ebfb9c5c  C[6]=2ef33fb6  D[6]=a3363d12
```

```
A[7]=e76deea6  B[7]=f9b1e6f7  C[7]=4c41f15e  D[7]=5cbadeca

Step 13: (r= 4, s=23)
A[0]=5fb0a998  B[0]=400e4fb5  C[0]=9ff509a4  D[0]=b5cac943
A[1]=9659eac6  B[1]=ed6aedee  C[1]=853ae688  D[1]=f4834c1e
A[2]=0d0c6bad  B[2]=12c3c878  C[2]=545c72b5  D[2]=63b0675d
A[3]=87b7475a  B[3]=5705cd6d  C[3]=57abcf49  D[3]=67d42217
A[4]=cfd91b91  B[4]=92e473fc  C[4]=67acb72d  D[4]=289e6fa4
A[5]=305b8166  B[5]=54ccf349  C[5]=0e3d74cf  D[5]=8f69a950
A[6]=b9c19c3c  B[6]=440638b0  C[6]=ebfb9c5c  D[6]=2ef33fb6
A[7]=0ddedb43  B[7]=76deea6e  C[7]=f9b1e6f7  D[7]=4c41f15e

Step 14: (r=23, s=11)
A[0]=77036714  B[0]=cc2fd854  C[0]=400e4fb5  D[0]=9ff509a4
A[1]=079df2c3  B[1]=634b2cf5  C[1]=ed6aedee  D[1]=853ae688
A[2]=d087ef1b  B[2]=d6868635  C[2]=12c3c878  D[2]=545c72b5
A[3]=72982a8e  B[3]=ad43dba3  C[3]=5705cd6d  D[3]=57abcf49
A[4]=c9ce5d24  B[4]=c8e7ec8d  C[4]=92e473fc  D[4]=67acb72d
A[5]=b9701bc6  B[5]=b3182dc0  C[5]=54ccf349  D[5]=0e3d74cf
A[6]=54614f26  B[6]=1e5ce0ce  C[6]=440638b0  D[6]=ebfb9c5c
A[7]=54b40fba  B[7]=a186ef6d  C[7]=76deea6e  D[7]=f9b1e6f7

Step 15: (r=11, s=26)
A[0]=c3d9e3a5  B[0]=1b38a3b8  C[0]=cc2fd854  D[0]=400e4fb5
A[1]=3c5f3045  B[1]=ef96183c  C[1]=634b2cf5  D[1]=ed6aedee
A[2]=7314c657  B[2]=3f78de84  C[2]=d6868635  D[2]=12c3c878
A[3]=c67d7559  B[3]=c1547394  C[3]=ad43dba3  D[3]=5705cd6d
A[4]=3521c981  B[4]=72e9264e  C[4]=c8e7ec8d  D[4]=92e473fc
A[5]=194ae7ee  B[5]=80de35cb  C[5]=b3182dc0  D[5]=54ccf349
A[6]=e52ffbaa  B[6]=0a7932a3  C[6]=1e5ce0ce  D[6]=440638b0
A[7]=0724b7c9  B[7]=a07dd2a5  C[7]=a186ef6d  D[7]=76deea6e

Step 16: (r=19, s=28)
A[0]=95ec1767  B[0]=1d2e1ecf  C[0]=1b38a3b8  D[0]=cc2fd854
A[1]=d3ff0277  B[1]=8229e2f9  C[1]=ef96183c  D[1]=634b2cf5
A[2]=2765b333  B[2]=32bb98a6  C[2]=3f78de84  D[2]=d6868635
A[3]=a6cf5a02  B[3]=aace33eb  C[3]=c1547394  D[3]=ad43dba3
A[4]=422278a2  B[4]=4c09a90e  C[4]=72e9264e  D[4]=c8e7ec8d
A[5]=1cbcaeee  B[5]=3f70ca57  C[5]=80de35cb  D[5]=b3182dc0
A[6]=6a80fb4b  B[6]=dd57297f  C[6]=0a7932a3  D[6]=1e5ce0ce
A[7]=9afff105  B[7]=be483925  C[7]=a07dd2a5  D[7]=a186ef6d

Step 17: (r=28, s= 7)
A[0]=91613c93  B[0]=795ec176  C[0]=1d2e1ecf  D[0]=1b38a3b8
A[1]=91dcd89d  B[1]=7d3ff027  C[1]=8229e2f9  D[1]=ef96183c
A[2]=129aa368  B[2]=32765b33  C[2]=32bb98a6  D[2]=3f78de84
A[3]=6f3c3a18  B[3]=2a6cf5a0  C[3]=aace33eb  D[3]=c1547394
A[4]=ac0c8c45  B[4]=2422278a  C[4]=4c09a90e  D[4]=72e9264e
A[5]=1a0bcc92  B[5]=e1cbcaee  C[5]=3f70ca57  D[5]=80de35cb
```

```
A[6]=3e592b68  B[6]=b6a80fb4  C[6]=dd57297f  D[6]=0a7932a3
A[7]=950951bb  B[7]=59afff10  C[7]=be483925  D[7]=a07dd2a5

Step 18: (r= 7, s=22)
A[0]=6bf5b106  B[0]=b09e49c8  C[0]=795ec176  D[0]=1d2e1ecf
A[1]=0bd4ab46  B[1]=ee6c4ec8  C[1]=7d3ff027  D[1]=8229e2f9
A[2]=889536d2  B[2]=4d51b409  C[2]=32765b33  D[2]=32bb98a6
A[3]=8f75747c  B[3]=9e1d0c37  C[3]=2a6cf5a0  D[3]=aace33eb
A[4]=6a01230b  B[4]=064622d6  C[4]=2422278a  D[4]=4c09a90e
A[5]=70b83e1f  B[5]=05e6490d  C[5]=e1cbcaee  D[5]=3f70ca57
A[6]=f9070a86  B[6]=2c95b41f  C[6]=b6a80fb4  D[6]=dd57297f
A[7]=9b6056eb  B[7]=84a8ddca  C[7]=59afff10  D[7]=be483925

Step 19: (r=22, s=19)
A[0]=7d4e4429  B[0]=419afd6c  C[0]=b09e49c8  D[0]=795ec176
A[1]=2b92e45b  B[1]=d182f52a  C[1]=ee6c4ec8  D[1]=7d3ff027
A[2]=24bba7f5  B[2]=b4a2254d  C[2]=4d51b409  D[2]=32765b33
A[3]=b4f70970  B[3]=1f23dd5d  C[3]=9e1d0c37  D[3]=2a6cf5a0
A[4]=45d00201  B[4]=c2da8048  C[4]=064622d6  D[4]=2422278a
A[5]=9afefc21  B[5]=87dc2e0f  C[5]=05e6490d  D[5]=e1cbcaee
A[6]=94471763  B[6]=a1be41c2  C[6]=2c95b41f  D[6]=b6a80fb4
A[7]=3a850060  B[7]=bae6d815  C[7]=84a8ddca  D[7]=59afff10

Step 20: (r=19, s=28)
A[0]=d1517bfe  B[0]=214bea72  C[0]=419afd6c  D[0]=b09e49c8
A[1]=43deb350  B[1]=22d95c97  C[1]=d182f52a  D[1]=ee6c4ec8
A[2]=0aa791ec  B[2]=3fa925dd  C[2]=b4a2254d  D[2]=4d51b409
A[3]=2d8fdaca  B[3]=4b85a7b8  C[3]=1f23dd5d  D[3]=9e1d0c37
A[4]=ec5ccdbc  B[4]=100a2e80  C[4]=c2da8048  D[4]=064622d6
A[5]=6b2bab4b  B[5]=e10cd7f7  C[5]=87dc2e0f  D[5]=05e6490d
A[6]=1de1d6cb  B[6]=bb1ca238  C[6]=a1be41c2  D[6]=2c95b41f
A[7]=c0853ece  B[7]=0301d428  C[7]=bae6d815  D[7]=84a8ddca

Step 21: (r=28, s= 7)
A[0]=28f75c0d  B[0]=ed1517bf  C[0]=214bea72  D[0]=419afd6c
A[1]=450cc69c  B[1]=043deb35  C[1]=22d95c97  D[1]=d182f52a
A[2]=ba4e9e02  B[2]=c0aa791e  C[2]=3fa925dd  D[2]=b4a2254d
A[3]=275c7443  B[3]=a2d8fdac  C[3]=4b85a7b8  D[3]=1f23dd5d
A[4]=b0ad865e  B[4]=cec5ccdb  C[4]=100a2e80  D[4]=c2da8048
A[5]=417aecf2  B[5]=b6b2bab4  C[5]=e10cd7f7  D[5]=87dc2e0f
A[6]=25ef6650  B[6]=b1de1d6c  C[6]=bb1ca238  D[6]=a1be41c2
A[7]=0d2cd454  B[7]=ec0853ec  C[7]=0301d428  D[7]=bae6d815

Step 22: (r= 7, s=22)
A[0]=74c407d9  B[0]=7bae0694  C[0]=ed1517bf  D[0]=214bea72
A[1]=d1f9fc6b  B[1]=86634e22  C[1]=043deb35  D[1]=22d95c97
A[2]=3522a1b4  B[2]=274f015d  C[2]=c0aa791e  D[2]=3fa925dd
A[3]=745df43b  B[3]=ae3a2193  C[3]=a2d8fdac  D[3]=4b85a7b8
A[4]=b20f3386  B[4]=56c32f58  C[4]=cec5ccdb  D[4]=100a2e80
```

```
A[5]=489fea04  B[5]=bd767920  C[5]=b6b2bab4  D[5]=e10cd7f7
A[6]=6c10d103  B[6]=f7b32812  C[6]=b1de1d6c  D[6]=bb1ca238
A[7]=d50ae2e9  B[7]=966a2a06  C[7]=ec0853ec  D[7]=0301d428

Step 23: (r=22, s=19)
A[0]=38f7b556  B[0]=f65d3101  C[0]=7bae0694  D[0]=ed1517bf
A[1]=13c2add3  B[1]=1af47e7f  C[1]=86634e22  D[1]=043deb35
A[2]=1a5d1b0b  B[2]=6d0d48a8  C[2]=274f015d  D[2]=c0aa791e
A[3]=33463c0e  B[3]=0edd177d  C[3]=ae3a2193  D[3]=a2d8fdac
A[4]=ff8a0251  B[4]=e1ac83cc  C[4]=56c32f58  D[4]=cec5ccdb
A[5]=9f4e9eda  B[5]=811227fa  C[5]=bd767920  D[5]=b6b2bab4
A[6]=daabc903  B[6]=40db0434  C[6]=f7b32812  D[6]=b1de1d6c
A[7]=36ff1b17  B[7]=ba7542b8  C[7]=966a2a06  D[7]=ec0853ec

Step 24: (r=15, s= 5)
A[0]=adfeb45a  B[0]=daab1c7b  C[0]=f65d3101  D[0]=7bae0694
A[1]=64c2bb4c  B[1]=56e989e1  C[1]=1af47e7f  D[1]=86634e22
A[2]=d553cd00  B[2]=8d858d2e  C[2]=6d0d48a8  D[2]=274f015d
A[3]=d9e2a088  B[3]=1e0719a3  C[3]=0edd177d  D[3]=ae3a2193
A[4]=7c95c1c8  B[4]=0128ffc5  C[4]=e1ac83cc  D[4]=56c32f58
A[5]=940f13a3  B[5]=4f6d4fa7  C[5]=811227fa  D[5]=bd767920
A[6]=58ee2ce8  B[6]=e481ed55  C[6]=40db0434  D[6]=f7b32812
A[7]=9346c449  B[7]=8d8b9b7f  C[7]=ba7542b8  D[7]=966a2a06

Step 25: (r= 5, s=29)
A[0]=0ad0c941  B[0]=bfd68b55  C[0]=daab1c7b  D[0]=f65d3101
A[1]=a3c6ca51  B[1]=9857698c  C[1]=56e989e1  D[1]=1af47e7f
A[2]=fbb0b094  B[2]=aa79a01a  C[2]=8d858d2e  D[2]=6d0d48a8
A[3]=36ad112c  B[3]=3c54111b  C[3]=1e0719a3  D[3]=0edd177d
A[4]=9695b1f5  B[4]=92b8390f  C[4]=0128ffc5  D[4]=e1ac83cc
A[5]=63ac2061  B[5]=81e27472  C[5]=4f6d4fa7  D[5]=811227fa
A[6]=e1eb6787  B[6]=1dc59d0b  C[6]=e481ed55  D[6]=40db0434
A[7]=b57cce35  B[7]=68d88932  C[7]=8d8b9b7f  D[7]=ba7542b8

Step 26: (r=29, s= 9)
A[0]=e3f73415  B[0]=215a1928  C[0]=bfd68b55  D[0]=daab1c7b
A[1]=63329e0d  B[1]=3478d94a  C[1]=9857698c  D[1]=56e989e1
A[2]=56165ecc  B[2]=9f761612  C[2]=aa79a01a  D[2]=8d858d2e
A[3]=25fd218c  B[3]=86d5a225  C[3]=3c54111b  D[3]=1e0719a3
A[4]=daf3a9ae  B[4]=b2d2b63e  C[4]=92b8390f  D[4]=0128ffc5
A[5]=e4a25a70  B[5]=2c75840c  C[5]=81e27472  D[5]=4f6d4fa7
A[6]=e1430e8a  B[6]=fc3d6cf0  C[6]=1dc59d0b  D[6]=e481ed55
A[7]=ed62a222  B[7]=b6af99c6  C[7]=68d88932  D[7]=8d8b9b7f

Step 27: (r= 9, s=15)
A[0]=297e83d6  B[0]=ee682bc7  C[0]=215a1928  D[0]=bfd68b55
A[1]=9766032b  B[1]=653c1ac6  C[1]=3478d94a  D[1]=9857698c
A[2]=995dcfce  B[2]=2cbd98ac  C[2]=9f761612  D[2]=aa79a01a
A[3]=b64d3ba5  B[3]=fa43184b  C[3]=86d5a225  D[3]=3c54111b
```

```
A[4]=9d01ee61  B[4]=e7535db5  C[4]=b2d2b63e  D[4]=92b8390f
A[5]=98886f4f  B[5]=44b4e1c9  C[5]=2c75840c  D[5]=81e27472
A[6]=81d6ba67  B[6]=861d15c2  C[6]=fc3d6cf0  D[6]=1dc59d0b
A[7]=ef5d24cc  B[7]=c54445da  C[7]=b6af99c6  D[7]=68d88932

Step 28: (r=15, s= 5)
A[0]=0a15509c  B[0]=41eb14bf  C[0]=ee682bc7  D[0]=215a1928
A[1]=64856075  B[1]=0195cbb3  C[1]=653c1ac6  D[1]=3478d94a
A[2]=3274ceed  B[2]=e7e74cae  C[2]=2cbd98ac  D[2]=9f761612
A[3]=51d0ec8d  B[3]=9dd2db26  C[3]=fa43184b  D[3]=86d5a225
A[4]=55692734  B[4]=f730ce80  C[4]=e7535db5  D[4]=b2d2b63e
A[5]=34836df3  B[5]=37a7cc44  C[5]=44b4e1c9  D[5]=2c75840c
A[6]=312c296a  B[6]=5d33c0eb  C[6]=861d15c2  D[6]=fc3d6cf0
A[7]=b11e1d8b  B[7]=926677ae  C[7]=c54445da  D[7]=b6af99c6

Step 29: (r= 5, s=29)
A[0]=af1d2c04  B[0]=42aa1381  C[0]=41eb14bf  D[0]=ee682bc7
A[1]=ed97193e  B[1]=90ac0eac  C[1]=0195cbb3  D[1]=653c1ac6
A[2]=263f4548  B[2]=4e99dda6  C[2]=e7e74cae  D[2]=2cbd98ac
A[3]=5ed2d7a1  B[3]=3a1d91aa  C[3]=9dd2db26  D[3]=fa43184b
A[4]=439fa2e9  B[4]=ad24e68a  C[4]=f730ce80  D[4]=e7535db5
A[5]=a3b5689d  B[5]=906dbe66  C[5]=37a7cc44  D[5]=44b4e1c9
A[6]=8bbc6981  B[6]=25852d46  C[6]=5d33c0eb  D[6]=861d15c2
A[7]=73a727be  B[7]=23c3b176  C[7]=926677ae  D[7]=c54445da

Step 30: (r=29, s= 9)
A[0]=cabbff11  B[0]=95e3a580  C[0]=42aa1381  D[0]=41eb14bf
A[1]=880190d0  B[1]=ddb2e327  C[1]=90ac0eac  D[1]=0195cbb3
A[2]=e404a99d  B[2]=04c7e8a9  C[2]=4e99dda6  D[2]=e7e74cae
A[3]=8023bca2  B[3]=2bda5af4  C[3]=3a1d91aa  D[3]=9dd2db26
A[4]=a9b81aa2  B[4]=2873f45d  C[4]=ad24e68a  D[4]=f730ce80
A[5]=46a0fe8f  B[5]=b476ad13  C[5]=906dbe66  D[5]=37a7cc44
A[6]=4b84bba0  B[6]=31778d30  C[6]=25852d46  D[6]=5d33c0eb
A[7]=520dc6ab  B[7]=ce74e4f7  C[7]=23c3b176  D[7]=926677ae

Step 31: (r= 9, s=15)
A[0]=b29eb405  B[0]=77fe2395  C[0]=95e3a580  D[0]=42aa1381
A[1]=d58f47f1  B[1]=0321a110  C[1]=ddb2e327  D[1]=90ac0eac
A[2]=ce05a8a2  B[2]=09533bc8  C[2]=04c7e8a9  D[2]=4e99dda6
A[3]=032d3b0a  B[3]=47794500  C[3]=2bda5af4  D[3]=3a1d91aa
A[4]=b2021a1a  B[4]=70354553  C[4]=2873f45d  D[4]=ad24e68a
A[5]=c0708fcc  B[5]=41fd1e8d  C[5]=b476ad13  D[5]=906dbe66
A[6]=4d6a1695  B[6]=09774097  C[6]=31778d30  D[6]=25852d46
A[7]=a4d6443e  B[7]=1b8d56a4  C[7]=ce74e4f7  D[7]=23c3b176

Feed-Forward Step 0: (r=15, s= 5)
A[0]=511aaddf  B[0]=5a02d94f  C[0]=77fe2395  D[0]=95e3a580
A[1]=e0e7ac9c  B[1]=a3f8eac7  C[1]=0321a110  D[1]=ddb2e327
A[2]=b7803dc1  B[2]=d4516702  C[2]=09533bc8  D[2]=04c7e8a9
```

```
A[3]=697a1593  B[3]=9d850196  C[3]=47794500  D[3]=2bda5af4
A[4]=ce829416  B[4]=0d0d5901  C[4]=70354553  D[4]=2873f45d
A[5]=a77cb53e  B[5]=47e66038  C[5]=41fd1e8d  D[5]=b476ad13
A[6]=1392faa3  B[6]=0b4aa6b5  C[6]=09774097  D[6]=31778d30
A[7]=bd0f12d7  B[7]=221f526b  C[7]=1b8d56a4  D[7]=ce74e4f7

Feed-Forward Step 1: (r= 5, s=29)
A[0]=2323420d  B[0]=2355bbea  C[0]=5a02d94f  D[0]=77fe2395
A[1]=99004b3c  B[1]=1cf5939c  C[1]=a3f8eac7  D[1]=0321a110
A[2]=88e59d33  B[2]=f007b836  C[2]=d4516702  D[2]=09533bc8
A[3]=39d9eaf6  B[3]=2f42b26d  C[3]=9d850196  D[3]=47794500
A[4]=ecf1b8c9  B[4]=d05282d9  C[4]=0d0d5901  D[4]=70354553
A[5]=e80f59a4  B[5]=ef96a7d4  C[5]=47e66038  D[5]=41fd1e8d
A[6]=9a375ac6  B[6]=725f5462  C[6]=0b4aa6b5  D[6]=09774097
A[7]=8a61daff  B[7]=a1e25af7  C[7]=221f526b  D[7]=1b8d56a4

Feed-Forward Step 2: (r=29, s= 9)
A[0]=99065863  B[0]=a4646841  C[0]=2355bbea  D[0]=5a02d94f
A[1]=a319fd7c  B[1]=93200967  C[1]=1cf5939c  D[1]=a3f8eac7
A[2]=61c11154  B[2]=711cb3a6  C[2]=f007b836  D[2]=d4516702
A[3]=4110b131  B[3]=c73b3d5e  C[3]=2f42b26d  D[3]=9d850196
A[4]=fb0aaee3  B[4]=3d9e3719  C[4]=d05282d9  D[4]=0d0d5901
A[5]=a44c4f79  B[5]=9d01eb34  C[5]=ef96a7d4  D[5]=47e66038
A[6]=8f95d209  B[6]=d346eb58  C[6]=725f5462  D[6]=0b4aa6b5
A[7]=c0ad932f  B[7]=f14c3b5f  C[7]=a1e25af7  D[7]=221f526b

Feed-Forward Step 3: (r= 9, s=15)
A[0]=d543e261  B[0]=0cb0c732  C[0]=a4646841  D[0]=2355bbea
A[1]=4bc7effd  B[1]=33faf946  C[1]=93200967  D[1]=1cf5939c
A[2]=58385815  B[2]=8222a8c3  C[2]=711cb3a6  D[2]=f007b836
A[3]=b4815ab1  B[3]=21626282  C[3]=c73b3d5e  D[3]=2f42b26d
A[4]=c9e23dfc  B[4]=155dc7f6  C[4]=3d9e3719  D[4]=d05282d9
A[5]=ff0de712  B[5]=989ef348  C[5]=9d01eb34  D[5]=ef96a7d4
A[6]=a5fc4fa0  B[6]=2ba4131f  C[6]=d346eb58  D[6]=725f5462
A[7]=14531876  B[7]=5b265f81  C[7]=f14c3b5f  D[7]=a1e25af7
```

Compression Function Output

```
A[0]=d543e261  B[0]=0cb0c732  C[0]=a4646841  D[0]=2355bbea
A[1]=4bc7effd  B[1]=33faf946  C[1]=93200967  D[1]=1cf5939c
A[2]=58385815  B[2]=8222a8c3  C[2]=711cb3a6  D[2]=f007b836
A[3]=b4815ab1  B[3]=21626282  C[3]=c73b3d5e  D[3]=2f42b26d
A[4]=c9e23dfc  B[4]=155dc7f6  C[4]=3d9e3719  D[4]=d05282d9
A[5]=ff0de712  B[5]=989ef348  C[5]=9d01eb34  D[5]=ef96a7d4
A[6]=a5fc4fa0  B[6]=2ba4131f  C[6]=d346eb58  D[6]=725f5462
A[7]=14531876  B[7]=5b265f81  C[7]=f14c3b5f  D[7]=a1e25af7
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
```

```
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   61  165  253   25  100  103   38  217
y[  8.. 15] =   83  222  217   81  155  191  230   68
y[ 16.. 23] =  160   84  131  211  120  256   67  256
y[ 24.. 31] =   70  153   56  134  184   54   47  116
y[ 32.. 39] =    3  142  144  243   16   32   20   71
y[ 40.. 47] =   63   73  194  216  243  207  172  210
y[ 48.. 55] =  183  243   53   83  146   42  138  255
y[ 56.. 63] =  108  123  230   72  215  135    9   14
y[ 64.. 71] =  119  197   87   94   48   28  240   38
y[ 72.. 79] =   57  190   59  107  148  226  117  121
y[ 80.. 87] =  177  224  217  112   89  175   90   39
y[ 88.. 95] =   72  226   62  109  209  193  100  189
y[ 96..103] =  243  143  181  173  213  195   59  237
y[104..111] =  200   30   90  227   52  251   86   58
y[112..119] =   43   98  145   86  103  101  123  134
y[120..127] =   12   87   90  153  210  217   69   88
y[128..135] =   49  202  114   85   10    7   72  150
y[136..143] =   27  145  150   29  212  176  137   42
y[144..151] =  207   26  236  156  247  111   43  111
y[152..159] =   40  214   54  233  183   56   63  251
y[160..167] =  107  225  223  124   94   78   90   39
y[168..175] =   47   37  173  151  124  160  195  157
y[176..183] =  184  124   57   27  221   68  229  112
y[184..191] =    2  244  137   38  152  232  101   96
y[192..199] =  248  170   23   16   62   82  127   72
y[200..207] =   53  177   51    3  219  141  250  246
y[208..215] =  190  143  150  255   21  192   20   71
y[216..223] =   38  141   48    1  158  174   10  178
y[224..231] =  124  224  186  194  154  172   51  130
y[232..239] =  167   80   20  140   58  116   24   52
y[240..247] =   67   12  222   24    7    9  244  233
y[248..255] =   98   23   20  214  157  150   41   22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2aaf3523  634efc84  08b6571c  3eb8211a
        1785484d  a2cbdd28  d8cda726  9778e87b
Z[17] = d472ab81  edb5923e  f74a6888  25753a5d
        22d83cfa  2f0a30c8  bf8ac069  36e128f1
Z[18] = 5d35029d  e2629d91  51e20df0  4e66116c
        28f136e1  b6d4c91f  6c04f3ce  c9feb5f5
Z[19] = c069bf8a  31a72e2b  e0a49f4f  e79c9857
        01be5e14  9778e87b  a489db6a  57fb07d7
Z[20] = f82967a9  14094bc9  360229d0  6ea1f131
        2e2b31a7  2c6d3365  dee6a10d  f9e765eb
Z[21] = c5a3ba50  a2cbdd28  124b4d87  116c4e66
        211a3eb8  29d03602  a9c3d630  08b6571c
Z[22] = 6c04f3ce  c227bdcc  a647d9ac  2c6d3365
        b19ace59  116c4e66  32862d4c  14e84aea
Z[23] = 3a5d2575  e1839e70  061959b9  f4ad6b25
        555e0a74  116c4e66  a8e4d70f  23b73c1b
```

```
Z[24] = d017afdc  4a0b15c7  061959b9  a2cbdd28
        9e70e183  1943468f  b971c682  24963b3c
Z[25] = 16a6492c  a805d7ee  60b1ff21  60b1ff21
        da8ba568  eb1894db  30c82f0a  fac6650c
Z[26] = e4209bd3  6c04f3ce  43f21be0  21f93dd9
        203b3f97  a3aadc49  ab81d472  a8e4d70f
Z[27] = 6c04f3ce  1785484d  3b3c2496  6190fe42
        f4ad6b25  211a3eb8  ea3995ba  53a00c32
Z[28] = b437cbbc  0df051e2  476e1864  3eb8211a
        ba50c5a3  029d5d35  9af4e4ff  f66b6967
Z[29] = 9cb2e341  fe426190  c761b892  3dd921f9
        9af4e4ff  00df5ef3  b7b3c840  bb2fc4c4
Z[30] = e3419cb2  c91fb6d4  b5f5c9fe  915fee94
        45b01a22  9a15e5de  650cfac6  2d4c3286
Z[31] = 0a74555e  14e84aea  07d757fb  eb1894db
        14094bc9  da8ba568  a2cbdd28  132a4ca8
```

Expanded Message

```
W[ 0] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
W[ 1] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
W[ 4] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
W[10] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
W[12] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
        ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
```

```
W[15] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
W[16] = d472ab81  edb5923e  f74a6888  25753a5d
        22d83cfa  2f0a30c8  bf8ac069  36e128f1
W[17] = 5d35029d  e2629d91  51e20df0  4e66116c
        28f136e1  b6d4c91f  6c04f3ce  c9feb5f5
W[18] = 3a5d2575  e1839e70  061959b9  f4ad6b25
        555e0a74  116c4e66  a8e4d70f  23b73c1b
W[19] = f82967a9  14094bc9  360229d0  6ea1f131
        2e2b31a7  2c6d3365  dee6a10d  f9e765eb
W[20] = 6c04f3ce  c227bdcc  a647d9ac  2c6d3365
        b19ace59  116c4e66  32862d4c  14e84aea
W[21] = c5a3ba50  a2cbdd28  124b4d87  116c4e66
        211a3eb8  29d03602  a9c3d630  08b6571c
W[22] = 2aaf3523  634efc84  08b6571c  3eb8211a
        1785484d  a2cbdd28  d8cda726  9778e87b
W[23] = c069bf8a  31a72e2b  e0a49f4f  e79c9857
        01be5e14  9778e87b  a489db6a  57fb07d7
W[24] = e3419cb2  c91fb6d4  b5f5c9fe  915fee94
        45b01a22  9a15e5de  650cfac6  2d4c3286
W[25] = d017afdc  4a0b15c7  061959b9  a2cbdd28
        9e70e183  1943468f  b971c682  24963b3c
W[26] = 16a6492c  a805d7ee  60b1ff21  60b1ff21
        da8ba568  eb1894db  30c82f0a  fac6650c
W[27] = 0a74555e  14e84aea  07d757fb  eb1894db
        14094bc9  da8ba568  a2cbdd28  132a4ca8
W[28] = 6c04f3ce  1785484d  3b3c2496  6190fe42
        f4ad6b25  211a3eb8  ea3995ba  53a00c32
W[29] = 9cb2e341  fe426190  c761b892  3dd921f9
        9af4e4ff  00df5ef3  b7b3c840  bb2fc4c4
W[30] = b437cbbc  0df051e2  476e1864  3eb8211a
        ba50c5a3  029d5d35  9af4e4ff  f66b6967
W[31] = e4209bd3  6c04f3ce  43f21be0  21f93dd9
        203b3f97  a3aadc49  ab81d472  a8e4d70f
```

Feistel Steps

```
IV :
A[0]=d543e261  B[0]=0cb0c732  C[0]=a4646841  D[0]=2355bbea
A[1]=4bc7effd  B[1]=33faf946  C[1]=93200967  D[1]=1cf5939c
A[2]=58385815  B[2]=8222a8c3  C[2]=711cb3a6  D[2]=f007b836
A[3]=b4815ab1  B[3]=21626282  C[3]=c73b3d5e  D[3]=2f42b26d
A[4]=c9e23dfc  B[4]=155dc7f6  C[4]=3d9e3719  D[4]=d05282d9
A[5]=ff0de712  B[5]=989ef348  C[5]=9d01eb34  D[5]=ef96a7d4
A[6]=a5fc4fa0  B[6]=2ba4131f  C[6]=d346eb58  D[6]=725f5462
A[7]=14531876  B[7]=5b265f81  C[7]=f14c3b5f  D[7]=a1e25af7

IV XOR M :
A[0]=d543e656  B[0]=0cb0c732  C[0]=a4646841  D[0]=2355bbea
```

```
A[1]=4bc7effd  B[1]=33faf946  C[1]=93200967  D[1]=1cf5939c
A[2]=58385815  B[2]=8222a8c3  C[2]=711cb3a6  D[2]=f007b836
A[3]=b4815ab1  B[3]=21626282  C[3]=c73b3d5e  D[3]=2f42b26d
A[4]=c9e23dfc  B[4]=155dc7f6  C[4]=3d9e3719  D[4]=d05282d9
A[5]=ff0de712  B[5]=989ef348  C[5]=9d01eb34  D[5]=ef96a7d4
A[6]=a5fc4fa0  B[6]=2ba4131f  C[6]=d346eb58  D[6]=725f5462
A[7]=14531876  B[7]=5b265f81  C[7]=f14c3b5f  D[7]=a1e25af7

Step  0: (r= 3, s=20)
A[0]=5e0141d7  B[0]=aa1f32b6  C[0]=0cb0c732  D[0]=a4646841
A[1]=663e7f21  B[1]=5e3f7fea  C[1]=33faf946  D[1]=93200967
A[2]=0c9d2c15  B[2]=c1c2c0aa  C[2]=8222a8c3  D[2]=711cb3a6
A[3]=a0ed9fea  B[3]=a40ad58d  C[3]=21626282  D[3]=c73b3d5e
A[4]=386c8cd2  B[4]=4f11efe6  C[4]=155dc7f6  D[4]=3d9e3719
A[5]=28cf3f51  B[5]=f86f3897  C[5]=989ef348  D[5]=9d01eb34
A[6]=31f5bdaa  B[6]=2fe27d05  C[6]=2ba4131f  D[6]=d346eb58
A[7]=d8c12323  B[7]=a298c3b0  C[7]=5b265f81  D[7]=f14c3b5f

Step  1: (r=20, s=14)
A[0]=fa8720ff  B[0]=1d75e014  C[0]=aa1f32b6  D[0]=0cb0c732
A[1]=f3227a73  B[1]=f21663e7  C[1]=5e3f7fea  D[1]=33faf946
A[2]=a29d11d0  B[2]=c150c9d2  C[2]=c1c2c0aa  D[2]=8222a8c3
A[3]=8978ba5b  B[3]=feaa0ed9  C[3]=a40ad58d  D[3]=21626282
A[4]=9216b772  B[4]=cd2386c8  C[4]=4f11efe6  D[4]=155dc7f6
A[5]=3b535bff  B[5]=f5128cf3  C[5]=f86f3897  D[5]=989ef348
A[6]=2124057c  B[6]=daa31f5b  C[6]=2fe27d05  D[6]=2ba4131f
A[7]=2b5bf4aa  B[7]=323d8c12  C[7]=a298c3b0  D[7]=5b265f81

Step  2: (r=14, s=27)
A[0]=dc3d1c00  B[0]=c83ffea1  C[0]=1d75e014  D[0]=aa1f32b6
A[1]=6b806b3b  B[1]=9e9cfcc8  C[1]=f21663e7  D[1]=5e3f7fea
A[2]=e36ef46c  B[2]=447428a7  C[2]=c150c9d2  D[2]=c1c2c0aa
A[3]=5b61caf3  B[3]=2e96e25e  C[3]=feaa0ed9  D[3]=a40ad58d
A[4]=dcdf98f3  B[4]=addca485  C[4]=cd2386c8  D[4]=4f11efe6
A[5]=e29760a1  B[5]=d6ffced4  C[5]=f5128cf3  D[5]=f86f3897
A[6]=aef3a6fe  B[6]=015f0849  C[6]=daa31f5b  D[6]=2fe27d05
A[7]=49b72539  B[7]=fd2a8ad6  C[7]=323d8c12  D[7]=a298c3b0

Step  3: (r=27, s= 3)
A[0]=a2f88470  B[0]=06e1e8e0  C[0]=c83ffea1  D[0]=1d75e014
A[1]=84d97374  B[1]=db5c0359  C[1]=9e9cfcc8  D[1]=f21663e7
A[2]=c02f4cb7  B[2]=671b77a3  C[2]=447428a7  D[2]=c150c9d2
A[3]=f9730c05  B[3]=9adb0e57  C[3]=2e96e25e  D[3]=feaa0ed9
A[4]=955f0890  B[4]=9ee6fcc7  C[4]=addca485  D[4]=cd2386c8
A[5]=6e92c26e  B[5]=0f14bb05  C[5]=d6ffced4  D[5]=f5128cf3
A[6]=47bfd925  B[6]=f5779d37  C[6]=015f0849  D[6]=daa31f5b
A[7]=79438106  B[7]=ca4db929  C[7]=fd2a8ad6  D[7]=323d8c12

Step  4: (r= 3, s=20)
```

```
A[0]=e74a0fc2  B[0]=17c42385  C[0]=06e1e8e0  D[0]=c83ffea1
A[1]=7cc1151d  B[1]=26cb9ba4  C[1]=db5c0359  D[1]=9e9cfcc8
A[2]=da1d4907  B[2]=017a65be  C[2]=671b77a3  D[2]=447428a7
A[3]=62b06f65  B[3]=cb98602f  C[3]=9adb0e57  D[3]=2e96e25e
A[4]=3430b186  B[4]=aaf84484  C[4]=9ee6fcc7  D[4]=addca485
A[5]=2f17cc9d  B[5]=74961373  C[5]=0f14bb05  D[5]=d6ffced4
A[6]=32ac3bec  B[6]=3dfec92a  C[6]=f5779d37  D[6]=015f0849
A[7]=ad557b3e  B[7]=ca1c0833  C[7]=ca4db929  D[7]=fd2a8ad6

Step  5: (r=20, s=14)
A[0]=8ca20fdd  B[0]=fc2e74a0  C[0]=17c42385  D[0]=06e1e8e0
A[1]=b315869b  B[1]=51d7cc11  C[1]=26cb9ba4  D[1]=db5c0359
A[2]=6fd647b3  B[2]=907da1d4  C[2]=017a65be  D[2]=671b77a3
A[3]=f64b9168  B[3]=f6562b06  C[3]=cb98602f  D[3]=9adb0e57
A[4]=7208005c  B[4]=1863430b  C[4]=aaf84484  D[4]=9ee6fcc7
A[5]=9998aa8d  B[5]=c9d2f17c  C[5]=74961373  D[5]=0f14bb05
A[6]=b8150552  B[6]=bec32ac3  C[6]=3dfec92a  D[6]=f5779d37
A[7]=cce85715  B[7]=b3ead557  C[7]=ca1c0833  D[7]=ca4db929

Step  6: (r=14, s=27)
A[0]=7290ca11  B[0]=83f76328  C[0]=fc2e74a0  D[0]=17c42385
A[1]=fbae23c6  B[1]=61a6ecc5  C[1]=51d7cc11  D[1]=26cb9ba4
A[2]=3edb0acf  B[2]=91ecdbf5  C[2]=907da1d4  D[2]=017a65be
A[3]=34953b4e  B[3]=e45a3d92  C[3]=f6562b06  D[3]=cb98602f
A[4]=ddebd1e8  B[4]=00171c82  C[4]=1863430b  D[4]=aaf84484
A[5]=8ad25ecc  B[5]=2aa36666  C[5]=c9d2f17c  D[5]=74961373
A[6]=5c781905  B[6]=4154ae05  C[6]=bec32ac3  D[6]=3dfec92a
A[7]=90f203ce  B[7]=15c5733a  C[7]=b3ead557  D[7]=ca1c0833

Step  7: (r=27, s= 3)
A[0]=80695af1  B[0]=8b948650  C[0]=83f76328  D[0]=fc2e74a0
A[1]=1dfffdd1  B[1]=37dd711e  C[1]=61a6ecc5  D[1]=51d7cc11
A[2]=b8de0324  B[2]=79f6d856  C[2]=91ecdbf5  D[2]=907da1d4
A[3]=6e35ed23  B[3]=71a4a9da  C[3]=e45a3d92  D[3]=f6562b06
A[4]=4d32cb73  B[4]=46ef5e8f  C[4]=00171c82  D[4]=1863430b
A[5]=6c0b03db  B[5]=645692f6  C[5]=2aa36666  D[5]=c9d2f17c
A[6]=84a4cbcc  B[6]=2ae3c0c8  C[6]=4154ae05  D[6]=bec32ac3
A[7]=f038961f  B[7]=7487901e  C[7]=15c5733a  D[7]=b3ead557

Step  8: (r=26, s= 4)
A[0]=cb84862f  B[0]=c601a56b  C[0]=8b948650  D[0]=83f76328
A[1]=56e3e318  B[1]=4477fff7  C[1]=37dd711e  D[1]=61a6ecc5
A[2]=9d10d341  B[2]=92e3780c  C[2]=79f6d856  D[2]=91ecdbf5
A[3]=e9c12b48  B[3]=8db8d7b4  C[3]=71a4a9da  D[3]=e45a3d92
A[4]=404eb215  B[4]=cd34cb2d  C[4]=46ef5e8f  D[4]=00171c82
A[5]=e35b398e  B[5]=6db02c0f  C[5]=645692f6  D[5]=2aa36666
A[6]=b5dd56e3  B[6]=3212932f  C[6]=2ae3c0c8  D[6]=4154ae05
A[7]=cb80d692  B[7]=7fc0e258  C[7]=7487901e  D[7]=15c5733a
```

```
Step  9: (r= 4, s=23)
A[0]=425d0672  B[0]=b84862fc  C[0]=c601a56b  D[0]=8b948650
A[1]=22800992  B[1]=6e3e3185  C[1]=4477fff7  D[1]=37dd711e
A[2]=bc225f09  B[2]=d10d3419  C[2]=92e3780c  D[2]=79f6d856
A[3]=e2a5a95b  B[3]=9c12b48e  C[3]=8db8d7b4  D[3]=71a4a9da
A[4]=9f741a31  B[4]=04eb2154  C[4]=cd34cb2d  D[4]=46ef5e8f
A[5]=ce630089  B[5]=35b398ee  C[5]=6db02c0f  D[5]=645692f6
A[6]=2c9fdcce  B[6]=5dd56e3b  C[6]=3212932f  D[6]=2ae3c0c8
A[7]=5fa0efad  B[7]=b80d692c  C[7]=7fc0e258  D[7]=7487901e

Step 10: (r=23, s=11)
A[0]=cfca16fe  B[0]=39212e83  C[0]=b84862fc  D[0]=c601a56b
A[1]=92e3653d  B[1]=c9114004  C[1]=6e3e3185  D[1]=4477fff7
A[2]=16b0bbbf  B[2]=84de112f  C[2]=d10d3419  D[2]=92e3780c
A[3]=48b233a3  B[3]=adf152d4  C[3]=9c12b48e  D[3]=8db8d7b4
A[4]=b0211560  B[4]=18cfba0d  C[4]=04eb2154  D[4]=cd34cb2d
A[5]=2c010d90  B[5]=44e73180  C[5]=35b398ee  D[5]=6db02c0f
A[6]=f8b52fb1  B[6]=67164fee  C[6]=5dd56e3b  D[6]=3212932f
A[7]=e8c58ba9  B[7]=d6afd077  C[7]=b80d692c  D[7]=7fc0e258

Step 11: (r=11, s=26)
A[0]=6408123e  B[0]=50b7f67e  C[0]=39212e83  D[0]=b84862fc
A[1]=7e248beb  B[1]=1b29ec97  C[1]=c9114004  D[1]=6e3e3185
A[2]=7ef3ce16  B[2]=85ddf8b5  C[2]=84de112f  D[2]=d10d3419
A[3]=4fd1a9cf  B[3]=919d1a45  C[3]=adf152d4  D[3]=9c12b48e
A[4]=62fc36b9  B[4]=08ab0581  C[4]=18cfba0d  D[4]=04eb2154
A[5]=c58b5259  B[5]=086c8160  C[5]=44e73180  D[5]=35b398ee
A[6]=d75173be  B[6]=a97d8fc5  C[6]=67164fee  D[6]=5dd56e3b
A[7]=a757bff4  B[7]=2c5d4f46  C[7]=d6afd077  D[7]=b80d692c

Step 12: (r=26, s= 4)
A[0]=613fe3b2  B[0]=f9902048  C[0]=50b7f67e  D[0]=39212e83
A[1]=ffcece40  B[1]=adf8922f  C[1]=1b29ec97  D[1]=c9114004
A[2]=9f8f9811  B[2]=59fbcf38  C[2]=85ddf8b5  D[2]=84de112f
A[3]=fbaab59f  B[3]=3d3f46a7  C[3]=919d1a45  D[3]=adf152d4
A[4]=538d79a7  B[4]=e58bf0da  C[4]=08ab0581  D[4]=18cfba0d
A[5]=7a390420  B[5]=67162d49  C[5]=086c8160  D[5]=44e73180
A[6]=acd5e9f5  B[6]=fb5d45ce  C[6]=a97d8fc5  D[6]=67164fee
A[7]=9cd4a863  B[7]=d29d5eff  C[7]=2c5d4f46  D[7]=d6afd077

Step 13: (r= 4, s=23)
A[0]=4225bd09  B[0]=13fe3b26  C[0]=f9902048  D[0]=50b7f67e
A[1]=16ef1e5f  B[1]=fcece40f  C[1]=adf8922f  D[1]=1b29ec97
A[2]=5af81da2  B[2]=f8f98119  C[2]=59fbcf38  D[2]=85ddf8b5
A[3]=e4ba63ca  B[3]=baab59ff  C[3]=3d3f46a7  D[3]=919d1a45
A[4]=5061e2fd  B[4]=38d79a75  C[4]=e58bf0da  D[4]=08ab0581
A[5]=95a27465  B[5]=a3904207  C[5]=67162d49  D[5]=086c8160
A[6]=4d41d760  B[6]=cd5e9f5a  C[6]=fb5d45ce  D[6]=a97d8fc5
A[7]=afad7d1a  B[7]=cd4a8639  C[7]=d29d5eff  D[7]=2c5d4f46
```

```
Step 14: (r=23, s=11)
A[0]=f13ea328  B[0]=84a112de  C[0]=13fe3b26  D[0]=f9902048
A[1]=4b774278  B[1]=2f8b778f  C[1]=fcece40f  D[1]=adf8922f
A[2]=e119a9f3  B[2]=d12d7c0e  C[2]=f8f98119  D[2]=59fbcf38
A[3]=bba22445  B[3]=e5725d31  C[3]=baab59ff  D[3]=3d3f46a7
A[4]=464609d2  B[4]=7ea830f1  C[4]=38d79a75  D[4]=e58bf0da
A[5]=fe750729  B[5]=32cad13a  C[5]=a3904207  D[5]=67162d49
A[6]=4590d115  B[6]=b026a0eb  C[6]=cd5e9f5a  D[6]=fb5d45ce
A[7]=c0a6b07b  B[7]=8d57d6be  C[7]=cd4a8639  D[7]=d29d5eff

Step 15: (r=11, s=26)
A[0]=7a1c68e6  B[0]=f5194789  C[0]=84a112de  D[0]=13fe3b26
A[1]=67fad706  B[1]=ba13c25b  C[1]=2f8b778f  D[1]=fcece40f
A[2]=16bfcee3  B[2]=cd4f9f08  C[2]=d12d7c0e  D[2]=f8f98119
A[3]=13f84928  B[3]=11222ddd  C[3]=e5725d31  D[3]=baab59ff
A[4]=fb91d2ac  B[4]=304e9232  C[4]=7ea830f1  D[4]=38d79a75
A[5]=5d292856  B[5]=a8394ff3  C[5]=32cad13a  D[5]=a3904207
A[6]=19a0bf0c  B[6]=8688aa2c  C[6]=b026a0eb  D[6]=cd5e9f5a
A[7]=5c380df7  B[7]=3583de05  C[7]=8d57d6be  D[7]=cd4a8639

Step 16: (r=19, s=28)
A[0]=b605e369  B[0]=4733d0e3  C[0]=f5194789  D[0]=84a112de
A[1]=c87f3670  B[1]=b8333fd6  C[1]=ba13c25b  D[1]=2f8b778f
A[2]=2495da3c  B[2]=7718b5fe  C[2]=cd4f9f08  D[2]=d12d7c0e
A[3]=d46ce115  B[3]=49409fc2  C[3]=11222ddd  D[3]=e5725d31
A[4]=4bb071e7  B[4]=9567dc8e  C[4]=304e9232  D[4]=7ea830f1
A[5]=35404152  B[5]=42b2e949  C[5]=a8394ff3  D[5]=32cad13a
A[6]=9291e26b  B[6]=f860cd05  C[6]=8688aa2c  D[6]=b026a0eb
A[7]=71f805d8  B[7]=6fbae1c0  C[7]=3583de05  D[7]=8d57d6be

Step 17: (r=28, s= 7)
A[0]=3a368bb7  B[0]=9b605e36  C[0]=4733d0e3  D[0]=f5194789
A[1]=6e4c8bf7  B[1]=0c87f367  C[1]=b8333fd6  D[1]=ba13c25b
A[2]=d06ffb3e  B[2]=c2495da3  C[2]=7718b5fe  D[2]=cd4f9f08
A[3]=9a062621  B[3]=5d46ce11  C[3]=49409fc2  D[3]=11222ddd
A[4]=3d465292  B[4]=74bb071e  C[4]=9567dc8e  D[4]=304e9232
A[5]=73949d95  B[5]=23540415  C[5]=42b2e949  D[5]=a8394ff3
A[6]=8ee96676  B[6]=b9291e26  C[6]=f860cd05  D[6]=8688aa2c
A[7]=ac884073  B[7]=871f805d  C[7]=6fbae1c0  D[7]=3583de05

Step 18: (r= 7, s=22)
A[0]=2143dfc7  B[0]=1b45db9d  C[0]=9b605e36  D[0]=4733d0e3
A[1]=81412f0d  B[1]=2645fbb7  C[1]=0c87f367  D[1]=b8333fd6
A[2]=733d7b4e  B[2]=37fd9f68  C[2]=c2495da3  D[2]=7718b5fe
A[3]=d4810eac  B[3]=031310cd  C[3]=5d46ce11  D[3]=49409fc2
A[4]=b42184d7  B[4]=a329491e  C[4]=74bb071e  D[4]=9567dc8e
A[5]=e5b4d668  B[5]=ca4ecab9  C[5]=23540415  D[5]=42b2e949
A[6]=3ecfe17b  B[6]=74b33b47  C[6]=b9291e26  D[6]=f860cd05
```

```
A[7]=178df90b  B[7]=442039d6  C[7]=871f805d  D[7]=6fbae1c0

Step 19: (r=22, s=19)
A[0]=d7fbde59  B[0]=f1c850f7  C[0]=1b45db9d  D[0]=9b605e36
A[1]=d2703559  B[1]=c360504b  C[1]=2645fbb7  D[1]=0c87f367
A[2]=5c8ab8b7  B[2]=d39ccf5e  C[2]=37fd9f68  D[2]=c2495da3
A[3]=cf4becd0  B[3]=ab352043  C[3]=031310cd  D[3]=5d46ce11
A[4]=7c657367  B[4]=35ed0861  C[4]=a329491e  D[4]=74bb071e
A[5]=bab9db71  B[5]=9a396d35  C[5]=ca4ecab9  D[5]=23540415
A[6]=3e6936b3  B[6]=5ecfb3f8  C[6]=74b33b47  D[6]=b9291e26
A[7]=b3448de7  B[7]=42c5e37e  C[7]=442039d6  D[7]=871f805d

Step 20: (r=19, s=28)
A[0]=c881864f  B[0]=f2cebfde  C[0]=f1c850f7  D[0]=1b45db9d
A[1]=dbdfc206  B[1]=aace9381  C[1]=c360504b  D[1]=2645fbb7
A[2]=428957cb  B[2]=c5bae455  C[2]=d39ccf5e  D[2]=37fd9f68
A[3]=37075678  B[3]=66867a5f  C[3]=ab352043  D[3]=031310cd
A[4]=c14a07bb  B[4]=9b3be32b  C[4]=35ed0861  D[4]=a329491e
A[5]=682b8505  B[5]=db8dd5ce  C[5]=9a396d35  D[5]=ca4ecab9
A[6]=c5e7421a  B[6]=b599f349  C[6]=5ecfb3f8  D[6]=74b33b47
A[7]=937eba9c  B[7]=6f3d9a24  C[7]=42c5e37e  D[7]=442039d6

Step 21: (r=28, s= 7)
A[0]=8d3efbe4  B[0]=fc881864  C[0]=f2cebfde  D[0]=f1c850f7
A[1]=f3c5e6b1  B[1]=6dbdfc20  C[1]=aace9381  D[1]=c360504b
A[2]=ed623f6a  B[2]=b428957c  C[2]=c5bae455  D[2]=d39ccf5e
A[3]=3126c33d  B[3]=83707567  C[3]=66867a5f  D[3]=ab352043
A[4]=83a3f4cb  B[4]=bc14a07b  C[4]=9b3be32b  D[4]=35ed0861
A[5]=ed9acc10  B[5]=5682b850  C[5]=db8dd5ce  D[5]=9a396d35
A[6]=df970875  B[6]=ac5e7421  C[6]=b599f349  D[6]=5ecfb3f8
A[7]=80a84f98  B[7]=c937eba9  C[7]=6f3d9a24  D[7]=42c5e37e

Step 22: (r= 7, s=22)
A[0]=d3ae0dd0  B[0]=9f7df246  C[0]=fc881864  D[0]=f2cebfde
A[1]=a788da3f  B[1]=e2f358f9  C[1]=6dbdfc20  D[1]=aace9381
A[2]=cb1667ec  B[2]=b11fb576  C[2]=b428957c  D[2]=c5bae455
A[3]=08fdaaae  B[3]=93619e98  C[3]=83707567  D[3]=66867a5f
A[4]=d9dbc824  B[4]=d1fa65c1  C[4]=bc14a07b  D[4]=9b3be32b
A[5]=5c66d97f  B[5]=cd660876  C[5]=5682b850  D[5]=db8dd5ce
A[6]=c2f0a82b  B[6]=cb843aef  C[6]=ac5e7421  D[6]=b599f349
A[7]=87e6d16b  B[7]=5427cc40  C[7]=c937eba9  D[7]=6f3d9a24

Step 23: (r=22, s=19)
A[0]=c69b0e16  B[0]=7434eb83  C[0]=9f7df246  D[0]=fc881864
A[1]=2f053b32  B[1]=8fe9e236  C[1]=e2f358f9  D[1]=6dbdfc20
A[2]=d3f3781b  B[2]=fb32c599  C[2]=b11fb576  D[2]=b428957c
A[3]=e608865a  B[3]=ab823f6a  C[3]=93619e98  D[3]=83707567
A[4]=8138a22c  B[4]=093676f2  C[4]=d1fa65c1  D[4]=bc14a07b
A[5]=45e85da0  B[5]=5fd719b6  C[5]=cd660876  D[5]=5682b850
```

```
A[6]=3223ed59  B[6]=0af0bc2a  C[6]=cb843aef  D[6]=ac5e7421
A[7]=06a6a26d  B[7]=5ae1f9b4  C[7]=5427cc40  D[7]=c937eba9

Step 24: (r=15, s= 5)
A[0]=456f0289  B[0]=870b634d  C[0]=7434eb83  D[0]=9f7df246
A[1]=612e212d  B[1]=9d991782  C[1]=8fe9e236  D[1]=e2f358f9
A[2]=eed211ef  B[2]=bc0de9f9  C[2]=fb32c599  D[2]=b11fb576
A[3]=c23e42b2  B[3]=432d7304  C[3]=ab823f6a  D[3]=93619e98
A[4]=a5b472be  B[4]=5116409c  C[4]=093676f2  D[4]=d1fa65c1
A[5]=1ced4533  B[5]=2ed022f4  C[5]=5fd719b6  D[5]=cd660876
A[6]=f33c360e  B[6]=f6ac9911  C[6]=0af0bc2a  D[6]=cb843aef
A[7]=1b6de37a  B[7]=51368353  C[7]=5ae1f9b4  D[7]=5427cc40

Step 25: (r= 5, s=29)
A[0]=8ed86fa2  B[0]=ade05128  C[0]=870b634d  D[0]=7434eb83
A[1]=9f615c92  B[1]=25c425ac  C[1]=9d991782  D[1]=8fe9e236
A[2]=bc6b8bcd  B[2]=da423dfd  C[2]=bc0de9f9  D[2]=fb32c599
A[3]=39ff650d  B[3]=47c85658  C[3]=432d7304  D[3]=ab823f6a
A[4]=76b6f362  B[4]=b68e57d4  C[4]=5116409c  D[4]=093676f2
A[5]=948bdc3a  B[5]=9da8a663  C[5]=2ed022f4  D[5]=5fd719b6
A[6]=e68aab06  B[6]=6786c1de  C[6]=f6ac9911  D[6]=0af0bc2a
A[7]=f6f4facd  B[7]=6dbc6f43  C[7]=51368353  D[7]=5ae1f9b4

Step 26: (r=29, s= 9)
A[0]=fbcad78a  B[0]=51db0df4  C[0]=ade05128  D[0]=870b634d
A[1]=6c549ddb  B[1]=53ec2b92  C[1]=25c425ac  D[1]=9d991782
A[2]=a8eeeb6f  B[2]=b78d7179  C[2]=da423dfd  D[2]=bc0de9f9
A[3]=4800050b  B[3]=a73feca1  C[3]=47c85658  D[3]=432d7304
A[4]=382058d7  B[4]=4ed6de6c  C[4]=b68e57d4  D[4]=5116409c
A[5]=48385f8c  B[5]=52917b87  C[5]=9da8a663  D[5]=2ed022f4
A[6]=12e4c2f6  B[6]=dcd15560  C[6]=6786c1de  D[6]=f6ac9911
A[7]=0f6f356a  B[7]=bede9f59  C[7]=6dbc6f43  D[7]=51368353

Step 27: (r= 9, s=15)
A[0]=1fd7a224  B[0]=95af15f7  C[0]=51db0df4  D[0]=ade05128
A[1]=36d092b2  B[1]=a93bb6d8  C[1]=53ec2b92  D[1]=25c425ac
A[2]=a57cc75d  B[2]=ddd6df51  C[2]=b78d7179  D[2]=da423dfd
A[3]=0d82ef25  B[3]=000a1690  C[3]=a73feca1  D[3]=47c85658
A[4]=8b840fcd  B[4]=40b1ae70  C[4]=4ed6de6c  D[4]=b68e57d4
A[5]=0b5da64e  B[5]=70bf1890  C[5]=52917b87  D[5]=9da8a663
A[6]=39a766ee  B[6]=c985ec25  C[6]=dcd15560  D[6]=6786c1de
A[7]=97ac802f  B[7]=de6ad41e  C[7]=bede9f59  D[7]=6dbc6f43

Step 28: (r=15, s= 5)
A[0]=41e278ad  B[0]=d1120feb  C[0]=95af15f7  D[0]=51db0df4
A[1]=f9562159  B[1]=49591b68  C[1]=a93bb6d8  D[1]=53ec2b92
A[2]=e2f9c45a  B[2]=63aed2be  C[2]=ddd6df51  D[2]=b78d7179
A[3]=30373a33  B[3]=779286c1  C[3]=000a1690  D[3]=a73feca1
A[4]=8d31326c  B[4]=07e6c5c2  C[4]=40b1ae70  D[4]=4ed6de6c
```

```
A[5]=33eab9e4  B[5]=d32705ae  C[5]=70bf1890  D[5]=52917b87
A[6]=a8cf4b5b  B[6]=b3771cd3  C[6]=c985ec25  D[6]=dcd15560
A[7]=bcd90f5f  B[7]=4017cbd6  C[7]=de6ad41e  D[7]=bede9f59

Step 29: (r= 5, s=29)
A[0]=f73e8d40  B[0]=3c4f15a8  C[0]=d1120feb  D[0]=95af15f7
A[1]=4e587e75  B[1]=2ac42b3f  C[1]=49591b68  D[1]=a93bb6d8
A[2]=e8acd5b4  B[2]=5f388b5c  C[2]=63aed2be  D[2]=ddd6df51
A[3]=8d698fe4  B[3]=06e74666  C[3]=779286c1  D[3]=000a1690
A[4]=97d918ae  B[4]=a6264d91  C[4]=07e6c5c2  D[4]=40b1ae70
A[5]=7405ea7a  B[5]=7d573c86  C[5]=d32705ae  D[5]=70bf1890
A[6]=0defdacf  B[6]=19e96b75  C[6]=b3771cd3  D[6]=c985ec25
A[7]=e82482f5  B[7]=9b21ebf7  C[7]=4017cbd6  D[7]=de6ad41e

Step 30: (r=29, s= 9)
A[0]=c6e3c6dc  B[0]=1ee7d1a8  C[0]=3c4f15a8  D[0]=d1120feb
A[1]=ea46695c  B[1]=a9cb0fce  C[1]=2ac42b3f  D[1]=49591b68
A[2]=3217a070  B[2]=9d159ab6  C[2]=5f388b5c  D[2]=63aed2be
A[3]=1e783fa2  B[3]=91ad31fc  C[3]=06e74666  D[3]=779286c1
A[4]=63305d01  B[4]=d2fb2315  C[4]=a6264d91  D[4]=07e6c5c2
A[5]=645a8286  B[5]=4e80bd4f  C[5]=7d573c86  D[5]=d32705ae
A[6]=7e2306ca  B[6]=e1bdfb59  C[6]=19e96b75  D[6]=b3771cd3
A[7]=16facae1  B[7]=bd04905e  C[7]=9b21ebf7  D[7]=4017cbd6

Step 31: (r= 9, s=15)
A[0]=a16d6cd3  B[0]=c78db98d  C[0]=1ee7d1a8  D[0]=3c4f15a8
A[1]=d24f3cda  B[1]=8cd2b9d4  C[1]=a9cb0fce  D[1]=2ac42b3f
A[2]=8296f857  B[2]=2f40e064  C[2]=9d159ab6  D[2]=5f388b5c
A[3]=73d61a69  B[3]=f07f443c  C[3]=91ad31fc  D[3]=06e74666
A[4]=f0c2beb7  B[4]=60ba02c6  C[4]=d2fb2315  D[4]=a6264d91
A[5]=dc11ab66  B[5]=b5050cc8  C[5]=4e80bd4f  D[5]=7d573c86
A[6]=5d904cb5  B[6]=460d94fc  C[6]=e1bdfb59  D[6]=19e96b75
A[7]=a76d884a  B[7]=f595c22d  C[7]=bd04905e  D[7]=9b21ebf7

Feed-Forward Step 0: (r=15, s= 5)
A[0]=c2c39f7d  B[0]=b669d0b6  C[0]=c78db98d  D[0]=1ee7d1a8
A[1]=c034b2ba  B[1]=9e6d6927  C[1]=8cd2b9d4  D[1]=a9cb0fce
A[2]=db8d84a5  B[2]=7c2bc14b  C[2]=2f40e064  D[2]=9d159ab6
A[3]=f9241bc0  B[3]=0d34b9eb  C[3]=f07f443c  D[3]=91ad31fc
A[4]=2e255082  B[4]=5f5bf861  C[4]=60ba02c6  D[4]=d2fb2315
A[5]=bc23f483  B[5]=d5b36e08  C[5]=b5050cc8  D[5]=4e80bd4f
A[6]=4693b5ea  B[6]=265aaec8  C[6]=460d94fc  D[6]=e1bdfb59
A[7]=b5ad3ff5  B[7]=c42553b6  C[7]=f595c22d  D[7]=bd04905e

Feed-Forward Step 1: (r= 5, s=29)
A[0]=480d5dec  B[0]=5873efb8  C[0]=b669d0b6  D[0]=c78db98d
A[1]=71d8fe6e  B[1]=06965758  C[1]=9e6d6927  D[1]=8cd2b9d4
A[2]=abe4342f  B[2]=71b094bb  C[2]=7c2bc14b  D[2]=2f40e064
A[3]=5e2835a7  B[3]=2483781f  C[3]=0d34b9eb  D[3]=f07f443c
```

```
A[4]=b95544f1  B[4]=c4aa1045  C[4]=5f5bf861  D[4]=60ba02c6
A[5]=a530e251  B[5]=847e9077  C[5]=d5b36e08  D[5]=b5050cc8
A[6]=471a26af  B[6]=d276bd48  C[6]=265aaec8  D[6]=460d94fc
A[7]=000aa8ea  B[7]=b5a7feb6  C[7]=c42553b6  D[7]=f595c22d

Feed-Forward Step 2: (r=29, s= 9)
A[0]=e7e065f1  B[0]=8901abbd  C[0]=5873efb8  D[0]=b669d0b6
A[1]=39184e32  B[1]=ce3b1fcd  C[1]=06965758  D[1]=9e6d6927
A[2]=47790676  B[2]=f57c8685  C[2]=71b094bb  D[2]=7c2bc14b
A[3]=d59e7c17  B[3]=ebc506b4  C[3]=2483781f  D[3]=0d34b9eb
A[4]=b1a9477c  B[4]=372aa89e  C[4]=c4aa1045  D[4]=5f5bf861
A[5]=6a8530d2  B[5]=34a61c4a  C[5]=847e9077  D[5]=d5b36e08
A[6]=1c9458c4  B[6]=e8e344d5  C[6]=d276bd48  D[6]=265aaec8
A[7]=9cf43113  B[7]=4001551d  C[7]=b5a7feb6  D[7]=c42553b6

Feed-Forward Step 3: (r= 9, s=15)
A[0]=eebbb2cc  B[0]=c0cbe3cf  C[0]=8901abbd  D[0]=5873efb8
A[1]=986789d5  B[1]=309c6472  C[1]=ce3b1fcd  D[1]=06965758
A[2]=30b8f94f  B[2]=f20cec8e  C[2]=f57c8685  D[2]=71b094bb
A[3]=209c3637  B[3]=3cf82fab  C[3]=ebc506b4  D[3]=2483781f
A[4]=0677b63b  B[4]=528ef963  C[4]=372aa89e  D[4]=c4aa1045
A[5]=83be1996  B[5]=0a61a4d5  C[5]=34a61c4a  D[5]=847e9077
A[6]=66881e5c  B[6]=28b18839  C[6]=e8e344d5  D[6]=d276bd48
A[7]=04297330  B[7]=e8622739  C[7]=4001551d  D[7]=b5a7feb6
```

Compression Function Output

```
A[0]=eebbb2cc  B[0]=c0cbe3cf  C[0]=8901abbd  D[0]=5873efb8
A[1]=986789d5  B[1]=309c6472  C[1]=ce3b1fcd  D[1]=06965758
A[2]=30b8f94f  B[2]=f20cec8e  C[2]=f57c8685  D[2]=71b094bb
A[3]=209c3637  B[3]=3cf82fab  C[3]=ebc506b4  D[3]=2483781f
A[4]=0677b63b  B[4]=528ef963  C[4]=372aa89e  D[4]=c4aa1045
A[5]=83be1996  B[5]=0a61a4d5  C[5]=34a61c4a  D[5]=847e9077
A[6]=66881e5c  B[6]=28b18839  C[6]=e8e344d5  D[6]=d276bd48
A[7]=04297330  B[7]=e8622739  C[7]=4001551d  D[7]=b5a7feb6
```

Hash Function Output

```
cc b2 bb ee d5 89 67 98 4f f9 b8 30 37 36 9c 20
3b b6 77 06 96 19 be 83 5c 1e 88 66 30 73 29 04
cf e3 cb c0 72 64 9c 30 8e ec 0c f2 ab 2f f8 3c
```

6.4 SIMD-512

6.4.1 Empty message

The first test vector is the empty message. It has no message blocks, and only a final block with the counter, which is zero.

Final block

```
M[  0..  7] = 00 00 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    2  203  156   47  118  214  107  106
y[  8.. 15] =   45   93  212   20  111   73  162  251
y[ 16.. 23] =   97  215  249   53  211   19    3   89
y[ 24.. 31] =   49  207  101   67  151  130  223   23
y[ 32.. 39] =  189  202  178  239  253  127  204   49
y[ 40.. 47] =   76  236   82  137  232  157   65   79
y[ 48.. 55] =   96  161  176  130  161   30   47    9
y[ 56.. 63] =  189  247   61  226  248   90  107   64
y[ 64.. 71] =    0   88  131  243  133   59  113  115
y[ 72.. 79] =   17  236   33  213   12  191  111   19
y[ 80.. 87] =  251   61  103  208   57   35  148  248
y[ 88.. 95] =   47  116   65  119  249  178  143   40
y[ 96..103] =  189  129    8  163  204  227  230  196
y[104..111] =  205  122  151   45  187   19  227   72
y[112..119] =  247  125  111  121  140  220    6  107
y[120..127] =   77   69   10  101   21   65  149  171
y[128..135] =  255   54  101  210  139   43  150  151
y[136..143] =  212  164   45  237  146  184   95    6
y[144..151] =  160   42    8  204   46  238  254  168
y[152..159] =  208   50  156  190  106  127   34  234
y[160..167] =   68   55   79   18    4  130   53  208
y[168..175] =  181   21  175  120   25  100  192  178
y[176..183] =  161   96   81  127   96  227  210  248
y[184..191] =   68   10  196   31    9  167  150  193
y[192..199] =    0  169  126   14  124  198  144  142
y[200..207] =  240   21  224   44  245   66  146  238
y[208..215] =    6  196  154   49  200  222  109    9
y[216..223] =  210  141  192  138    8   79  114  217
y[224..231] =   68  128  249   94   53   30   27   61
```

```
y[232..239] =   52  135  106  212   70  238   30  185
y[240..247] =   10  132  146  136  117   37  251  150
y[248..255] =  180  188  247  156  236  192  108   86
```

Intermediate Expanded Message

```
Z[ 0] = d8fa0172  21f7b703  e0ed5546  4c9a4d53
        43352085  0e74df7b  34c15037  fbaabb59
Z[ 1] = e1a64619  264dfa38  0dbbdec2  4051022b
        dbde2369  306b48fd  a439b366  109fe76e
Z[ 2] = d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
        f0d336ec  a9483b42  b7bcedef  39172ef9
Z[ 3] = baa04560  a439c577  15aebaa0  068121f7
        f8c6cedc  e9992c15  410af97f  2e404d53
Z[ 4] = 3f980000  f5e2a4f2  2aa3a664  531b51a9
        f0d30c49  e03417d9  d04e08ac  0dbb5037
Z[ 5] = 2c15fbaa  dc974a6f  194b2931  f97fb13b
        53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
Z[ 6] = a380cedc  bc1205c8  ea52d9b3  d3ebec7d
        582ada6c  2085b366  0dbbcd6a  3408ea52
Z[ 7] = 5a55f8c6  57715037  e543ab73  4d530456
        31dd37a5  48fd073a  2ef90f2d  c1dab1f4
Z[ 8] = 2706fe8e  de0948fd  1f13aaba  b366b2ad
        bccbdf7b  f18c2085  cb3fafc9  045644a7
Z[ 9] = 1e5ab9e7  d9b305c8  f245213e  bfaffdd5
        2422dc97  cf95b703  5bc74c9a  ef611892
Z[10] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
Z[11] = 4560baa0  5bc73a89  ea524560  f97fde09
        073a3124  1667d3eb  bef60681  d1c0b2ad
Z[12] = c0680000  0a1e5b0e  d55d599c  ace5ae57
        0f2df3b7  1fcce827  2fb2f754  f245afc9
Z[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
Z[14] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
Z[15] = a5ab073a  a88fafc9  1abd548d  b2adfbaa
        ce23c85b  b703f8c6  d107f0d3  3e264e0c
Z[16] = fe4201be  57fba805  993666ca  a2cb5d35
        d8cd2733  2733d8cd  9f4f60b1  52c1ad3f
Z[17] = ab81547f  06f8f908  2812d7ee  fd63029d
        d5512aaf  a80557fb  5c56a3aa  1d9ee262
Z[18] = 3b3cc4c4  44d1bb2f  037cfc84  2e2bd1d5
        bdcc4234  b892476e  15c7ea39  c761389f
Z[19] = ac6053a0  468fb971  53a0ac60  d70f28f1
        3b3cc4c4  cadd3523  07d7f829  a2cb5d35
Z[20] = 00000000  6dc2923e  6c0493fc  9d91626f
        f1310ecf  e3411cbf  f58c0a74  9f4f60b1
Z[21] = 053afac6  a64759b9  ce5931a7  5ef3a10d
```

```
         d70f28f1  c761389f  06f8f908  634e9cb2
Z[22] =  3b3cc4c4  f90806f8  2e2bd1d5  1785e87b
         2d4cd2b4  5c56a3aa  3cfac306  1a22e5de
Z[23] =  08b6f74a  9f4f60b1  65eb9a15  fac6053a
         bced4313  f74a08b6  edb5124b  5e14a1ec
Z[24] =  2f0ad0f6  d70f28f1  2575da8b  a3aa5c56
         aefd5103  ee94116c  c0693f97  053afac6
Z[25] =  2496db6a  d1d52e2b  ef73108d  b2794d87
         2b8ed472  c5a33a5d  6ea1915f  ebf71409
Z[26] =  2fe9d017  0faef052  915f6ea1  d5512aaf
         124bedb5  68889778  571ca8e4  bb2f44d1
Z[27] =  53a0ac60  6ea1915f  e5de1a22  f82907d7
         08b6f74a  1b01e4ff  b19a4e66  c84037c0
Z[28] =  b3584ca8  0c32f3ce  cc9b3365  9bd3642d
         124bedb5  2654d9ac  397ec682  ef73108d
Z[29] =  cadd3523  2aafd551  e1831e7d  07d7f829
         9af4650c  985767a9  44d1bb2f  dd2822d8
Z[30] =  6f809080  51e2ae1e  1a22e5de  3523cadd
         95ba6a46  d8cd2733  ef73108d  c1483eb8
Z[31] =  931d6ce3  96996967  203bdfc5  a2cb5d35
         c3e53c1b  a80557fb  c761389f  4aeab516
```

Expanded Message

```
W[ 0] =  3f980000  f5e2a4f2  2aa3a664  531b51a9
         f0d30c49  e03417d9  d04e08ac  0dbb5037
W[ 1] =  a380cedc  bc1205c8  ea52d9b3  d3ebec7d
         582ada6c  2085b366  0dbbcd6a  3408ea52
W[ 2] =  d8fa0172  21f7b703  e0ed5546  4c9a4d53
         43352085  0e74df7b  34c15037  fbaabb59
W[ 3] =  d841cedc  f2fec6e9  5bc7fd1c  2369d9b3
         f0d336ec  a9483b42  b7bcedef  39172ef9
W[ 4] =  5a55f8c6  57715037  e543ab73  4d530456
         31dd37a5  48fd073a  2ef90f2d  c1dab1f4
W[ 5] =  2c15fbaa  dc974a6f  194b2931  f97fb13b
         53d421f7  55ff2ef9  c6e9fa38  1ce8ad9e
W[ 6] =  baa04560  a439c577  15aebaa0  068121f7
         f8c6cedc  e9992c15  410af97f  2e404d53
W[ 7] =  e1a64619  264dfa38  0dbbdec2  4051022b
         dbde2369  306b48fd  a439b366  109fe76e
W[ 8] =  a5ab073a  a88fafc9  1abd548d  b2adfbaa
         ce23c85b  b703f8c6  d107f0d3  3e264e0c
W[ 9] =  4560baa0  5bc73a89  ea524560  f97fde09
         073a3124  1667d3eb  bef60681  d1c0b2ad
W[10] =  c0680000  0a1e5b0e  d55d599c  ace5ae57
         0f2df3b7  1fcce827  2fb2f754  f245afc9
W[11] =  2706fe8e  de0948fd  1f13aaba  b366b2ad
         bccbdf7b  f18c2085  cb3fafc9  045644a7
W[12] =  1e5ab9e7  d9b305c8  f245213e  bfaffdd5
```

```
        2422dc97  cf95b703  5bc74c9a  ef611892
W[13] = d3eb0456  2369b591  e6b5d6cf  06814ec5
        ac2cde09  aa01d107  391705c8  e3185262
W[14] = 27bf3124  0d023917  a43902e4  dc97264d
        0f2dc914  56b8c4be  48441211  c6e9d107
W[15] = 5c803124  43eefa38  15ae264d  2c151383
        a7d62594  df7b4c9a  f2453296  cbf815ae
W[16] = ab81547f  06f8f908  2812d7ee  fd63029d
        d5512aaf  a80557fb  5c56a3aa  1d9ee262
W[17] = 3b3cc4c4  44d1bb2f  037cfc84  2e2bd1d5
        bdcc4234  b892476e  15c7ea39  c761389f
W[18] = 08b6f74a  9f4f60b1  65eb9a15  fac6053a
        bced4313  f74a08b6  edb5124b  5e14a1ec
W[19] = 00000000  6dc2923e  6c0493fc  9d91626f
        f1310ecf  e3411cbf  f58c0a74  9f4f60b1
W[20] = 3b3cc4c4  f90806f8  2e2bd1d5  1785e87b
        2d4cd2b4  5c56a3aa  3cfac306  1a22e5de
W[21] = 053afac6  a64759b9  ce5931a7  5ef3a10d
        d70f28f1  c761389f  06f8f908  634e9cb2
W[22] = fe4201be  57fba805  993666ca  a2cb5d35
        d8cd2733  2733d8cd  9f4f60b1  52c1ad3f
W[23] = ac6053a0  468fb971  53a0ac60  d70f28f1
        3b3cc4c4  cadd3523  07d7f829  a2cb5d35
W[24] = 6f809080  51e2ae1e  1a22e5de  3523cadd
        95ba6a46  d8cd2733  ef73108d  c1483eb8
W[25] = 2f0ad0f6  d70f28f1  2575da8b  a3aa5c56
        aefd5103  ee94116c  c0693f97  053afac6
W[26] = 2496db6a  d1d52e2b  ef73108d  b2794d87
        2b8ed472  c5a33a5d  6ea1915f  ebf71409
W[27] = 931d6ce3  96996967  203bdfc5  a2cb5d35
        c3e53c1b  a80557fb  c761389f  4aeab516
W[28] = 53a0ac60  6ea1915f  e5de1a22  f82907d7
        08b6f74a  1b01e4ff  b19a4e66  c84037c0
W[29] = cadd3523  2aafd551  e1831e7d  07d7f829
        9af4650c  985767a9  44d1bb2f  dd2822d8
W[30] = b3584ca8  0c32f3ce  cc9b3365  9bd3642d
        124bedb5  2654d9ac  397ec682  ef73108d
W[31] = 2fe9d017  0faef052  915f6ea1  d5512aaf
        124bedb5  68889778  571ca8e4  bb2f44d1
```

Feistel Steps

```
IV :
A[0]=b314b806  B[0]=f778d95b  C[0]=14c1303a  D[0]=d10eca9e
A[1]=676cf96e  B[1]=6e5e21da  C[1]=b5b890d5  D[1]=ea3c1b82
A[2]=ed91a471  B[2]=ad570671  C[2]=82e61e95  D[2]=5061c319
A[3]=5f306791  B[3]=4584c064  C[3]=94f47683  D[3]=0c2a9f5c
A[4]=4ea515ee  B[4]=ac201a0f  C[4]=6ebc9ce7  D[4]=fcfc980e
A[5]=de2a06cf  B[5]=d4ce2a86  C[5]=f9af5b29  D[5]=bab373c6
```

```
A[6]=c9c96851  B[6]=c6d663f4  C[6]=f4177798  D[6]=1699d7c9
A[7]=4f49a403  B[7]=8ec5d766  C[7]=f6cec3ee  D[7]=0822d6af

IV XOR M :
A[0]=b314b806  B[0]=f778d95b  C[0]=14c1303a  D[0]=d10eca9e
A[1]=676cf96e  B[1]=6e5e21da  C[1]=b5b890d5  D[1]=ea3c1b82
A[2]=ed91a471  B[2]=ad570671  C[2]=82e61e95  D[2]=5061c319
A[3]=5f306791  B[3]=4584c064  C[3]=94f47683  D[3]=0c2a9f5c
A[4]=4ea515ee  B[4]=ac201a0f  C[4]=6ebc9ce7  D[4]=fcfc980e
A[5]=de2a06cf  B[5]=d4ce2a86  C[5]=f9af5b29  D[5]=bab373c6
A[6]=c9c96851  B[6]=c6d663f4  C[6]=f4177798  D[6]=1699d7c9
A[7]=4f49a403  B[7]=8ec5d766  C[7]=f6cec3ee  D[7]=0822d6af

Step  0: (r= 3, s=20)
A[0]=68f452f9  B[0]=98a5c035  C[0]=f778d95b  D[0]=14c1303a
A[1]=bda32fe3  B[1]=3b67cb73  C[1]=6e5e21da  D[1]=b5b890d5
A[2]=80a5e452  B[2]=6c8d238f  C[2]=ad570671  D[2]=82e61e95
A[3]=7cff7433  B[3]=f9833c8a  C[3]=4584c064  D[3]=94f47683
A[4]=b7b1d701  B[4]=7528af72  C[4]=ac201a0f  D[4]=6ebc9ce7
A[5]=e981b6e0  B[5]=f150367e  C[5]=d4ce2a86  D[5]=f9af5b29
A[6]=ff2adbff  B[6]=4e4b428e  C[6]=c6d663f4  D[6]=f4177798
A[7]=3b988cec  B[7]=7a4d201a  C[7]=8ec5d766  D[7]=f6cec3ee

Step  1: (r=20, s=14)
A[0]=f73a6059  B[0]=2f968f45  C[0]=98a5c035  D[0]=f778d95b
A[1]=abbe0b49  B[1]=fe3bda32  C[1]=3b67cb73  D[1]=6e5e21da
A[2]=36317609  B[2]=45280a5e  C[2]=6c8d238f  D[2]=ad570671
A[3]=040d92cb  B[3]=4337cff7  C[3]=f9833c8a  D[3]=4584c064
A[4]=c19833af  B[4]=701b7b1d  C[4]=7528af72  D[4]=ac201a0f
A[5]=a200fd68  B[5]=6e0e981b  C[5]=f150367e  D[5]=d4ce2a86
A[6]=d9ff8f49  B[6]=bffff2ad  C[6]=4e4b428e  D[6]=c6d663f4
A[7]=ae615264  B[7]=cec3b988  C[7]=7a4d201a  D[7]=8ec5d766

Step  2: (r=14, s=27)
A[0]=e4997e71  B[0]=98167dce  C[0]=2f968f45  D[0]=98a5c035
A[1]=5e290397  B[1]=82d26aef  C[1]=fe3bda32  D[1]=3b67cb73
A[2]=6e31ab7a  B[2]=5d824d8c  C[2]=45280a5e  D[2]=6c8d238f
A[3]=e1492649  B[3]=64b2c103  C[3]=4337cff7  D[3]=f9833c8a
A[4]=efcf30d2  B[4]=0cebf066  C[4]=701b7b1d  D[4]=7528af72
A[5]=5836eaac  B[5]=3f5a2880  C[5]=6e0e981b  D[5]=f150367e
A[6]=57af26a4  B[6]=e3d2767f  C[6]=bffff2ad  D[6]=4e4b428e
A[7]=635c6be4  B[7]=54992b98  C[7]=cec3b988  D[7]=7a4d201a

Step  3: (r=27, s= 3)
A[0]=7772dc35  B[0]=8f24cbf3  C[0]=98167dce  D[0]=2f968f45
A[1]=e68d1f73  B[1]=baf1481c  C[1]=82d26aef  D[1]=fe3bda32
A[2]=cda6c6ed  B[2]=d3718d5b  C[2]=5d824d8c  D[2]=45280a5e
A[3]=1c39e302  B[3]=4f0a4932  C[3]=64b2c103  D[3]=4337cff7
A[4]=a5dfd95f  B[4]=977e7986  C[4]=0cebf066  D[4]=701b7b1d
```

```
A[5]=80869aba  B[5]=62c1b755  C[5]=3f5a2880  D[5]=6e0e981b
A[6]=624ac2b2  B[6]=22bd7935  C[6]=e3d2767f  D[6]=bffff2ad
A[7]=4f0a9e0e  B[7]=231ae35f  C[7]=54992b98  D[7]=cec3b988

Step  4: (r= 3, s=20)
A[0]=948b8dd5  B[0]=bb96e1ab  C[0]=8f24cbf3  D[0]=98167dce
A[1]=0a266992  B[1]=3468fb9f  C[1]=baf1481c  D[1]=82d26aef
A[2]=1baf98f8  B[2]=6d36376e  C[2]=d3718d5b  D[2]=5d824d8c
A[3]=c23403c7  B[3]=e1cf1810  C[3]=4f0a4932  D[3]=64b2c103
A[4]=c4b7555e  B[4]=2efecafd  C[4]=977e7986  D[4]=0cebf066
A[5]=cd5c67e2  B[5]=0434d5d4  C[5]=62c1b755  D[5]=3f5a2880
A[6]=b96a0da9  B[6]=12561593  C[6]=22bd7935  D[6]=e3d2767f
A[7]=7c039124  B[7]=7854f072  C[7]=231ae35f  D[7]=54992b98

Step  5: (r=20, s=14)
A[0]=605c93e5  B[0]=dd5948b8  C[0]=bb96e1ab  D[0]=8f24cbf3
A[1]=c43b49b2  B[1]=9920a266  C[1]=3468fb9f  D[1]=baf1481c
A[2]=22673d39  B[2]=8f81baf9  C[2]=6d36376e  D[2]=d3718d5b
A[3]=b7f4aab6  B[3]=3c7c2340  C[3]=e1cf1810  D[3]=4f0a4932
A[4]=75aa908f  B[4]=55ec4b75  C[4]=2efecafd  D[4]=977e7986
A[5]=a61b36a4  B[5]=7e2cd5c6  C[5]=0434d5d4  D[5]=62c1b755
A[6]=f98682c3  B[6]=da9b96a0  C[6]=12561593  D[6]=22bd7935
A[7]=b0d8102b  B[7]=1247c039  C[7]=7854f072  D[7]=231ae35f

Step  6: (r=14, s=27)
A[0]=e623facd  B[0]=24f95817  C[0]=dd5948b8  D[0]=bb96e1ab
A[1]=f04b9e2b  B[1]=d26cb10e  C[1]=9920a266  D[1]=3468fb9f
A[2]=6e6b65c1  B[2]=cf4e4899  C[2]=8f81baf9  D[2]=6d36376e
A[3]=6c801a13  B[3]=2aadadfd  C[3]=3c7c2340  D[3]=e1cf1810
A[4]=22df4e97  B[4]=a423dd6a  C[4]=55ec4b75  D[4]=2efecafd
A[5]=42e30662  B[5]=cda92986  C[5]=7e2cd5c6  D[5]=0434d5d4
A[6]=8c5fa957  B[6]=a0b0fe61  C[6]=da9b96a0  D[6]=12561593
A[7]=9106d81e  B[7]=040aec36  C[7]=1247c039  D[7]=7854f072

Step  7: (r=27, s= 3)
A[0]=c6cafd80  B[0]=6f311fd6  C[0]=24f95817  D[0]=dd5948b8
A[1]=6b14585c  B[1]=5f825cf1  C[1]=d26cb10e  D[1]=9920a266
A[2]=0e4ef594  B[2]=0b735b2e  C[2]=cf4e4899  D[2]=8f81baf9
A[3]=6aea6322  B[3]=9b6400d0  C[3]=2aadadfd  D[3]=3c7c2340
A[4]=ed930ebf  B[4]=b916fa74  C[4]=a423dd6a  D[4]=55ec4b75
A[5]=79cb81ad  B[5]=12171833  C[5]=cda92986  D[5]=7e2cd5c6
A[6]=04cf95ff  B[6]=bc62fd4a  C[6]=a0b0fe61  D[6]=da9b96a0
A[7]=634101c4  B[7]=f48836c0  C[7]=040aec36  D[7]=1247c039

Step  8: (r=26, s= 4)
A[0]=050329ff  B[0]=031b2bf6  C[0]=6f311fd6  D[0]=24f95817
A[1]=d4afe407  B[1]=71ac5161  C[1]=5f825cf1  D[1]=d26cb10e
A[2]=e1c232c3  B[2]=50393bd6  C[2]=0b735b2e  D[2]=cf4e4899
A[3]=e933f855  B[3]=89aba98c  C[3]=9b6400d0  D[3]=2aadadfd
```

```
A[4]=8a162252  B[4]=ffb64c3a  C[4]=b916fa74  D[4]=a423dd6a
A[5]=94f5b736  B[5]=b5e72e06  C[5]=12171833  D[5]=cda92986
A[6]=12f56fdc  B[6]=fc133e57  C[6]=bc62fd4a  D[6]=a0b0fe61
A[7]=43a2f1d2  B[7]=118d0407  C[7]=f48836c0  D[7]=040aec36

Step  9: (r= 4, s=23)
A[0]=730df2e7  B[0]=50329ff0  C[0]=031b2bf6  D[0]=6f311fd6
A[1]=d7847580  B[1]=4afe407d  C[1]=71ac5161  D[1]=5f825cf1
A[2]=43b488f4  B[2]=1c232c3e  C[2]=50393bd6  D[2]=0b735b2e
A[3]=905e0b17  B[3]=933f855e  C[3]=89aba98c  D[3]=9b6400d0
A[4]=918a3834  B[4]=a1622528  C[4]=ffb64c3a  D[4]=b916fa74
A[5]=f66c9939  B[5]=4f5b7369  C[5]=b5e72e06  D[5]=12171833
A[6]=3d700289  B[6]=2f56fdc1  C[6]=fc133e57  D[6]=bc62fd4a
A[7]=c2211d3b  B[7]=3a2f1d24  C[7]=118d0407  D[7]=f48836c0

Step 10: (r=23, s=11)
A[0]=fbbf448b  B[0]=73b986f9  C[0]=50329ff0  D[0]=031b2bf6
A[1]=ac61be63  B[1]=c06bc23a  C[1]=4afe407d  D[1]=71ac5161
A[2]=6c7b3dd3  B[2]=7a21da44  C[2]=1c232c3e  D[2]=50393bd6
A[3]=64cef42c  B[3]=8bc82f05  C[3]=933f855e  D[3]=89aba98c
A[4]=665adcc0  B[4]=1a48c51c  C[4]=a1622528  D[4]=ffb64c3a
A[5]=f3de2611  B[5]=9cfb364c  C[5]=4f5b7369  D[5]=b5e72e06
A[6]=09f77105  B[6]=449eb801  C[6]=2f56fdc1  D[6]=fc133e57
A[7]=4bd6f6cc  B[7]=9de1108e  C[7]=3a2f1d24  D[7]=118d0407

Step 11: (r=11, s=26)
A[0]=cd5d725b  B[0]=fa245fdd  C[0]=73b986f9  D[0]=50329ff0
A[1]=617b6510  B[1]=0df31d63  C[1]=c06bc23a  D[1]=4afe407d
A[2]=af25e04a  B[2]=d9ee9b63  C[2]=7a21da44  D[2]=1c232c3e
A[3]=f6fa9064  B[3]=77a16326  C[3]=8bc82f05  D[3]=933f855e
A[4]=6f240c20  B[4]=d6e60332  C[4]=1a48c51c  D[4]=a1622528
A[5]=db04587a  B[5]=f1308f9e  C[5]=9cfb364c  D[5]=4f5b7369
A[6]=61a6420e  B[6]=bb88284f  C[6]=449eb801  D[6]=2f56fdc1
A[7]=e0e094af  B[7]=b7b6625e  C[7]=9de1108e  D[7]=3a2f1d24

Step 12: (r=26, s= 4)
A[0]=de30f89a  B[0]=6f3575c9  C[0]=fa245fdd  D[0]=73b986f9
A[1]=d1fe2d3f  B[1]=4185ed94  C[1]=0df31d63  D[1]=c06bc23a
A[2]=2cbe6621  B[2]=2abc9781  C[2]=d9ee9b63  D[2]=7a21da44
A[3]=d836fcf5  B[3]=93dbea41  C[3]=77a16326  D[3]=8bc82f05
A[4]=29fc8053  B[4]=81bc9030  C[4]=d6e60332  D[4]=1a48c51c
A[5]=03d11cdf  B[5]=eb6c1161  C[5]=f1308f9e  D[5]=9cfb364c
A[6]=8a4aa900  B[6]=39869908  C[6]=bb88284f  D[6]=449eb801
A[7]=308afd55  B[7]=bf838252  C[7]=b7b6625e  D[7]=9de1108e

Step 13: (r= 4, s=23)
A[0]=60094e96  B[0]=e30f89ad  C[0]=6f3575c9  D[0]=fa245fdd
A[1]=0482b5af  B[1]=1fe2d3fd  C[1]=4185ed94  D[1]=0df31d63
A[2]=fd5454d1  B[2]=cbe66212  C[2]=2abc9781  D[2]=d9ee9b63
```

```
A[3]=3795d2b1  B[3]=836fcf5d  C[3]=93dbea41  D[3]=77a16326
A[4]=504ec919  B[4]=9fc80532  C[4]=81bc9030  D[4]=d6e60332
A[5]=a1c50be5  B[5]=3d11cdf0  C[5]=eb6c1161  D[5]=f1308f9e
A[6]=0864a565  B[6]=a4aa9008  C[6]=39869908  D[6]=bb88284f
A[7]=e02e0c12  B[7]=08afd553  C[7]=bf838252  D[7]=b7b6625e

Step 14: (r=23, s=11)
A[0]=90648b2d  B[0]=4b3004a7  C[0]=e30f89ad  D[0]=6f3575c9
A[1]=74e5eb55  B[1]=d782415a  C[1]=1fe2d3fd  D[1]=4185ed94
A[2]=d277a5d5  B[2]=68feaa2a  C[2]=cbe66212  D[2]=2abc9781
A[3]=4f464ea4  B[3]=589bcae9  C[3]=836fcf5d  D[3]=93dbea41
A[4]=5b077ea8  B[4]=8ca82764  C[4]=9fc80532  D[4]=81bc9030
A[5]=dbf099b3  B[5]=f2d0e285  C[5]=3d11cdf0  D[5]=eb6c1161
A[6]=6ddd82bd  B[6]=b2843252  C[6]=a4aa9008  D[6]=39869908
A[7]=c8edbde1  B[7]=09701706  C[7]=08afd553  D[7]=bf838252

Step 15: (r=11, s=26)
A[0]=a630ab9a  B[0]=24596c83  C[0]=4b3004a7  D[0]=e30f89ad
A[1]=2c42fd8b  B[1]=2f5aaba7  C[1]=d782415a  D[1]=1fe2d3fd
A[2]=6c4370ed  B[2]=bd2eae93  C[2]=68feaa2a  D[2]=cbe66212
A[3]=321c1179  B[3]=3275227a  C[3]=589bcae9  D[3]=836fcf5d
A[4]=b77dd7f6  B[4]=3bf542d8  C[4]=8ca82764  D[4]=9fc80532
A[5]=e2758c45  B[5]=84cd9edf  C[5]=f2d0e285  D[5]=3d11cdf0
A[6]=98701009  B[6]=ec15eb6e  C[6]=b2843252  D[6]=a4aa9008
A[7]=40c6c72f  B[7]=6def0e47  C[7]=09701706  D[7]=08afd553

Step 16: (r=19, s=28)
A[0]=2c1372c4  B[0]=5cd53185  C[0]=24596c83  D[0]=4b3004a7
A[1]=df3f18f2  B[1]=ec596217  C[1]=2f5aaba7  D[1]=d782415a
A[2]=bdd50f28  B[2]=876b621b  C[2]=bd2eae93  D[2]=68feaa2a
A[3]=b7220bea  B[3]=8bc990e0  C[3]=3275227a  D[3]=589bcae9
A[4]=7d3ffcd7  B[4]=bfb5bbee  C[4]=3bf542d8  D[4]=8ca82764
A[5]=c7138d39  B[5]=622f13ac  C[5]=84cd9edf  D[5]=f2d0e285
A[6]=04335b96  B[6]=804cc380  C[6]=ec15eb6e  D[6]=b2843252
A[7]=4751105b  B[7]=397a0636  C[7]=6def0e47  D[7]=09701706

Step 17: (r=28, s= 7)
A[0]=eee04a3b  B[0]=42c1372c  C[0]=5cd53185  D[0]=24596c83
A[1]=0241f0c2  B[1]=2df3f18f  C[1]=ec596217  D[1]=2f5aaba7
A[2]=3665dc24  B[2]=8bdd50f2  C[2]=876b621b  D[2]=bd2eae93
A[3]=3c52c894  B[3]=ab7220be  C[3]=8bc990e0  D[3]=3275227a
A[4]=955568fe  B[4]=77d3ffcd  C[4]=bfb5bbee  D[4]=3bf542d8
A[5]=cd9401fc  B[5]=9c7138d3  C[5]=622f13ac  D[5]=84cd9edf
A[6]=a05439a5  B[6]=604335b9  C[6]=804cc380  D[6]=ec15eb6e
A[7]=042016d0  B[7]=b4751105  C[7]=397a0636  D[7]=6def0e47

Step 18: (r= 7, s=22)
A[0]=ee6b6167  B[0]=70251df7  C[0]=42c1372c  D[0]=5cd53185
A[1]=e60b93cf  B[1]=20f86101  C[1]=2df3f18f  D[1]=ec596217
```

```
A[2]=82ea98d4  B[2]=32ee121b  C[2]=8bdd50f2  D[2]=876b621b
A[3]=d4eac4d8  B[3]=29644a1e  C[3]=ab7220be  D[3]=8bc990e0
A[4]=97327f3e  B[4]=aab47f4a  C[4]=77d3ffcd  D[4]=bfb5bbee
A[5]=cc38a6c9  B[5]=ca00fe66  C[5]=9c7138d3  D[5]=622f13ac
A[6]=77b6e5fd  B[6]=2a1cd2d0  C[6]=604335b9  D[6]=804cc380
A[7]=86677d67  B[7]=100b6802  C[7]=b4751105  D[7]=397a0636

Step 19: (r=22, s=19)
A[0]=174bb851  B[0]=59fb9ad8  C[0]=70251df7  D[0]=42c1372c
A[1]=5d272ecb  B[1]=f3f982e4  C[1]=20f86101  D[1]=2df3f18f
A[2]=b1ade933  B[2]=3520baa6  C[2]=32ee121b  D[2]=8bdd50f2
A[3]=f64c4039  B[3]=36353ab1  C[3]=29644a1e  D[3]=ab7220be
A[4]=ae40399e  B[4]=cfa5cc9f  C[4]=aab47f4a  D[4]=77d3ffcd
A[5]=69e27073  B[5]=b2730e29  C[5]=ca00fe66  D[5]=9c7138d3
A[6]=2b457c1a  B[6]=7f5dedb9  C[6]=2a1cd2d0  D[6]=604335b9
A[7]=ad7d8197  B[7]=59e199df  C[7]=100b6802  D[7]=b4751105

Step 20: (r=19, s=28)
A[0]=93518285  B[0]=c288ba5d  C[0]=59fb9ad8  D[0]=70251df7
A[1]=4c180c11  B[1]=765ae939  C[1]=f3f982e4  D[1]=20f86101
A[2]=b08b1031  B[2]=499d8d6f  C[2]=3520baa6  D[2]=32ee121b
A[3]=793352a6  B[3]=01cfb262  C[3]=36353ab1  D[3]=29644a1e
A[4]=78d7a414  B[4]=ccf57201  C[4]=cfa5cc9f  D[4]=aab47f4a
A[5]=db2817af  B[5]=839b4f13  C[5]=b2730e29  D[5]=ca00fe66
A[6]=89472b41  B[6]=e0d15a2b  C[6]=7f5dedb9  D[6]=2a1cd2d0
A[7]=8f517232  B[7]=0cbd6bec  C[7]=59e199df  D[7]=100b6802

Step 21: (r=28, s= 7)
A[0]=b7e27e27  B[0]=59351828  C[0]=c288ba5d  D[0]=59fb9ad8
A[1]=33b4aac8  B[1]=14c180c1  C[1]=765ae939  D[1]=f3f982e4
A[2]=c1a30cc1  B[2]=1b08b103  C[2]=499d8d6f  D[2]=3520baa6
A[3]=dc50679d  B[3]=6793352a  C[3]=01cfb262  D[3]=36353ab1
A[4]=755a9adb  B[4]=478d7a41  C[4]=ccf57201  D[4]=cfa5cc9f
A[5]=77982f35  B[5]=fdb2817a  C[5]=839b4f13  D[5]=b2730e29
A[6]=7d28face  B[6]=189472b4  C[6]=e0d15a2b  D[6]=7f5dedb9
A[7]=a372daba  B[7]=28f51723  C[7]=0cbd6bec  D[7]=59e199df

Step 22: (r= 7, s=22)
A[0]=6a3854c6  B[0]=f13f13db  C[0]=59351828  D[0]=c288ba5d
A[1]=811e18b2  B[1]=da556419  C[1]=14c180c1  D[1]=765ae939
A[2]=78dd92e6  B[2]=d18660e0  C[2]=1b08b103  D[2]=499d8d6f
A[3]=715522ad  B[3]=2833ceee  C[3]=6793352a  D[3]=01cfb262
A[4]=ad2f6309  B[4]=ad4d6dba  C[4]=478d7a41  D[4]=ccf57201
A[5]=5bfab11d  B[5]=cc179abb  C[5]=fdb2817a  D[5]=839b4f13
A[6]=207b338b  B[6]=947d673e  C[6]=189472b4  D[6]=e0d15a2b
A[7]=a3747a03  B[7]=b96d5d51  C[7]=28f51723  D[7]=0cbd6bec

Step 23: (r=22, s=19)
A[0]=b8aa8d08  B[0]=319a8e15  C[0]=f13f13db  D[0]=59351828
```

```
A[1]=613168a9  B[1]=2ca04786  C[1]=da556419  D[1]=14c180c1
A[2]=3857d523  B[2]=b99e3764  C[2]=d18660e0  D[2]=1b08b103
A[3]=90f2acae  B[3]=ab5c5548  C[3]=2833ceee  D[3]=6793352a
A[4]=40103812  B[4]=c26b4bd8  C[4]=ad4d6dba  D[4]=478d7a41
A[5]=d829a8de  B[5]=4756feac  C[5]=cc179abb  D[5]=fdb2817a
A[6]=ea36009a  B[6]=e2c81ecc  C[6]=947d673e  D[6]=189472b4
A[7]=ec7f1d39  B[7]=80e8dd1e  C[7]=b96d5d51  D[7]=28f51723

Step 24: (r=15, s= 5)
A[0]=fefd9fff  B[0]=46845c55  C[0]=319a8e15  D[0]=f13f13db
A[1]=6792ca39  B[1]=b454b098  C[1]=2ca04786  D[1]=da556419
A[2]=2e90e09e  B[2]=ea919c2b  C[2]=b99e3764  D[2]=d18660e0
A[3]=8b9a6613  B[3]=56574879  C[3]=ab5c5548  D[3]=2833ceee
A[4]=2715b40d  B[4]=1c092008  C[4]=c26b4bd8  D[4]=ad4d6dba
A[5]=6ed58b4b  B[5]=d46f6c14  C[5]=4756feac  D[5]=cc179abb
A[6]=58ba53fe  B[6]=004d751b  C[6]=e2c81ecc  D[6]=947d673e
A[7]=7503db8a  B[7]=8e9cf63f  C[7]=80e8dd1e  D[7]=b96d5d51

Step 25: (r= 5, s=29)
A[0]=9f1613e9  B[0]=dfb3ffff  C[0]=46845c55  D[0]=319a8e15
A[1]=8eff64c6  B[1]=f259472c  C[1]=b454b098  D[1]=2ca04786
A[2]=96075a59  B[2]=d21c13c5  C[2]=ea919c2b  D[2]=b99e3764
A[3]=b01fd6bf  B[3]=734cc271  C[3]=56574879  D[3]=ab5c5548
A[4]=bb61451d  B[4]=e2b681a4  C[4]=1c092008  D[4]=c26b4bd8
A[5]=2079d667  B[5]=dab1696d  C[5]=d46f6c14  D[5]=4756feac
A[6]=e19c6221  B[6]=174a7fcb  C[6]=004d751b  D[6]=e2c81ecc
A[7]=83238f33  B[7]=a07b714e  C[7]=8e9cf63f  D[7]=80e8dd1e

Step 26: (r=29, s= 9)
A[0]=f7f76a51  B[0]=33e2c27d  C[0]=dfb3ffff  D[0]=46845c55
A[1]=dac727a5  B[1]=d1dfec98  C[1]=f259472c  D[1]=b454b098
A[2]=2fcbe413  B[2]=32c0eb4b  C[2]=d21c13c5  D[2]=ea919c2b
A[3]=fc46aa4b  B[3]=f603fad7  C[3]=734cc271  D[3]=56574879
A[4]=3a8697ff  B[4]=b76c28a3  C[4]=e2b681a4  D[4]=1c092008
A[5]=9603e90d  B[5]=e40f3acc  C[5]=dab1696d  D[5]=d46f6c14
A[6]=382e793d  B[6]=3c338c44  C[6]=174a7fcb  D[6]=004d751b
A[7]=72a72e70  B[7]=706471e6  C[7]=a07b714e  D[7]=8e9cf63f

Step 27: (r= 9, s=15)
A[0]=5dcb8937  B[0]=eed4a3ef  C[0]=33e2c27d  D[0]=dfb3ffff
A[1]=c715b912  B[1]=8e4f4bb5  C[1]=d1dfec98  D[1]=f259472c
A[2]=94ce7941  B[2]=97c8265f  C[2]=32c0eb4b  D[2]=d21c13c5
A[3]=166dd8fb  B[3]=8d5497f8  C[3]=f603fad7  D[3]=734cc271
A[4]=1d380d00  B[4]=0d2ffe75  C[4]=b76c28a3  D[4]=e2b681a4
A[5]=848cf048  B[5]=07d21b2c  C[5]=e40f3acc  D[5]=dab1696d
A[6]=f60829e7  B[6]=5cf27a70  C[6]=3c338c44  D[6]=174a7fcb
A[7]=9bb67cfa  B[7]=4e5ce0e5  C[7]=706471e6  D[7]=a07b714e

Step 28: (r=15, s= 5)
```

```
A[0]=3f6f5f60  B[0]=c49baee5  C[0]=eed4a3ef  D[0]=33e2c27d
A[1]=cff3f24a  B[1]=dc89638a  C[1]=8e4f4bb5  D[1]=d1dfec98
A[2]=c4d0b17f  B[2]=3ca0ca67  C[2]=97c8265f  D[2]=32c0eb4b
A[3]=741572c7  B[3]=ec7d8b36  C[3]=8d5497f8  D[3]=f603fad7
A[4]=8b58e427  B[4]=06800e9c  C[4]=0d2ffe75  D[4]=b76c28a3
A[5]=4eb125ab  B[5]=78244246  C[5]=07d21b2c  D[5]=e40f3acc
A[6]=e15c2083  B[6]=14f3fb04  C[6]=5cf27a70  D[6]=3c338c44
A[7]=7af7399c  B[7]=3e7d4ddb  C[7]=4e5ce0e5  D[7]=706471e6

Step 29: (r= 5, s=29)
A[0]=57ca24e8  B[0]=edebec07  C[0]=c49baee5  D[0]=eed4a3ef
A[1]=fc19bd9c  B[1]=fe7e4959  C[1]=dc89638a  D[1]=8e4f4bb5
A[2]=e30c818f  B[2]=9a162ff8  C[2]=3ca0ca67  D[2]=97c8265f
A[3]=dbc47a37  B[3]=82ae58ee  C[3]=ec7d8b36  D[3]=8d5497f8
A[4]=b7b13ff8  B[4]=6b1c84f1  C[4]=06800e9c  D[4]=0d2ffe75
A[5]=d84a0843  B[5]=d624b569  C[5]=78244246  D[5]=07d21b2c
A[6]=e5db7d1f  B[6]=2b84107c  C[6]=14f3fb04  D[6]=5cf27a70
A[7]=4fa5f53c  B[7]=5ee7338f  C[7]=3e7d4ddb  D[7]=4e5ce0e5

Step 30: (r=29, s= 9)
A[0]=7b2fb776  B[0]=0af9449d  C[0]=edebec07  D[0]=c49baee5
A[1]=340da6d0  B[1]=9f8337b3  C[1]=fe7e4959  D[1]=dc89638a
A[2]=4ad4a744  B[2]=fc619031  C[2]=9a162ff8  D[2]=3ca0ca67
A[3]=3fa2dfe7  B[3]=fb788f46  C[3]=82ae58ee  D[3]=ec7d8b36
A[4]=136ed3d4  B[4]=16f627ff  C[4]=6b1c84f1  D[4]=06800e9c
A[5]=924bc63d  B[5]=7b094108  C[5]=d624b569  D[5]=78244246
A[6]=28f7552b  B[6]=fcbb6fa3  C[6]=2b84107c  D[6]=14f3fb04
A[7]=75c767d6  B[7]=89f4bea7  C[7]=5ee7338f  D[7]=3e7d4ddb

Step 31: (r= 9, s=15)
A[0]=8f31585e  B[0]=5f6eecf6  C[0]=0af9449d  D[0]=edebec07
A[1]=55635047  B[1]=1b4da068  C[1]=9f8337b3  D[1]=fe7e4959
A[2]=5ee6aa7b  B[2]=a94e8895  C[2]=fc619031  D[2]=9a162ff8
A[3]=59b56ba7  B[3]=45bfce7f  C[3]=fb788f46  D[3]=82ae58ee
A[4]=a192031b  B[4]=dda7a826  C[4]=16f627ff  D[4]=6b1c84f1
A[5]=6ac179c3  B[5]=978c7b24  C[5]=7b094108  D[5]=d624b569
A[6]=a5d852f8  B[6]=eeaa5651  C[6]=fcbb6fa3  D[6]=2b84107c
A[7]=2ad97a48  B[7]=8ecfaceb  C[7]=89f4bea7  D[7]=5ee7338f

Feed-Forward Step 0: (r=15, s= 5)
A[0]=c541c747  B[0]=ac2f4798  C[0]=5f6eecf6  D[0]=0af9449d
A[1]=e1bc9e78  B[1]=a823aab1  C[1]=1b4da068  D[1]=9f8337b3
A[2]=b3c13c1f  B[2]=553daf73  C[2]=a94e8895  D[2]=fc619031
A[3]=10cf8c4b  B[3]=b5d3acda  C[3]=45bfce7f  D[3]=fb788f46
A[4]=f1d9ae0a  B[4]=018dd0c9  C[4]=dda7a826  D[4]=16f627ff
A[5]=fc7478e1  B[5]=bce1b560  C[5]=978c7b24  D[5]=7b094108
A[6]=fc43198a  B[6]=297c52ec  C[6]=eeaa5651  D[6]=fcbb6fa3
A[7]=6d4ce313  B[7]=bd24156c  C[7]=8ecfaceb  D[7]=89f4bea7
```

```
Feed-Forward Step 1: (r= 5, s=29)
A[0]=8c3bb5ab  B[0]=a838e8f8  C[0]=ac2f4798  D[0]=5f6eecf6
A[1]=d2f9e9d9  B[1]=3793cf1c  C[1]=a823aab1  D[1]=1b4da068
A[2]=6091f15e  B[2]=782783f6  C[2]=553daf73  D[2]=a94e8895
A[3]=4a71f2e1  B[3]=19f18962  C[3]=b5d3acda  D[3]=45bfce7f
A[4]=e27be9a6  B[4]=3b35c15e  C[4]=018dd0c9  D[4]=dda7a826
A[5]=eb94564b  B[5]=8e8f1c3f  C[5]=bce1b560  D[5]=978c7b24
A[6]=590506ac  B[6]=8863315f  C[6]=297c52ec  D[6]=eeaa5651
A[7]=479750bd  B[7]=a99c626d  C[7]=bd24156c  D[7]=8ecfaceb

Feed-Forward Step 2: (r=29, s= 9)
A[0]=82f2ba4f  B[0]=718776b5  C[0]=a838e8f8  D[0]=ac2f4798
A[1]=bf198aec  B[1]=3a5f3d3b  C[1]=3793cf1c  D[1]=a823aab1
A[2]=41dfce0b  B[2]=cc123e2b  C[2]=782783f6  D[2]=553daf73
A[3]=2bf27665  B[3]=294e3e5c  C[3]=19f18962  D[3]=b5d3acda
A[4]=5d7af73c  B[4]=dc4f7d34  C[4]=3b35c15e  D[4]=018dd0c9
A[5]=0f292e8b  B[5]=7d728ac9  C[5]=8e8f1c3f  D[5]=bce1b560
A[6]=b09ba751  B[6]=8b20a0d5  C[6]=8863315f  D[6]=297c52ec
A[7]=16f40333  B[7]=a8f2ea17  C[7]=a99c626d  D[7]=bd24156c

Feed-Forward Step 3: (r= 9, s=15)
A[0]=38644b9e  B[0]=e5749f05  C[0]=718776b5  D[0]=a838e8f8
A[1]=dc12fc9b  B[1]=3315d97e  C[1]=3a5f3d3b  D[1]=3793cf1c
A[2]=f8943249  B[2]=bf9c1683  C[2]=cc123e2b  D[2]=782783f6
A[3]=edc4e3ce  B[3]=e4ecca57  C[3]=294e3e5c  D[3]=19f18962
A[4]=d49b5d71  B[4]=f5ee78ba  C[4]=dc4f7d34  D[4]=3b35c15e
A[5]=d5075c1b  B[5]=525d161e  C[5]=7d728ac9  D[5]=8e8f1c3f
A[6]=2d267abe  B[6]=374ea361  C[6]=8b20a0d5  D[6]=8863315f
A[7]=8c2a01f6  B[7]=e806662d  C[7]=a8f2ea17  D[7]=a99c626d
```

Compression Function Output

```
A[0]=38644b9e  B[0]=e5749f05  C[0]=718776b5  D[0]=a838e8f8
A[1]=dc12fc9b  B[1]=3315d97e  C[1]=3a5f3d3b  D[1]=3793cf1c
A[2]=f8943249  B[2]=bf9c1683  C[2]=cc123e2b  D[2]=782783f6
A[3]=edc4e3ce  B[3]=e4ecca57  C[3]=294e3e5c  D[3]=19f18962
A[4]=d49b5d71  B[4]=f5ee78ba  C[4]=dc4f7d34  D[4]=3b35c15e
A[5]=d5075c1b  B[5]=525d161e  C[5]=7d728ac9  D[5]=8e8f1c3f
A[6]=2d267abe  B[6]=374ea361  C[6]=8b20a0d5  D[6]=8863315f
A[7]=8c2a01f6  B[7]=e806662d  C[7]=a8f2ea17  D[7]=a99c626d
```

Hash Function Output

```
9e 4b 64 38 9b fc 12 dc 49 32 94 f8 ce e3 c4 ed
71 5d 9b d4 1b 5c 07 d5 be 7a 26 2d f6 01 2a 8c
05 9f 74 e5 7e d9 15 33 83 16 9c bf 57 ca ec e4
ba 78 ee f5 1e 16 5d 52 61 a3 4e 37 2d 66 06 e8
```

6.4.2 One block message

We use the message block `0x00 0x01 0x02` ... as an example.

First message block

```
M[  0..  7] = 00 01 02 03 04 05 06 07
M[  8.. 15] = 08 09 0a 0b 0c 0d 0e 0f
M[ 16.. 23] = 10 11 12 13 14 15 16 17
M[ 24.. 31] = 18 19 1a 1b 1c 1d 1e 1f
M[ 32.. 39] = 20 21 22 23 24 25 26 27
M[ 40.. 47] = 28 29 2a 2b 2c 2d 2e 2f
M[ 48.. 55] = 30 31 32 33 34 35 36 37
M[ 56.. 63] = 38 39 3a 3b 3c 3d 3e 3f
M[ 64.. 71] = 40 41 42 43 44 45 46 47
M[ 72.. 79] = 48 49 4a 4b 4c 4d 4e 4f
M[ 80.. 87] = 50 51 52 53 54 55 56 57
M[ 88.. 95] = 58 59 5a 5b 5c 5d 5e 5f
M[ 96..103] = 60 61 62 63 64 65 66 67
M[104..111] = 68 69 6a 6b 6c 6d 6e 6f
M[112..119] = 70 71 72 73 74 75 76 77
M[120..127] = 78 79 7a 7b 7c 7d 7e 7f
```

NTT Output

```
y[  0..  7] =  162   85  125  159   75  219   54   22
y[  8.. 15] =  128  171   94  185    6   71   55   63
y[ 16.. 23] =    0  203    4  152  200   45   80  133
y[ 24.. 31] =  245  117  101  152   61   77  169  230
y[ 32.. 39] =  150  100  200  254  121   31  253   22
y[ 40.. 47] =  186  171   27   59  145   41  103  177
y[ 48.. 55] =   23   10  157    5  176   84  216   88
y[ 56.. 63] =   57   20  253    9  130  255   53   84
y[ 64.. 71] =  181  160  241   61   47  252  168   18
y[ 72.. 79] =  237   26   30   19  166   18  110  113
y[ 80.. 87] =   21  240   15  103  230   72   61  142
y[ 88.. 95] =  138  119   66   45   86   29   84  243
y[ 96..103] =  202   33  131  121  206  189   63   26
y[104..111] =  129  171   92   61  218   92  254   87
y[112..119] =   84  189  205  152  233    8  203  182
y[120..127] =  168  207  190  143  124  129   57   30
y[128..135] =  192  141   92  168  121  110  169   28
y[136..143] =  128  161  211  146  197   45   44  249
y[144..151] =  171  249   62   82  157  156   70   32
y[152..159] =  122  202  163   42  174   32   21  256
y[160..167] =  244   93  107    0   28  137   44  134
y[168..175] =  129  255  154   17   97  197  180   68
y[176..183] =  132  107  244   30   65  163  147  190
y[184..191] =  115  193   79   65   69  180   30   67
y[192..199] =  205    3  191  238   12   69   15  256
```

```
y[200..207] =  106   66  122   90  108  168    4   39
y[208..215] =   82  251  217  159   43   47   16  138
y[216..223] =   62   41  152   21   23  239  124  246
y[224..231] =  176   51  194   43   74   68  188  100
y[232..239] =   19  207   16  134  197   67  195   38
y[240..247] =    3  145  211  141   79   12    7  226
y[248..255] =   91   41  102  109  195  181  241   46
```

Intermediate Expanded Message

```
Z[ 0] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
Z[ 1] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
Z[ 2] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
Z[ 3] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
Z[ 4] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
Z[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
Z[ 6] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
Z[ 7] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
Z[ 8] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
Z[ 9] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
Z[10] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
Z[11] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
Z[12] = 022bda6c  f245d04e  31dd08ac  ff470ad7
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
Z[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
Z[14] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
Z[15] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
Z[16] = c761ad3f  50246ce3  69674155  b3582f0a
        6f806f80  d7ee51e2  cbbc053a  26542fe9
Z[17] = b5160000  3602037c  a8e4ce59  3cfa45b0
        6a46f58c  ae1e57fb  b7b33523  124bb358
Z[18] = f4ada2cb  5d35ce59  18646967  2654fc84
        9080c227  a6471785  547f9e70  bced59b9
Z[19] = 931d1409  f4ada8e4  389fb971  a02edc49
```

```
            642d31a7  44d1fc84  3c1b915f  1a222e2b
Z[20] =  d2b4bdcc  c682f210  0a7428f1  0d11b279
            5c56ee94  6a461a22  5e14b0bb  037c5fd2
Z[21] =  476e124b  dd280d11  2575e87b  0df03523
            36029857  a489397e  14094aea  6c04492c
Z[22] =  b971d017  c91f923e  4076d393  c3e536e1
            108d9080  0df05024  cbbcde07  c9fefd63
Z[23] =  029d492c  d7eed2b4  44d1eb18  0619d0f6
            4f45b279  58dac5a3  c9fe6c04  f21031a7
Z[24] =  9af44a0b  b279aaa2  5fd2dee6  1864132a
            ac60b516  9f4fc148  27333dd9  f90836e1
Z[25] =  f908d0f6  476ea489  a8052733  1be093fc
            d01765eb  2496a489  1be04313  ff21e87b
Z[26] =  5103571c  0000fd63  97781b01  94db132a
            fe42b516  0ecf3365  cbbc23b7  3b3cba50
Z[27] =  5d3508b6  1a22045b  ae1e492c  c5a34ca8
            c840116c  389f07d7  bcedfe42  3a5d492c
Z[28] =  029dab81  ef733523  3c1bfba5  ff210fae
            397e16a6  4e66108d  b2790fae  21f9626f
Z[29] =  fac6f131  aaa259b9  28f13eb8  98579bd3
            23b767a9  124b2733  f0521943  f66bf3ce
Z[30] =  2c6d1cbf  25756967  3b3cc4c4  571c16a6
            d472b516  94db3523  3a5d5024  211a4bc9
Z[31] =  9e70c4c4  9af4a489  0a7406f8  e4ffbeab
            23b7d472  5ef39cb2  bdcc9080  28121a22
```

Expanded Message

```
W[ 0] = b9e7c914  2c15f470  fc6321f7  0d02bfaf
        12caf18c  0dbb15ae  0d02be3d  51a94f7e
W[ 1] = 17d9d841  5771a4f2  cedcdb25  12ca2d87
        c1daa380  2c15427c  427ce3d1  3edffdd5
W[ 2] = 3d6dbb59  b92e5a55  e48a3633  0fe62706
        c1da5c80  cbf843ee  334f0456  2d8727bf
W[ 3] = 4844b2ad  fdd5d6cf  16675771  0fe6fd1c
        c1daccb1  2aa31383  1da1af10  c6304a6f
W[ 4] = cedc3cb4  b41fda6c  05c8eea8  c9cdd8fa
        dbdebfaf  ad9ecf95  a380599c  15ae2931
W[ 5] = f3b70f2d  4a6f0ad7  3408ec7d  ace52c15
        55ffaa01  20852fb2  14f53e26  f5e23cb4
W[ 6] = 073a109f  039db7bc  3cb4c577  3f98e25f
        0e742931  0681fd1c  fe8ea439  3cb4264d
W[ 7] = d8fa0000  b41f02e4  2085d6cf  a66439d0
        548df754  b41f48fd  37a52c15  ec7dc068
W[ 8] = af10022b  ac2cdec2  08ac3917  e999050f
        1da141c3  4ec549b6  c914d332  213ef470
W[ 9] = 4d53a5ab  15aef69b  bc122ef9  cf95b082
        d1c0531b  2ef93917  c85b31dd  306b15ae
W[10] = 022bda6c  f245d04e  31dd08ac  ff470ad7
```

```
        2fb24c9a  410a582a  bfaf4e0c  1c2f02e4
W[11] = ac2cd107  bfaf427c  4f7e5771  143cc068
        baa05c80  afc9dec2  2085d4a4  fa381fcc
W[12] = fa38c1da  3b422cce  b703b7bc  17203296
        d841582a  1e5abc12  1720c405  ff470f2d
W[13] = fbaa3b42  b92ee318  21f71f13  aa010b90
        1da12cce  0f2db41f  f2fe109f  f80d599c
W[14] = 4335f69b  00004d53  a948143c  a71d1fcc
        fe8ea380  0c49b591  d4a44619  3124c85b
W[15] = 24dbc577  1f13d279  3124357a  4844ce23
        dbde0dbb  a71d0b90  306bd4a4  1b76d332
W[16] = b5160000  3602037c  a8e4ce59  3cfa45b0
        6a46f58c  ae1e57fb  b7b33523  124bb358
W[17] = f4ada2cb  5d35ce59  18646967  2654fc84
        9080c227  a6471785  547f9e70  bced59b9
W[18] = 029d492c  d7eed2b4  44d1eb18  0619d0f6
        4f45b279  58dac5a3  c9fe6c04  f21031a7
W[19] = d2b4bdcc  c682f210  0a7428f1  0d11b279
        5c56ee94  6a461a22  5e14b0bb  037c5fd2
W[20] = b971d017  c91f923e  4076d393  c3e536e1
        108d9080  0df05024  cbbcde07  c9fefd63
W[21] = 476e124b  dd280d11  2575e87b  0df03523
        36029857  a489397e  14094aea  6c04492c
W[22] = c761ad3f  50246ce3  69674155  b3582f0a
        6f806f80  d7ee51e2  cbbc053a  26542fe9
W[23] = 931d1409  f4ada8e4  389fb971  a02edc49
        642d31a7  44d1fc84  3c1b915f  1a222e2b
W[24] = 2c6d1cbf  25756967  3b3cc4c4  571c16a6
        d472b516  94db3523  3a5d5024  211a4bc9
W[25] = 9af44a0b  b279aaa2  5fd2dee6  1864132a
        ac60b516  9f4fc148  27333dd9  f90836e1
W[26] = f908d0f6  476ea489  a8052733  1be093fc
        d01765eb  2496a489  1be04313  ff21e87b
W[27] = 9e70c4c4  9af4a489  0a7406f8  e4ffbeab
        23b7d472  5ef39cb2  bdcc9080  28121a22
W[28] = 5d3508b6  1a22045b  ae1e492c  c5a34ca8
        c840116c  389f07d7  bcedfe42  3a5d492c
W[29] = fac6f131  aaa259b9  28f13eb8  98579bd3
        23b767a9  124b2733  f0521943  f66bf3ce
W[30] = 029dab81  ef733523  3c1bfba5  ff210fae
        397e16a6  4e66108d  b2790fae  21f9626f
W[31] = 5103571c  0000fd63  97781b01  94db132a
        fe42b516  0ecf3365  cbbc23b7  3b3cba50
```

Feistel Steps

```
IV :
A[0]=b314b806  B[0]=f778d95b  C[0]=14c1303a  D[0]=d10eca9e
A[1]=676cf96e  B[1]=6e5e21da  C[1]=b5b890d5  D[1]=ea3c1b82
```

```
A[2]=ed91a471  B[2]=ad570671  C[2]=82e61e95  D[2]=5061c319
A[3]=5f306791  B[3]=4584c064  C[3]=94f47683  D[3]=0c2a9f5c
A[4]=4ea515ee  B[4]=ac201a0f  C[4]=6ebc9ce7  D[4]=fcfc980e
A[5]=de2a06cf  B[5]=d4ce2a86  C[5]=f9af5b29  D[5]=bab373c6
A[6]=c9c96851  B[6]=c6d663f4  C[6]=f4177798  D[6]=1699d7c9
A[7]=4f49a403  B[7]=8ec5d766  C[7]=f6cec3ee  D[7]=0822d6af

IV XOR M :
A[0]=b016b906  B[0]=d45af87b  C[0]=5783717a  D[0]=b26cabfe
A[1]=606afc6a  B[1]=497804fe  C[1]=f2fed591  D[1]=8d5a7ee6
A[2]=e69bad79  B[2]=867d2f59  C[2]=c9ac57dd  D[2]=3b0baa71
A[3]=503e6a9d  B[3]=6aaaed48  C[3]=dbba3bcf  D[3]=6344f230
A[4]=5db704fe  B[4]=9f122b3f  C[4]=3deecdb7  D[4]=8f8ee97e
A[5]=c93c13db  B[5]=e3f81fb2  C[5]=aef90e7d  D[5]=cdc506b2
A[6]=d2d37149  B[6]=fdec5acc  C[6]=af4d2ec0  D[6]=6de3aeb1
A[7]=5057b91f  B[7]=b1fbea5a  C[7]=a9909eb2  D[7]=775cabd3

Step  0: (r= 3, s=20)
A[0]=dc1c21d9  B[0]=80b5c835  C[0]=d45af87b  D[0]=5783717a
A[1]=15ce8efc  B[1]=0357e353  C[1]=497804fe  D[1]=f2fed591
A[2]=464fbfae  B[2]=34dd6bcf  C[2]=867d2f59  D[2]=c9ac57dd
A[3]=e7712af1  B[3]=81f354ea  C[3]=6aaaed48  D[3]=dbba3bcf
A[4]=8e7e9a28  B[4]=edb827f2  C[4]=9f122b3f  D[4]=3deecdb7
A[5]=af245f85  B[5]=49e09ede  C[5]=e3f81fb2  D[5]=aef90e7d
A[6]=3e255426  B[6]=969b8a4e  C[6]=fdec5acc  D[6]=af4d2ec0
A[7]=3753b7e8  B[7]=82bdc8fa  C[7]=b1fbea5a  D[7]=a9909eb2

Step  1: (r=20, s=14)
A[0]=036020e8  B[0]=1d9dc1c2  C[0]=80b5c835  D[0]=d45af87b
A[1]=6e53dc0b  B[1]=efc15ce8  C[1]=0357e353  D[1]=497804fe
A[2]=b5560903  B[2]=fae464fb  C[2]=34dd6bcf  D[2]=867d2f59
A[3]=fb90fb08  B[3]=af1e7712  C[3]=81f354ea  D[3]=6aaaed48
A[4]=a77f8995  B[4]=a288e7e9  C[4]=edb827f2  D[4]=9f122b3f
A[5]=1a6f3e7c  B[5]=f85af245  C[5]=49e09ede  D[5]=e3f81fb2
A[6]=69e0da4d  B[6]=4263e255  C[6]=969b8a4e  D[6]=fdec5acc
A[7]=91bb4d0f  B[7]=7e83753b  C[7]=82bdc8fa  D[7]=b1fbea5a

Step  2: (r=14, s=27)
A[0]=1fded853  B[0]=083a00d8  C[0]=1d9dc1c2  D[0]=80b5c835
A[1]=9222b96d  B[1]=f702db94  C[1]=efc15ce8  D[1]=0357e353
A[2]=a87dacdd  B[2]=8240ed55  C[2]=fae464fb  D[2]=34dd6bcf
A[3]=63958e40  B[3]=3ec23ee4  C[3]=af1e7712  D[3]=81f354ea
A[4]=511de861  B[4]=e26569df  C[4]=a288e7e9  D[4]=edb827f2
A[5]=b28ec608  B[5]=cf9f069b  C[5]=f85af245  D[5]=49e09ede
A[6]=3f40949f  B[6]=36935a78  C[6]=4263e255  D[6]=969b8a4e
A[7]=afca5798  B[7]=d343e46e  C[7]=7e83753b  D[7]=82bdc8fa

Step  3: (r=27, s= 3)
A[0]=9334d4d9  B[0]=98fef6c2  C[0]=083a00d8  D[0]=1d9dc1c2
```

```
A[1]=4d213360  B[1]=6c9115cb  C[1]=f702db94  D[1]=efc15ce8
A[2]=ea27825c  B[2]=ed43ed66  C[2]=8240ed55  D[2]=fae464fb
A[3]=c8a4dd7e  B[3]=031cac72  C[3]=3ec23ee4  D[3]=af1e7712
A[4]=29c21a26  B[4]=0a88ef43  C[4]=e26569df  D[4]=a288e7e9
A[5]=67a05b3c  B[5]=45947630  C[5]=cf9f069b  D[5]=f85af245
A[6]=40494b17  B[6]=f9fa04a4  C[6]=36935a78  D[6]=4263e255
A[7]=e4a86912  B[7]=c57e52bc  C[7]=d343e46e  D[7]=7e83753b

Step  4: (r= 3, s=20)
A[0]=9df1e68f  B[0]=99a6a6cc  C[0]=98fef6c2  D[0]=083a00d8
A[1]=4ae7b4f0  B[1]=69099b02  C[1]=6c9115cb  D[1]=f702db94
A[2]=54a59b0a  B[2]=513c12e7  C[2]=ed43ed66  D[2]=8240ed55
A[3]=196449f7  B[3]=4526ebf6  C[3]=031cac72  D[3]=3ec23ee4
A[4]=6afd6c64  B[4]=4e10d131  C[4]=0a88ef43  D[4]=e26569df
A[5]=cf3faa12  B[5]=3d02d9e3  C[5]=45947630  D[5]=cf9f069b
A[6]=8798b48f  B[6]=024a58ba  C[6]=f9fa04a4  D[6]=36935a78
A[7]=eceff279  B[7]=25434897  C[7]=c57e52bc  D[7]=d343e46e

Step  5: (r=20, s=14)
A[0]=ae5a2fd2  B[0]=68f9df1e  C[0]=99a6a6cc  D[0]=98fef6c2
A[1]=7e7d00c0  B[1]=4f04ae7b  C[1]=69099b02  D[1]=6c9115cb
A[2]=4647e1f9  B[2]=b0a54a59  C[2]=513c12e7  D[2]=ed43ed66
A[3]=6440a9ae  B[3]=9f719644  C[3]=4526ebf6  D[3]=031cac72
A[4]=c948da4a  B[4]=c646afd6  C[4]=4e10d131  D[4]=0a88ef43
A[5]=f3be9e4d  B[5]=a12cf3fa  C[5]=3d02d9e3  D[5]=45947630
A[6]=7199e3ae  B[6]=48f8798b  C[6]=024a58ba  D[6]=f9fa04a4
A[7]=fe24df9f  B[7]=279eceff  C[7]=25434897  D[7]=c57e52bc

Step  6: (r=14, s=27)
A[0]=32319d42  B[0]=8bf4ab96  C[0]=68f9df1e  D[0]=99a6a6cc
A[1]=c7e57f24  B[1]=40301f9f  C[1]=4f04ae7b  D[1]=69099b02
A[2]=5b646c9d  B[2]=f87e5191  C[2]=b0a54a59  D[2]=513c12e7
A[3]=f2d36427  B[3]=2a6b9910  C[3]=9f719644  D[3]=4526ebf6
A[4]=61a588ae  B[4]=3692b252  C[4]=c646afd6  D[4]=4e10d131
A[5]=b8687c0a  B[5]=a7937cef  C[5]=a12cf3fa  D[5]=3d02d9e3
A[6]=79fb28b3  B[6]=78eb9c66  C[6]=48f8798b  D[6]=024a58ba
A[7]=cd3e75d3  B[7]=37e7ff89  C[7]=279eceff  D[7]=25434897

Step  7: (r=27, s= 3)
A[0]=5f9f5b59  B[0]=11918cea  C[0]=8bf4ab96  D[0]=68f9df1e
A[1]=782a2d0b  B[1]=263f2bf9  C[1]=40301f9f  D[1]=4f04ae7b
A[2]=ed016bc0  B[2]=eadb2364  C[2]=f87e5191  D[2]=b0a54a59
A[3]=ce5fc203  B[3]=3f969b21  C[3]=2a6b9910  D[3]=9f719644
A[4]=5abd27c2  B[4]=730d2c45  C[4]=3692b252  D[4]=c646afd6
A[5]=b8942a4d  B[5]=55c343e0  C[5]=a7937cef  D[5]=a12cf3fa
A[6]=82310ef9  B[6]=9bcfd945  C[6]=78eb9c66  D[6]=48f8798b
A[7]=0b96e1f2  B[7]=9e69f3ae  C[7]=37e7ff89  D[7]=279eceff

Step  8: (r=26, s= 4)
```

```
A[0]=cd994a2e  B[0]=657e7d6d  C[0]=11918cea  D[0]=8bf4ab96
A[1]=1c3b0b0e  B[1]=2de0a8b4  C[1]=263f2bf9  D[1]=40301f9f
A[2]=2c44eb23  B[2]=03b405af  C[2]=eadb2364  D[2]=f87e5191
A[3]=77c76bfa  B[3]=0f397f08  C[3]=3f969b21  D[3]=2a6b9910
A[4]=d65caf3e  B[4]=096af49f  C[4]=730d2c45  D[4]=3692b252
A[5]=80c43dbf  B[5]=36e250a9  C[5]=55c343e0  D[5]=a7937cef
A[6]=95bcabc7  B[6]=e608c43b  C[6]=9bcfd945  D[6]=78eb9c66
A[7]=5a04f5e3  B[7]=c82e5b87  C[7]=9e69f3ae  D[7]=37e7ff89

Step  9: (r= 4, s=23)
A[0]=dae5e2c1  B[0]=d994a2ec  C[0]=657e7d6d  D[0]=11918cea
A[1]=1438c146  B[1]=c3b0b0e1  C[1]=2de0a8b4  D[1]=263f2bf9
A[2]=d2503aac  B[2]=c44eb232  C[2]=03b405af  D[2]=eadb2364
A[3]=11353a83  B[3]=7c76bfa7  C[3]=0f397f08  D[3]=3f969b21
A[4]=41df8acd  B[4]=65caf3ed  C[4]=096af49f  D[4]=730d2c45
A[5]=17e58639  B[5]=0c43dbf8  C[5]=36e250a9  D[5]=55c343e0
A[6]=8932bd3c  B[6]=5bcabc79  C[6]=e608c43b  D[6]=9bcfd945
A[7]=6f5e3c2c  B[7]=a04f5e35  C[7]=c82e5b87  D[7]=9e69f3ae

Step 10: (r=23, s=11)
A[0]=f771bfa8  B[0]=60ed72f1  C[0]=d994a2ec  D[0]=657e7d6d
A[1]=4b6e5371  B[1]=a30a1c60  C[1]=c3b0b0e1  D[1]=2de0a8b4
A[2]=ffa591b7  B[2]=5669281d  C[2]=c44eb232  D[2]=03b405af
A[3]=37cd0aad  B[3]=41889a9d  C[3]=7c76bfa7  D[3]=0f397f08
A[4]=95069202  B[4]=66a0efc5  C[4]=65caf3ed  D[4]=096af49f
A[5]=e1df3df5  B[5]=1c8bf2c3  C[5]=0c43dbf8  D[5]=36e250a9
A[6]=f42682b4  B[6]=9e44995e  C[6]=5bcabc79  D[6]=e608c43b
A[7]=9b9f3dc9  B[7]=1637af1e  C[7]=a04f5e35  D[7]=c82e5b87

Step 11: (r=11, s=26)
A[0]=967a56ad  B[0]=8dfd47bb  C[0]=60ed72f1  D[0]=d994a2ec
A[1]=3bb4597e  B[1]=729b8a5b  C[1]=a30a1c60  D[1]=c3b0b0e1
A[2]=0abc1d9d  B[2]=2c8dbffd  C[2]=5669281d  D[2]=c44eb232
A[3]=f7a310d7  B[3]=685569be  C[3]=41889a9d  D[3]=7c76bfa7
A[4]=bea0988f  B[4]=349014a8  C[4]=66a0efc5  D[4]=65caf3ed
A[5]=46686ae3  B[5]=f9efaf0e  C[5]=1c8bf2c3  D[5]=0c43dbf8
A[6]=1f272d51  B[6]=3415a7a1  C[6]=9e44995e  D[6]=5bcabc79
A[7]=a8286168  B[7]=f9ee4cdc  C[7]=1637af1e  D[7]=a04f5e35

Step 12: (r=26, s= 4)
A[0]=859a895a  B[0]=b659e95a  C[0]=8dfd47bb  D[0]=60ed72f1
A[1]=df294bed  B[1]=f8eed165  C[1]=729b8a5b  D[1]=a30a1c60
A[2]=ffd904fb  B[2]=742af076  C[2]=2c8dbffd  D[2]=5669281d
A[3]=c5ab9e45  B[3]=5fde8c43  C[3]=685569be  D[3]=41889a9d
A[4]=d7e82bf2  B[4]=3efa8262  C[4]=349014a8  D[4]=66a0efc5
A[5]=b7a2af3a  B[5]=8d19a1ab  C[5]=f9efaf0e  D[5]=1c8bf2c3
A[6]=b1b37e7e  B[6]=447c9cb5  C[6]=3415a7a1  D[6]=9e44995e
A[7]=c0ca489a  B[7]=a2a0a185  C[7]=f9ee4cdc  D[7]=1637af1e
```

```
Step 13: (r= 4, s=23)
A[0]=c481887a  B[0]=59a895a8  C[0]=b659e95a  D[0]=8dfd47bb
A[1]=cd6556c1  B[1]=f294bedd  C[1]=f8eed165  D[1]=729b8a5b
A[2]=71a30aa6  B[2]=fd904fbf  C[2]=742af076  D[2]=2c8dbffd
A[3]=2cb17376  B[3]=5ab9e45c  C[3]=5fde8c43  D[3]=685569be
A[4]=d61584fa  B[4]=7e82bf2d  C[4]=3efa8262  D[4]=349014a8
A[5]=13193c57  B[5]=7a2af3ab  C[5]=8d19a1ab  D[5]=f9efaf0e
A[6]=d7e57b61  B[6]=1b37e7eb  C[6]=447c9cb5  D[6]=3415a7a1
A[7]=25a28b53  B[7]=0ca489ac  C[7]=a2a0a185  D[7]=f9ee4cdc

Step 14: (r=23, s=11)
A[0]=8fd15672  B[0]=3d6240c4  C[0]=59a895a8  D[0]=b659e95a
A[1]=b65f8e19  B[1]=60e6b2ab  C[1]=f294bedd  D[1]=f8eed165
A[2]=ec8106f9  B[2]=5338d185  C[2]=fd904fbf  D[2]=742af076
A[3]=e0da0e33  B[3]=bb1658b9  C[3]=5ab9e45c  D[3]=5fde8c43
A[4]=450aee46  B[4]=7d6b0ac2  C[4]=7e82bf2d  D[4]=3efa8262
A[5]=ebeb228f  B[5]=2b898c9e  C[5]=7a2af3ab  D[5]=8d19a1ab
A[6]=e0538dac  B[6]=b0ebf2bd  C[6]=1b37e7eb  D[6]=447c9cb5
A[7]=da582341  B[7]=a992d145  C[7]=0ca489ac  D[7]=a2a0a185

Step 15: (r=11, s=26)
A[0]=1f568a36  B[0]=8ab3947e  C[0]=3d6240c4  D[0]=59a895a8
A[1]=353fe4e8  B[1]=fc70cdb2  C[1]=60e6b2ab  D[1]=f294bedd
A[2]=52f8e4b8  B[2]=0837cf64  C[2]=5338d185  D[2]=fd904fbf
A[3]=3fa5056c  B[3]=d0719f06  C[3]=bb1658b9  D[3]=5ab9e45c
A[4]=19132177  B[4]=57723228  C[4]=7d6b0ac2  D[4]=7e82bf2d
A[5]=26f056f1  B[5]=59147f5f  C[5]=2b898c9e  D[5]=7a2af3ab
A[6]=20cd40c8  B[6]=9c6d6702  C[6]=b0ebf2bd  D[6]=1b37e7eb
A[7]=c18c3edd  B[7]=c11a0ed2  C[7]=a992d145  D[7]=0ca489ac

Step 16: (r=19, s=28)
A[0]=0ad0bf68  B[0]=51b0fab4  C[0]=8ab3947e  D[0]=3d6240c4
A[1]=1b897443  B[1]=2741a9ff  C[1]=fc70cdb2  D[1]=60e6b2ab
A[2]=05dc5c5b  B[2]=25c297c7  C[2]=0837cf64  D[2]=5338d185
A[3]=38411041  B[3]=2b61fd28  C[3]=d0719f06  D[3]=bb1658b9
A[4]=4d6d7577  B[4]=0bb8c899  C[4]=57723228  D[4]=7d6b0ac2
A[5]=5ecefb39  B[5]=b7893782  C[5]=59147f5f  D[5]=2b898c9e
A[6]=2d23bd55  B[6]=0641066a  C[6]=9c6d6702  D[6]=b0ebf2bd
A[7]=46c1b737  B[7]=f6ee0c61  C[7]=c11a0ed2  D[7]=a992d145

Step 17: (r=28, s= 7)
A[0]=122ca89e  B[0]=80ad0bf6  C[0]=51b0fab4  D[0]=8ab3947e
A[1]=da998cd6  B[1]=31b89744  C[1]=2741a9ff  D[1]=fc70cdb2
A[2]=411635b2  B[2]=b05dc5c5  C[2]=25c297c7  D[2]=0837cf64
A[3]=2032b928  B[3]=13841104  C[3]=2b61fd28  D[3]=d0719f06
A[4]=e5d9bce9  B[4]=74d6d757  C[4]=0bb8c899  D[4]=57723228
A[5]=28d9d067  B[5]=95ecefb3  C[5]=b7893782  D[5]=59147f5f
A[6]=51428f23  B[6]=52d23bd5  C[6]=0641066a  D[6]=9c6d6702
A[7]=c308df4a  B[7]=746c1b73  C[7]=f6ee0c61  D[7]=c11a0ed2
```

```
Step 18: (r= 7, s=22)
A[0]=9ca368af  B[0]=16544f09  C[0]=80ad0bf6  D[0]=51b0fab4
A[1]=160a1fb9  B[1]=4cc66b6d  C[1]=31b89744  D[1]=2741a9ff
A[2]=fd44ab24  B[2]=8b1ad920  C[2]=b05dc5c5  D[2]=25c297c7
A[3]=2c16e823  B[3]=195c9410  C[3]=13841104  D[3]=2b61fd28
A[4]=55e1fe3e  B[4]=ecde74f2  C[4]=74d6d757  D[4]=0bb8c899
A[5]=b46d472b  B[5]=6ce83394  C[5]=95ecefb3  D[5]=b7893782
A[6]=e0b59724  B[6]=a14791a8  C[6]=52d23bd5  D[6]=0641066a
A[7]=0d5e551f  B[7]=846fa561  C[7]=746c1b73  D[7]=f6ee0c61

Step 19: (r=22, s=19)
A[0]=ae5f3c0f  B[0]=2be728da  C[0]=16544f09  D[0]=80ad0bf6
A[1]=06cdb70a  B[1]=ee458287  C[1]=4cc66b6d  D[1]=31b89744
A[2]=3e05f7e9  B[2]=c93f512a  C[2]=8b1ad920  D[2]=b05dc5c5
A[3]=4cedf7d7  B[3]=08cb05ba  C[3]=195c9410  D[3]=13841104
A[4]=90ed900b  B[4]=8f95787f  C[4]=ecde74f2  D[4]=74d6d757
A[5]=d7e7c046  B[5]=caed1b51  C[5]=6ce83394  D[5]=95ecefb3
A[6]=51f00615  B[6]=c9382d65  C[6]=a14791a8  D[6]=52d23bd5
A[7]=e56e7c7d  B[7]=47c35795  C[7]=846fa561  D[7]=746c1b73

Step 20: (r=19, s=28)
A[0]=3ed796ee  B[0]=e07d72f9  C[0]=2be728da  D[0]=16544f09
A[1]=f5174fc2  B[1]=b850366d  C[1]=ee458287  D[1]=4cc66b6d
A[2]=c679ae17  B[2]=bf49f02f  C[2]=c93f512a  D[2]=8b1ad920
A[3]=3d4d5e06  B[3]=beba676f  C[3]=08cb05ba  D[3]=195c9410
A[4]=235adcc3  B[4]=805c876c  C[4]=8f95787f  D[4]=ecde74f2
A[5]=37892c9e  B[5]=0236bf3e  C[5]=caed1b51  D[5]=6ce83394
A[6]=01ef1d63  B[6]=30aa8f80  C[6]=c9382d65  D[6]=a14791a8
A[7]=e0e83864  B[7]=e3ef2b73  C[7]=47c35795  D[7]=846fa561

Step 21: (r=28, s= 7)
A[0]=d931c225  B[0]=e3ed796e  C[0]=e07d72f9  D[0]=2be728da
A[1]=85947873  B[1]=2f5174fc  C[1]=b850366d  D[1]=ee458287
A[2]=e9465eae  B[2]=7c679ae1  C[2]=bf49f02f  D[2]=c93f512a
A[3]=3b59a5ae  B[3]=63d4d5e0  C[3]=beba676f  D[3]=08cb05ba
A[4]=4f13ce29  B[4]=3235adcc  C[4]=805c876c  D[4]=8f95787f
A[5]=5d649b90  B[5]=e37892c9  C[5]=0236bf3e  D[5]=caed1b51
A[6]=afaaa7a7  B[6]=301ef1d6  C[6]=30aa8f80  D[6]=c9382d65
A[7]=130d9433  B[7]=4e0e8386  C[7]=e3ef2b73  D[7]=47c35795

Step 22: (r= 7, s=22)
A[0]=a87f4b1b  B[0]=98e112ec  C[0]=e3ed796e  D[0]=e07d72f9
A[1]=cf4ec26f  B[1]=ca3c39c2  C[1]=2f5174fc  D[1]=b850366d
A[2]=fdd9c3c9  B[2]=a32f5774  C[2]=7c679ae1  D[2]=bf49f02f
A[3]=36a513ad  B[3]=acd2d71d  C[3]=63d4d5e0  D[3]=beba676f
A[4]=879321fa  B[4]=89e714a7  C[4]=3235adcc  D[4]=805c876c
A[5]=d628eb76  B[5]=b24dc82e  C[5]=e37892c9  D[5]=0236bf3e
A[6]=53ada178  B[6]=d553d3d7  C[6]=301ef1d6  D[6]=30aa8f80
```

```
A[7]=454d5cae  B[7]=86ca1989  C[7]=4e0e8386  D[7]=e3ef2b73

Step 23: (r=22, s=19)
A[0]=9222c907  B[0]=c6ea1fd2  C[0]=98e112ec  D[0]=e3ed796e
A[1]=5fb16d0c  B[1]=9bf3d3b0  C[1]=ca3c39c2  D[1]=2f5174fc
A[2]=4a249633  B[2]=f27f7670  C[2]=a32f5774  D[2]=7c679ae1
A[3]=06bd8147  B[3]=eb4da944  C[3]=acd2d71d  D[3]=63d4d5e0
A[4]=bef561d8  B[4]=7ea1e4c8  C[4]=89e714a7  D[4]=3235adcc
A[5]=cd759f3c  B[5]=ddb58a3a  C[5]=b24dc82e  D[5]=e37892c9
A[6]=882d65a0  B[6]=5e14eb68  C[6]=d553d3d7  D[6]=301ef1d6
A[7]=84afcc3f  B[7]=2b915357  C[7]=86ca1989  D[7]=4e0e8386

Step 24: (r=15, s= 5)
A[0]=1e3c72cb  B[0]=6483c911  C[0]=c6ea1fd2  D[0]=98e112ec
A[1]=7509cdcf  B[1]=b6862fd8  C[1]=9bf3d3b0  D[1]=ca3c39c2
A[2]=1b1a6691  B[2]=4b19a512  C[2]=f27f7670  D[2]=a32f5774
A[3]=f332215e  B[3]=c0a3835e  C[3]=eb4da944  D[3]=acd2d71d
A[4]=991960e2  B[4]=b0ec5f7a  C[4]=7ea1e4c8  D[4]=89e714a7
A[5]=a31ea448  B[5]=cf9e66ba  C[5]=ddb58a3a  D[5]=b24dc82e
A[6]=e086708f  B[6]=b2d04416  C[6]=5e14eb68  D[6]=d553d3d7
A[7]=f01460e4  B[7]=e61fc257  C[7]=2b915357  D[7]=86ca1989

Step 25: (r= 5, s=29)
A[0]=825fc764  B[0]=c78e5963  C[0]=6483c911  D[0]=c6ea1fd2
A[1]=edb92c69  B[1]=a139b9ee  C[1]=b6862fd8  D[1]=9bf3d3b0
A[2]=255e46bc  B[2]=634cd223  C[2]=4b19a512  D[2]=f27f7670
A[3]=52ee8862  B[3]=66442bde  C[3]=c0a3835e  D[3]=eb4da944
A[4]=f66c23c0  B[4]=232c1c53  C[4]=b0ec5f7a  D[4]=7ea1e4c8
A[5]=08b7b394  B[5]=63d48914  C[5]=cf9e66ba  D[5]=ddb58a3a
A[6]=fa8f17f5  B[6]=10ce11fc  C[6]=b2d04416  D[6]=5e14eb68
A[7]=91417d8c  B[7]=028c1c9e  C[7]=e61fc257  D[7]=2b915357

Step 26: (r=29, s= 9)
A[0]=949ca2fe  B[0]=904bf8ec  C[0]=c78e5963  D[0]=6483c911
A[1]=029a462b  B[1]=3db7258d  C[1]=a139b9ee  D[1]=b6862fd8
A[2]=2618807d  B[2]=84abc8d7  C[2]=634cd223  D[2]=4b19a512
A[3]=055ec20a  B[3]=4a5dd10c  C[3]=66442bde  D[3]=c0a3835e
A[4]=15ac2bee  B[4]=1ecd8478  C[4]=232c1c53  D[4]=b0ec5f7a
A[5]=5693cc6a  B[5]=8116f672  C[5]=63d48914  D[5]=cf9e66ba
A[6]=e4b808a2  B[6]=bf51e2fe  C[6]=10ce11fc  D[6]=b2d04416
A[7]=34015c0d  B[7]=92282fb1  C[7]=028c1c9e  D[7]=e61fc257

Step 27: (r= 9, s=15)
A[0]=1c39472a  B[0]=3945fd29  C[0]=904bf8ec  D[0]=c78e5963
A[1]=70b04e44  B[1]=348c5605  C[1]=3db7258d  D[1]=a139b9ee
A[2]=af421336  B[2]=3100fa4c  C[2]=84abc8d7  D[2]=634cd223
A[3]=18aa9e68  B[3]=bd84140a  C[3]=4a5dd10c  D[3]=66442bde
A[4]=5d7882c1  B[4]=5857dc2b  C[4]=1ecd8478  D[4]=232c1c53
A[5]=98fd7df9  B[5]=2798d4ad  C[5]=8116f672  D[5]=63d48914
```

```
A[6]=a44b0cc5  B[6]=701145c9  C[6]=bf51e2fe  D[6]=10ce11fc
A[7]=b20a2468  B[7]=02b81a68  C[7]=92282fb1  D[7]=028c1c9e

Step 28: (r=15, s= 5)
A[0]=c8ce207f  B[0]=a3950e1c  C[0]=3945fd29  D[0]=904bf8ec
A[1]=a59597fa  B[1]=27223858  C[1]=348c5605  D[1]=3db7258d
A[2]=1cf2c10b  B[2]=099b57a1  C[2]=3100fa4c  D[2]=84abc8d7
A[3]=981ce969  B[3]=4f340c55  C[3]=bd84140a  D[3]=4a5dd10c
A[4]=b8331186  B[4]=4160aebc  C[4]=5857dc2b  D[4]=1ecd8478
A[5]=03716b3f  B[5]=befccc7e  C[5]=2798d4ad  D[5]=8116f672
A[6]=53defa75  B[6]=8662d225  C[6]=701145c9  D[6]=bf51e2fe
A[7]=6895587e  B[7]=12345905  C[7]=02b81a68  D[7]=92282fb1

Step 29: (r= 5, s=29)
A[0]=e4f3242e  B[0]=19c40ff9  C[0]=a3950e1c  D[0]=3945fd29
A[1]=c558dfe6  B[1]=b2b2ff54  C[1]=27223858  D[1]=348c5605
A[2]=32aa0b4c  B[2]=9e582163  C[2]=099b57a1  D[2]=3100fa4c
A[3]=c2ac2e79  B[3]=039d2d33  C[3]=4f340c55  D[3]=bd84140a
A[4]=6f3e5fc3  B[4]=066230d7  C[4]=4160aebc  D[4]=5857dc2b
A[5]=aa166d09  B[5]=6e2d67e0  C[5]=befccc7e  D[5]=2798d4ad
A[6]=c6a10aab  B[6]=7bdf4eaa  C[6]=8662d225  D[6]=701145c9
A[7]=df96775d  B[7]=12ab0fcd  C[7]=12345905  D[7]=02b81a68

Step 30: (r=29, s= 9)
A[0]=2d609ca6  B[0]=dc9e6485  C[0]=19c40ff9  D[0]=a3950e1c
A[1]=dde91aeb  B[1]=d8ab1bfc  C[1]=b2b2ff54  D[1]=27223858
A[2]=a33572b0  B[2]=86554169  C[2]=9e582163  D[2]=099b57a1
A[3]=30881df8  B[3]=385585cf  C[3]=039d2d33  D[3]=4f340c55
A[4]=a8b8d781  B[4]=6de7cbf8  C[4]=066230d7  D[4]=4160aebc
A[5]=fcfa85b1  B[5]=3542cda1  C[5]=6e2d67e0  D[5]=befccc7e
A[6]=b3eb61ce  B[6]=78d42155  C[6]=7bdf4eaa  D[6]=8662d225
A[7]=ac56acf3  B[7]=bbf2ceeb  C[7]=12ab0fcd  D[7]=12345905

Step 31: (r= 9, s=15)
A[0]=aa9d8c7f  B[0]=c1394c5a  C[0]=dc9e6485  D[0]=19c40ff9
A[1]=1de763e0  B[1]=d235d7bb  C[1]=d8ab1bfc  D[1]=b2b2ff54
A[2]=40c5311b  B[2]=6ae56146  C[2]=86554169  D[2]=9e582163
A[3]=c416f1ae  B[3]=103bf061  C[3]=385585cf  D[3]=039d2d33
A[4]=dd0b029d  B[4]=71af0351  C[4]=6de7cbf8  D[4]=066230d7
A[5]=34f7fcd6  B[5]=f50b63f9  C[5]=3542cda1  D[5]=6e2d67e0
A[6]=96bac845  B[6]=d6c39d67  C[6]=78d42155  D[6]=7bdf4eaa
A[7]=e15bf492  B[7]=ad59e758  C[7]=bbf2ceeb  D[7]=12ab0fcd

Feed-Forward Step 0: (r=15, s= 5)
A[0]=d076aa27  B[0]=c63fd54e  C[0]=c1394c5a  D[0]=dc9e6485
A[1]=0fea652b  B[1]=b1f00ef3  C[1]=d235d7bb  D[1]=d8ab1bfc
A[2]=d0bc48d5  B[2]=988da062  C[2]=6ae56146  D[2]=86554169
A[3]=fcbec515  B[3]=78d7620b  C[3]=103bf061  D[3]=385585cf
A[4]=dd4d6153  B[4]=814eee85  C[4]=71af0351  D[4]=6de7cbf8
```

```
A[5]=aca90295  B[5]=fe6b1a7b  C[5]=f50b63f9  D[5]=3542cda1
A[6]=88357ab5  B[6]=6422cb5d  C[6]=d6c39d67  D[6]=78d42155
A[7]=21f71480  B[7]=fa4970ad  C[7]=ad59e758  D[7]=bbf2ceeb

Feed-Forward Step 1: (r= 5, s=29)
A[0]=ea33fb01  B[0]=0ed544fa  C[0]=c63fd54e  D[0]=c1394c5a
A[1]=baf87d50  B[1]=fd4ca561  C[1]=b1f00ef3  D[1]=d235d7bb
A[2]=aca4721d  B[2]=17891aba  C[2]=988da062  D[2]=6ae56146
A[3]=9c1adc33  B[3]=97d8a2bf  C[3]=78d7620b  D[3]=103bf061
A[4]=1e2e1fb2  B[4]=a9ac2a7b  C[4]=814eee85  D[4]=71af0351
A[5]=3fca1b78  B[5]=952052b5  C[5]=fe6b1a7b  D[5]=f50b63f9
A[6]=bc7dd50f  B[6]=06af56b1  C[6]=6422cb5d  D[6]=d6c39d67
A[7]=d400a5fa  B[7]=3ee29004  C[7]=fa4970ad  D[7]=ad59e758

Feed-Forward Step 2: (r=29, s= 9)
A[0]=8a01da87  B[0]=3d467f60  C[0]=0ed544fa  D[0]=c63fd54e
A[1]=64b0a123  B[1]=175f0faa  C[1]=fd4ca561  D[1]=b1f00ef3
A[2]=b21ded73  B[2]=b5948e43  C[2]=17891aba  D[2]=988da062
A[3]=5fd8032a  B[3]=73835b86  C[3]=97d8a2bf  D[3]=78d7620b
A[4]=24983a59  B[4]=43c5c3f6  C[4]=a9ac2a7b  D[4]=814eee85
A[5]=6d3739ca  B[5]=07f9436f  C[5]=952052b5  D[5]=fe6b1a7b
A[6]=2c45afc8  B[6]=f78fbaa1  C[6]=06af56b1  D[6]=6422cb5d
A[7]=223d1724  B[7]=5a8014bf  C[7]=3ee29004  D[7]=fa4970ad

Feed-Forward Step 3: (r= 9, s=15)
A[0]=afa7045a  B[0]=03b50f14  C[0]=3d467f60  D[0]=0ed544fa
A[1]=865f319e  B[1]=614246c9  C[1]=175f0faa  D[1]=fd4ca561
A[2]=8c82df9a  B[2]=3bdae764  C[2]=b5948e43  D[2]=17891aba
A[3]=ccad7485  B[3]=b00654bf  C[3]=73835b86  D[3]=97d8a2bf
A[4]=c837930b  B[4]=3074b249  C[4]=43c5c3f6  D[4]=a9ac2a7b
A[5]=4a226df0  B[5]=6e7394da  C[5]=07f9436f  D[5]=952052b5
A[6]=8ac6b81a  B[6]=8b5f9058  C[6]=f78fbaa1  D[6]=06af56b1
A[7]=1dc66556  B[7]=7a2e4844  C[7]=5a8014bf  D[7]=3ee29004
```

Compression Function Output

```
A[0]=afa7045a  B[0]=03b50f14  C[0]=3d467f60  D[0]=0ed544fa
A[1]=865f319e  B[1]=614246c9  C[1]=175f0faa  D[1]=fd4ca561
A[2]=8c82df9a  B[2]=3bdae764  C[2]=b5948e43  D[2]=17891aba
A[3]=ccad7485  B[3]=b00654bf  C[3]=73835b86  D[3]=97d8a2bf
A[4]=c837930b  B[4]=3074b249  C[4]=43c5c3f6  D[4]=a9ac2a7b
A[5]=4a226df0  B[5]=6e7394da  C[5]=07f9436f  D[5]=952052b5
A[6]=8ac6b81a  B[6]=8b5f9058  C[6]=f78fbaa1  D[6]=06af56b1
A[7]=1dc66556  B[7]=7a2e4844  C[7]=5a8014bf  D[7]=3ee29004
```

Final block

```
M[  0.. 7] = 00 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
```

```
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =    6  110  198  227   45   48  240  162
y[  8.. 15] =   28  167  162   26  100  136  175   13
y[ 16.. 23] =  105   29   76  156   65  201   12  201
y[ 24.. 31] =   15   98    1   79  129  256  249   61
y[ 32.. 39] =  205   87   89  188  218  234  222   16
y[ 40.. 47] =    8   18  139  161  188  152  117  155
y[ 48.. 55] =  128  188  255   28   91  244   83  200
y[ 56.. 63] =   53   68  175   17  160   80  211  216
y[ 64.. 71] =   64  142   32   39  250  230  185  240
y[ 72.. 79] =    2  135    4   52   93  171   62   66
y[ 80.. 87] =  122  169  162   57   34  120   35  241
y[ 88.. 95] =   17  171    7   54  154  138   45  134
y[ 96..103] =  188   88  126  118  158  140    4  182
y[104..111] =  145  232   35  172  254  196   31    3
y[112..119] =  245   43   90   31   48   46   68   79
y[120..127] =  214   32   35   98  155  162   14   33
y[128..135] =  251  147   59   30  212  209   17   95
y[136..143] =  229   90   95  231  157  121   82  244
y[144..151] =  152  228  181  101  192   56  245   56
y[152..159] =  242  159  256  178  128    1    8  196
y[160..167] =   52  170  168   69   39   23   35  241
y[168..175] =  249  239  118   96   69  105  140  102
y[176..183] =  129   69    2  229  166   13  174   57
y[184..191] =  204  189   82  240   97  177   46   41
y[192..199] =  193  115  225  218    7   27   72   17
y[200..207] =  255  122  253  205  164   86  195  191
y[208..215] =  135   88   95  200  223  137  222   16
y[216..223] =  240   86  250  203  103  119  212  123
y[224..231] =   69  169  131  139   99  117  253   75
y[232..239] =  112   25  222   85    3   61  226  254
y[240..247] =   12  214  167  226  209  211  189  178
y[248..255] =   43  225  222  159  102   95  243  224
```

Intermediate Expanded Message

```
Z[ 0] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
Z[ 1] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
Z[ 2] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
Z[ 3] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
Z[ 4] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
Z[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
Z[ 6] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
Z[ 7] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
Z[ 8] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
Z[ 9] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
Z[10] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
Z[11] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
Z[12] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
Z[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
Z[14] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
Z[15] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
Z[16] = fac6053a  3365cc9b  d8cd2733  0ecff131
        e79c1864  52c1ad3f  a8e4571c  476eb892
Z[17] = a4895b77  bdcc4234  c761389f  f58c0a74
        f2ef0d11  ff2100df  6f809080  06f8f908
Z[18] = 2d4cd2b4  b2794d87  21f9de07  1e7de183
        f90806f8  66ca9936  3c1bc3e5  9a1565eb
Z[19] = 90806f80  01befe42  b0bb4f45  b7b3484d
        d1d52e2b  476eb892  547fab81  2812d7ee
Z[20] = c84037c0  e4201be0  0619f9e7  3eb8c148
        fe4201be  fc84037c  aefd5103  c9fe3602
Z[21] = 95ba6a46  52c1ad3f  e2621d9e  e1831e7d
        f1310ecf  f9e70619  59b9a647  d8cd2733
Z[22] = 3c1bc3e5  923e6dc2  563da9c3  fc84037c
        61909e70  e1831e7d  029dfd63  e4ff1b01
Z[23] = 0a74f58c  b19a4e66  d63029d0  c4c43b3c
        2575da8b  e1831e7d  58daa726  f3ce0c32
```

```
Z[24] = a02e5fd2  1a22e5de  d63029d0  52c1ad3f
        4e66b19a  e95a16a6  69679699  f4ad0b53
Z[25] = e6bd1943  57fba805  30c8cf38  30c8cf38
        aaa2555e  bb2f44d1  00dfff21  cadd3523
Z[26] = b4374bc9  3c1bc3e5  1409ebf7  f2100df0
        f0520fae  53a0ac60  5b77a489  58daa726
Z[27] = 3c1bc3e5  e79c1864  0b53f4ad  31a7ce59
        c4c43b3c  f1310ecf  ba5045b0  23b7dc49
Z[28] = 642d9bd3  de0721f9  1785e87b  0ecff131
        6a4695ba  d2b42d4c  4aeab516  c682397e
Z[29] = 4ca8b358  ce5931a7  97786888  0df0f210
        4aeab516  d0f62f0a  67a99857  6b2594db
Z[30] = b3584ca8  993666ca  65eb9a15  4155beab
        15c7ea39  4a0bb5f5  3523cadd  fd63029d
Z[31] = da8b2575  e4ff1b01  d7ee2812  bb2f44d1
        e4201be0  aaa2555e  52c1ad3f  e3411cbf
```

Expanded Message

```
W[ 0] = ace52e40  1c2f1720  ec7dfaf1  f3b7cbf8
        a7d60172  259402e4  c1da4335  2fb22cce
W[ 1] = 3f98ce23  55465b0e  ab73b875  c9cd02e4
        edefaf10  c293194b  d3ebfdd5  022b1667
W[ 2] = 4f7e0456  ea52d55d  22b02085  bb59f3b7
        bef6143c  12cabb59  a88f4844  0965c4be
W[ 3] = 3edfda6c  ce234051  ef61e3d1  0b90e6b5
        0d0205c8  baa0aaba  b41fce23  b64a548d
W[ 4] = 1f13f754  1667410a  213e22b0  39173124
        1720e0ed  46d2194b  bb59b64a  17d90a1e
W[ 5] = c068582a  2931bb59  56b81892  f470194b
        c1da0c49  2706050f  aa01b591  a71d2085
W[ 6] = ce235c80  143cfe8e  f69b41c3  d6cf3bfb
        3124264d  0c49c4be  39d0b9e7  e25fdec2
W[ 7] = 14f54be1  b70336ec  d7882ef9  d78808ac
        46d20ad7  391700b9  ff47a380  2c15fa38
W[ 8] = e0ed08ac  e999bef6  dec2dd50  c6e9cedc
        e8e01f13  b92ee6b5  44a749b6  e827f5e2
W[ 9] = 31dda380  ebc40172  0965be3d  2931c405
        cedcd9b3  f3b73b42  c6304619  1da1213e
W[10] = 531bd1c0  e3d1e8e0  1383050f  0c493408
        582afe8e  da6cfd1c  3e26bccb  d04ed332
W[11] = b082fbaa  15ae2aa3  dd50df7b  44a70c49
        410aebc4  ed3644a7  5771b7bc  f69b3b42
W[12] = eb0bb41f  48fdc914  2878d107  2878f754
        b92ef529  c6e9ff47  00b95c80  d3eb05c8
W[13] = 3f98a7d6  d6cf44a7  a948e76e  0b90e6b5
        3e26f3b7  d8fafaf1  55ff4a6f  58e3df7b
W[14] = c1212594  31ddbfaf  109f1c2f  f470194b
        f2fefa38  45605546  4be131dd  49b6ab73
```

```
W[15] = c06831dd  aabaa4f2  548d478b  3633fd1c
        121150f0  3d6de6b5  2c15022b  fdd5e999
W[16] = a4895b77  bdcc4234  c761389f  f58c0a74
        f2ef0d11  ff2100df  6f809080  06f8f908
W[17] = 2d4cd2b4  b2794d87  21f9de07  1e7de183
        f90806f8  66ca9936  3c1bc3e5  9a1565eb
W[18] = 0a74f58c  b19a4e66  d63029d0  c4c43b3c
        2575da8b  e1831e7d  58daa726  f3ce0c32
W[19] = c84037c0  e4201be0  0619f9e7  3eb8c148
        fe4201be  fc84037c  aefd5103  c9fe3602
W[20] = 3c1bc3e5  923e6dc2  563da9c3  fc84037c
        61909e70  e1831e7d  029dfd63  e4ff1b01
W[21] = 95ba6a46  52c1ad3f  e2621d9e  e1831e7d
        f1310ecf  f9e70619  59b9a647  d8cd2733
W[22] = fac6053a  3365cc9b  d8cd2733  0ecff131
        e79c1864  52c1ad3f  a8e4571c  476eb892
W[23] = 90806f80  01befe42  b0bb4f45  b7b3484d
        d1d52e2b  476eb892  547fab81  2812d7ee
W[24] = b3584ca8  993666ca  65eb9a15  4155beab
        15c7ea39  4a0bb5f5  3523cadd  fd63029d
W[25] = a02e5fd2  1a22e5de  d63029d0  52c1ad3f
        4e66b19a  e95a16a6  69679699  f4ad0b53
W[26] = e6bd1943  57fba805  30c8cf38  30c8cf38
        aaa2555e  bb2f44d1  00dfff21  cadd3523
W[27] = da8b2575  e4ff1b01  d7ee2812  bb2f44d1
        e4201be0  aaa2555e  52c1ad3f  e3411cbf
W[28] = 3c1bc3e5  e79c1864  0b53f4ad  31a7ce59
        c4c43b3c  f1310ecf  ba5045b0  23b7dc49
W[29] = 4ca8b358  ce5931a7  97786888  0df0f210
        4aeab516  d0f62f0a  67a99857  6b2594db
W[30] = 642d9bd3  de0721f9  1785e87b  0ecff131
        6a4695ba  d2b42d4c  4aeab516  c682397e
W[31] = b4374bc9  3c1bc3e5  1409ebf7  f2100df0
        f0520fae  53a0ac60  5b77a489  58daa726
```

Feistel Steps

```
IV :
A[0]=afa7045a  B[0]=03b50f14  C[0]=3d467f60  D[0]=0ed544fa
A[1]=865f319e  B[1]=614246c9  C[1]=175f0faa  D[1]=fd4ca561
A[2]=8c82df9a  B[2]=3bdae764  C[2]=b5948e43  D[2]=17891aba
A[3]=ccad7485  B[3]=b00654bf  C[3]=73835b86  D[3]=97d8a2bf
A[4]=c837930b  B[4]=3074b249  C[4]=43c5c3f6  D[4]=a9ac2a7b
A[5]=4a226df0  B[5]=6e7394da  C[5]=07f9436f  D[5]=952052b5
A[6]=8ac6b81a  B[6]=8b5f9058  C[6]=f78fbaa1  D[6]=06af56b1
A[7]=1dc66556  B[7]=7a2e4844  C[7]=5a8014bf  D[7]=3ee29004

IV XOR M :
A[0]=afa7005a  B[0]=03b50f14  C[0]=3d467f60  D[0]=0ed544fa
```

```
A[1]=865f319e  B[1]=614246c9  C[1]=175f0faa  D[1]=fd4ca561
A[2]=8c82df9a  B[2]=3bdae764  C[2]=b5948e43  D[2]=17891aba
A[3]=ccad7485  B[3]=b00654bf  C[3]=73835b86  D[3]=97d8a2bf
A[4]=c837930b  B[4]=3074b249  C[4]=43c5c3f6  D[4]=a9ac2a7b
A[5]=4a226df0  B[5]=6e7394da  C[5]=07f9436f  D[5]=952052b5
A[6]=8ac6b81a  B[6]=8b5f9058  C[6]=f78fbaa1  D[6]=06af56b1
A[7]=1dc66556  B[7]=7a2e4844  C[7]=5a8014bf  D[7]=3ee29004

Step  0: (r= 3, s=20)
A[0]=59a686f3  B[0]=7d3802d5  C[0]=03b50f14  D[0]=3d467f60
A[1]=2fcaaeb1  B[1]=32f98cf4  C[1]=614246c9  D[1]=175f0faa
A[2]=342f7e0b  B[2]=6416fcd4  C[2]=3bdae764  D[2]=b5948e43
A[3]=47fae640  B[3]=656ba42e  C[3]=b00654bf  D[3]=73835b86
A[4]=3fb8c6f1  B[4]=41bc985e  C[4]=3074b249  D[4]=43c5c3f6
A[5]=093d4353  B[5]=51136f82  C[5]=6e7394da  D[5]=07f9436f
A[6]=b82fa842  B[6]=5635c0d4  C[6]=8b5f9058  D[6]=f78fbaa1
A[7]=32324a84  B[7]=ee332ab0  C[7]=7a2e4844  D[7]=5a8014bf

Step  1: (r=20, s=14)
A[0]=f70978fb  B[0]=6f359a68  C[0]=7d3802d5  D[0]=03b50f14
A[1]=f1f0b389  B[1]=eb12fcaa  C[1]=32f98cf4  D[1]=614246c9
A[2]=403cbe9f  B[2]=e0b342f7  C[2]=6416fcd4  D[2]=3bdae764
A[3]=afdd4959  B[3]=64047fae  C[3]=656ba42e  D[3]=b00654bf
A[4]=0d030fe6  B[4]=6f13fb8c  C[4]=41bc985e  D[4]=3074b249
A[5]=b5542f9c  B[5]=353093d4  C[5]=51136f82  D[5]=6e7394da
A[6]=c147b348  B[6]=842b82fa  C[6]=5635c0d4  D[6]=8b5f9058
A[7]=82aa458e  B[7]=a8432324  C[7]=ee332ab0  D[7]=7a2e4844

Step  2: (r=14, s=27)
A[0]=4776c218  B[0]=5e3efdc2  C[0]=6f359a68  D[0]=7d3802d5
A[1]=fe47a71a  B[1]=2ce27c7c  C[1]=eb12fcaa  D[1]=32f98cf4
A[2]=11fd17ab  B[2]=2fa7d00f  C[2]=e0b342f7  D[2]=6416fcd4
A[3]=ea75bced  B[3]=52566bf7  C[3]=64047fae  D[3]=656ba42e
A[4]=5c3fbf08  B[4]=c3f98340  C[4]=6f13fb8c  D[4]=41bc985e
A[5]=7f5a5cad  B[5]=0be72d55  C[5]=353093d4  D[5]=51136f82
A[6]=f3339157  B[6]=ecd23051  C[6]=842b82fa  D[6]=5635c0d4
A[7]=11bc3783  B[7]=9163a0aa  C[7]=a8432324  D[7]=ee332ab0

Step  3: (r=27, s= 3)
A[0]=955fab01  B[0]=c23bb610  C[0]=5e3efdc2  D[0]=6f359a68
A[1]=df7522ce  B[1]=d7f23d38  C[1]=2ce27c7c  D[1]=eb12fcaa
A[2]=689b24ab  B[2]=588fe8bd  C[2]=2fa7d00f  D[2]=e0b342f7
A[3]=d3159811  B[3]=6f53ade7  C[3]=52566bf7  D[3]=64047fae
A[4]=51fec365  B[4]=42e1fdf8  C[4]=c3f98340  D[4]=6f13fb8c
A[5]=90a789c0  B[5]=6bfad2e5  C[5]=0be72d55  D[5]=353093d4
A[6]=cc0cf844  B[6]=bf999c8a  C[6]=ecd23051  D[6]=842b82fa
A[7]=5e58ad01  B[7]=188de1bc  C[7]=9163a0aa  D[7]=a8432324

Step  4: (r= 3, s=20)
```

```
A[0]=076f5f0b  B[0]=aafd580c  C[0]=c23bb610  D[0]=5e3efdc2
A[1]=4e0b6ed3  B[1]=fba91676  C[1]=d7f23d38  D[1]=2ce27c7c
A[2]=fe1368a2  B[2]=44d9255b  C[2]=588fe8bd  D[2]=2fa7d00f
A[3]=f1782c90  B[3]=98acc08e  C[3]=6f53ade7  D[3]=52566bf7
A[4]=82d8f0ed  B[4]=8ff61b2a  C[4]=42e1fdf8  D[4]=c3f98340
A[5]=fe3e99cd  B[5]=853c4e04  C[5]=6bfad2e5  D[5]=0be72d55
A[6]=0b0829e9  B[6]=6067c226  C[6]=bf999c8a  D[6]=ecd23051
A[7]=4f154882  B[7]=f2c5680a  C[7]=188de1bc  D[7]=9163a0aa

Step  5: (r=20, s=14)
A[0]=372d097f  B[0]=f0b076f5  C[0]=aafd580c  D[0]=c23bb610
A[1]=a6a0e4f1  B[1]=ed34e0b6  C[1]=fba91676  D[1]=d7f23d38
A[2]=c507afb3  B[2]=8a2fe136  C[2]=44d9255b  D[2]=588fe8bd
A[3]=b9a6f0c5  B[3]=c90f1782  C[3]=98acc08e  D[3]=6f53ade7
A[4]=c0ecf2b3  B[4]=0ed82d8f  C[4]=8ff61b2a  D[4]=42e1fdf8
A[5]=8b6f39df  B[5]=9cdfe3e9  C[5]=853c4e04  D[5]=6bfad2e5
A[6]=6a7b5e06  B[6]=9e90b082  C[6]=6067c226  D[6]=bf999c8a
A[7]=274e48aa  B[7]=8824f154  C[7]=f2c5680a  D[7]=188de1bc

Step  6: (r=14, s=27)
A[0]=fc436d2b  B[0]=425fcdcb  C[0]=f0b076f5  D[0]=aafd580c
A[1]=be601ba3  B[1]=393c69a8  C[1]=ed34e0b6  D[1]=fba91676
A[2]=6711b958  B[2]=ebecf141  C[2]=8a2fe136  D[2]=44d9255b
A[3]=83ab7e0e  B[3]=bc316e69  C[3]=c90f1782  D[3]=98acc08e
A[4]=3c498168  B[4]=3cacf03b  C[4]=0ed82d8f  D[4]=8ff61b2a
A[5]=6c1b115c  B[5]=ce77e2db  C[5]=9cdfe3e9  D[5]=853c4e04
A[6]=f45b5aeb  B[6]=d7819a9e  C[6]=9e90b082  D[6]=6067c226
A[7]=87495f0f  B[7]=922a89d3  C[7]=8824f154  D[7]=f2c5680a

Step  7: (r=27, s= 3)
A[0]=c412dad0  B[0]=5fe21b69  C[0]=425fcdcb  D[0]=f0b076f5
A[1]=626690ad  B[1]=1df300dd  C[1]=393c69a8  D[1]=ed34e0b6
A[2]=9c1d07f7  B[2]=c3388dca  C[2]=ebecf141  D[2]=8a2fe136
A[3]=473c851f  B[3]=741d5bf0  C[3]=bc316e69  D[3]=c90f1782
A[4]=fc6854c9  B[4]=41e24c0b  C[4]=3cacf03b  D[4]=0ed82d8f
A[5]=738c9591  B[5]=e360d88a  C[5]=ce77e2db  D[5]=9cdfe3e9
A[6]=75408f4b  B[6]=5fa2dad7  C[6]=d7819a9e  D[6]=9e90b082
A[7]=7c3f38bd  B[7]=7c3a4af8  C[7]=922a89d3  D[7]=8824f154

Step  8: (r=26, s= 4)
A[0]=34538903  B[0]=43104b6b  C[0]=5fe21b69  D[0]=425fcdcb
A[1]=47a0df0a  B[1]=b5899a42  C[1]=1df300dd  D[1]=393c69a8
A[2]=4bd83698  B[2]=de70741f  C[2]=c3388dca  D[2]=ebecf141
A[3]=9fd59107  B[3]=7d1cf214  C[3]=741d5bf0  D[3]=bc316e69
A[4]=cfa14029  B[4]=27f1a153  C[4]=41e24c0b  D[4]=3cacf03b
A[5]=801d77d7  B[5]=45ce3256  C[5]=e360d88a  D[5]=ce77e2db
A[6]=a18a4ddd  B[6]=2dd5023d  C[6]=5fa2dad7  D[6]=d7819a9e
A[7]=164c1543  B[7]=f5f0fce2  C[7]=7c3a4af8  D[7]=922a89d3
```

```
Step  9: (r= 4, s=23)
A[0]=18e3604a  B[0]=45389033  C[0]=43104b6b  D[0]=5fe21b69
A[1]=f5fa7a7b  B[1]=7a0df0a4  C[1]=b5899a42  D[1]=1df300dd
A[2]=b19871e9  B[2]=bd836984  C[2]=de70741f  D[2]=c3388dca
A[3]=2b3f30aa  B[3]=fd591079  C[3]=7d1cf214  D[3]=741d5bf0
A[4]=112e9444  B[4]=fa14029c  C[4]=27f1a153  D[4]=41e24c0b
A[5]=a254221d  B[5]=01d77d78  C[5]=45ce3256  D[5]=e360d88a
A[6]=6522abd5  B[6]=18a4ddda  C[6]=2dd5023d  D[6]=5fa2dad7
A[7]=076d9c7d  B[7]=64c15431  C[7]=f5f0fce2  D[7]=7c3a4af8

Step 10: (r=23, s=11)
A[0]=ae461e7f  B[0]=250c71b0  C[0]=45389033  D[0]=43104b6b
A[1]=61817ce3  B[1]=3dfafd3d  C[1]=7a0df0a4  D[1]=b5899a42
A[2]=ee94a8c5  B[2]=f4d8cc38  C[2]=bd836984  D[2]=de70741f
A[3]=251a3f36  B[3]=55159f98  C[3]=fd591079  D[3]=7d1cf214
A[4]=6873261f  B[4]=2208974a  C[4]=fa14029c  D[4]=27f1a153
A[5]=5508cc55  B[5]=0ed12a11  C[5]=01d77d78  D[5]=45ce3256
A[6]=3707d272  B[6]=eab29155  C[6]=18a4ddda  D[6]=2dd5023d
A[7]=f9a35bba  B[7]=3e83b6ce  C[7]=64c15431  D[7]=f5f0fce2

Step 11: (r=11, s=26)
A[0]=ae943aa0  B[0]=30f3fd72  C[0]=250c71b0  D[0]=45389033
A[1]=6e7dbdac  B[1]=0be71b0c  C[1]=3dfafd3d  D[1]=7a0df0a4
A[2]=a958e62a  B[2]=a5462f74  C[2]=f4d8cc38  D[2]=bd836984
A[3]=f55a2c43  B[3]=d1f9b128  C[3]=55159f98  D[3]=fd591079
A[4]=b55fffc0  B[4]=9930fb43  C[4]=2208974a  D[4]=fa14029c
A[5]=e4c689cc  B[5]=4662aaa8  C[5]=0ed12a11  D[5]=01d77d78
A[6]=ec05d4d3  B[6]=3e9391b8  C[6]=eab29155  D[6]=18a4ddda
A[7]=8e9eee62  B[7]=1addd7cd  C[7]=3e83b6ce  D[7]=64c15431

Step 12: (r=26, s= 4)
A[0]=ff45d71b  B[0]=82ba50ea  C[0]=30f3fd72  D[0]=250c71b0
A[1]=b371bf39  B[1]=b1b9f6f6  C[1]=0be71b0c  D[1]=3dfafd3d
A[2]=c527f4e9  B[2]=aaa56398  C[2]=a5462f74  D[2]=f4d8cc38
A[3]=5d61b0f7  B[3]=0fd568b1  C[3]=d1f9b128  D[3]=55159f98
A[4]=79528a9d  B[4]=02d57fff  C[4]=9930fb43  D[4]=2208974a
A[5]=fb17f46f  B[5]=33931a27  C[5]=4662aaa8  D[5]=0ed12a11
A[6]=09573e69  B[6]=4fb01753  C[6]=3e9391b8  D[6]=eab29155
A[7]=c47523c8  B[7]=8a3a7bb9  C[7]=1addd7cd  D[7]=3e83b6ce

Step 13: (r= 4, s=23)
A[0]=d28b1b13  B[0]=f45d71bf  C[0]=82ba50ea  D[0]=30f3fd72
A[1]=667f6d75  B[1]=371bf39b  C[1]=b1b9f6f6  D[1]=0be71b0c
A[2]=c37f164c  B[2]=527f4e9c  C[2]=aaa56398  D[2]=a5462f74
A[3]=b67b3fb6  B[3]=d61b0f75  C[3]=0fd568b1  D[3]=d1f9b128
A[4]=05b0a6d3  B[4]=9528a9d7  C[4]=02d57fff  D[4]=9930fb43
A[5]=dfffac7b  B[5]=b17f46ff  C[5]=33931a27  D[5]=4662aaa8
A[6]=33d0cc50  B[6]=9573e690  C[6]=4fb01753  D[6]=3e9391b8
A[7]=ba903984  B[7]=47523c8c  C[7]=8a3a7bb9  D[7]=1addd7cd
```

```
Step 14: (r=23, s=11)
A[0]=46035641  B[0]=89e9458d  C[0]=f45d71bf  D[0]=82ba50ea
A[1]=2eaf7c0e  B[1]=bab33fb6  C[1]=371bf39b  D[1]=b1b9f6f6
A[2]=6281fb99  B[2]=2661bf8b  C[2]=527f4e9c  D[2]=aaa56398
A[3]=91541b39  B[3]=db5b3d9f  C[3]=d61b0f75  D[3]=0fd568b1
A[4]=e085d22e  B[4]=6982d853  C[4]=9528a9d7  D[4]=02d57fff
A[5]=36d52989  B[5]=3defffd6  C[5]=b17f46ff  D[5]=33931a27
A[6]=e7026cc9  B[6]=2819e866  C[6]=9573e690  D[6]=4fb01753
A[7]=bfcfad02  B[7]=c25d481c  C[7]=47523c8c  D[7]=8a3a7bb9

Step 15: (r=11, s=26)
A[0]=7eaf2665  B[0]=1ab20a30  C[0]=89e9458d  D[0]=f45d71bf
A[1]=c3b90a24  B[1]=7be07175  C[1]=bab33fb6  D[1]=371bf39b
A[2]=04eca1e2  B[2]=0fdccb14  C[2]=2661bf8b  D[2]=527f4e9c
A[3]=a5cda812  B[3]=a0d9cc8a  C[3]=db5b3d9f  D[3]=d61b0f75
A[4]=368ba8d5  B[4]=2e917704  C[4]=6982d853  D[4]=9528a9d7
A[5]=6a7c7337  B[5]=a94c49b6  C[5]=3defffd6  D[5]=b17f46ff
A[6]=08602f2c  B[6]=13664f38  C[6]=2819e866  D[6]=9573e690
A[7]=1a178acf  B[7]=7d6815fe  C[7]=c25d481c  D[7]=47523c8c

Step 16: (r=19, s=28)
A[0]=3472aed5  B[0]=332bf579  C[0]=1ab20a30  D[0]=89e9458d
A[1]=8a349c31  B[1]=51261dc8  C[1]=7be07175  D[1]=bab33fb6
A[2]=84a010d1  B[2]=0f102765  C[2]=0fdccb14  D[2]=2661bf8b
A[3]=9b7852dc  B[3]=40952e6d  C[3]=a0d9cc8a  D[3]=db5b3d9f
A[4]=8934e651  B[4]=46a9b45d  C[4]=2e917704  D[4]=6982d853
A[5]=9590b5ba  B[5]=99bb53e3  C[5]=a94c49b6  D[5]=3defffd6
A[6]=f8cfb523  B[6]=79604301  C[6]=13664f38  D[6]=2819e866
A[7]=9bc97a68  B[7]=5678d0bc  C[7]=7d6815fe  D[7]=c25d481c

Step 17: (r=28, s= 7)
A[0]=04a85a85  B[0]=53472aed  C[0]=332bf579  D[0]=1ab20a30
A[1]=523cc61c  B[1]=18a349c3  C[1]=51261dc8  D[1]=7be07175
A[2]=2f7b9698  B[2]=184a010d  C[2]=0f102765  D[2]=0fdccb14
A[3]=4dfa01d0  B[3]=c9b7852d  C[3]=40952e6d  D[3]=a0d9cc8a
A[4]=d5d74b96  B[4]=18934e65  C[4]=46a9b45d  D[4]=2e917704
A[5]=d535f0d5  B[5]=a9590b5b  C[5]=99bb53e3  D[5]=a94c49b6
A[6]=e38f00d4  B[6]=3f8cfb52  C[6]=79604301  D[6]=13664f38
A[7]=16daee44  B[7]=89bc97a6  C[7]=5678d0bc  D[7]=7d6815fe

Step 18: (r= 7, s=22)
A[0]=5bcd2cb6  B[0]=542d4282  C[0]=53472aed  D[0]=332bf579
A[1]=2e5011b7  B[1]=1e630e29  C[1]=18a349c3  D[1]=51261dc8
A[2]=2f7400af  B[2]=bdcb4c17  C[2]=184a010d  D[2]=0f102765
A[3]=a891a0b7  B[3]=fd00e826  C[3]=c9b7852d  D[3]=40952e6d
A[4]=f41a98f9  B[4]=eba5cb6a  C[4]=18934e65  D[4]=46a9b45d
A[5]=a75066b1  B[5]=9af86aea  C[5]=a9590b5b  D[5]=99bb53e3
A[6]=8a4d1977  B[6]=c7806a71  C[6]=3f8cfb52  D[6]=79604301
```

```
A[7]=8f59be30  B[7]=6d77220b  C[7]=89bc97a6  D[7]=5678d0bc

Step 19: (r=22, s=19)
A[0]=be9f627f  B[0]=2d96f34b  C[0]=542d4282  D[0]=53472aed
A[1]=bcb47565  B[1]=6dcb9404  C[1]=1e630e29  D[1]=18a349c3
A[2]=707d26e7  B[2]=2bcbdd00  C[2]=bdcb4c17  D[2]=184a010d
A[3]=333f1a13  B[3]=2dea2468  C[3]=fd00e826  D[3]=c9b7852d
A[4]=51d05eb7  B[4]=3e7d06a6  C[4]=eba5cb6a  D[4]=18934e65
A[5]=881498ca  B[5]=ac69d419  C[5]=9af86aea  D[5]=a9590b5b
A[6]=1f7adbf3  B[6]=5de29346  C[6]=c7806a71  D[6]=3f8cfb52
A[7]=800b97c9  B[7]=8c23d66f  C[7]=6d77220b  D[7]=89bc97a6

Step 20: (r=19, s=28)
A[0]=87ee0ab4  B[0]=13fdf4fb  C[0]=2d96f34b  D[0]=542d4282
A[1]=c27a41b5  B[1]=ab2de5a3  C[1]=6dcb9404  D[1]=1e630e29
A[2]=4b1ec965  B[2]=373b83e9  C[2]=2bcbdd00  D[2]=bdcb4c17
A[3]=e771def5  B[3]=d09999f8  C[3]=2dea2468  D[3]=fd00e826
A[4]=85b5d45b  B[4]=f5ba8e82  C[4]=3e7d06a6  D[4]=eba5cb6a
A[5]=16efdeac  B[5]=c65440a4  C[5]=ac69d419  D[5]=9af86aea
A[6]=486cdd9e  B[6]=df98fbd6  C[6]=5de29346  D[6]=c7806a71
A[7]=0f46f065  B[7]=be4c005c  C[7]=8c23d66f  D[7]=6d77220b

Step 21: (r=28, s= 7)
A[0]=4801ce8e  B[0]=487ee0ab  C[0]=13fdf4fb  D[0]=2d96f34b
A[1]=a6b7a49d  B[1]=5c27a41b  C[1]=ab2de5a3  D[1]=6dcb9404
A[2]=ed186c10  B[2]=54b1ec96  C[2]=373b83e9  D[2]=2bcbdd00
A[3]=9af971fd  B[3]=5e771def  C[3]=d09999f8  D[3]=2dea2468
A[4]=2eb72ba2  B[4]=b85b5d45  C[4]=f5ba8e82  D[4]=3e7d06a6
A[5]=f7974693  B[5]=c16efdea  C[5]=c65440a4  D[5]=ac69d419
A[6]=49d1a484  B[6]=e486cdd9  C[6]=df98fbd6  D[6]=5de29346
A[7]=06fbd3d4  B[7]=50f46f06  C[7]=be4c005c  D[7]=8c23d66f

Step 22: (r= 7, s=22)
A[0]=ca0620ba  B[0]=00e74724  C[0]=487ee0ab  D[0]=13fdf4fb
A[1]=37661865  B[1]=5bd24ed3  C[1]=5c27a41b  D[1]=ab2de5a3
A[2]=fc81beb7  B[2]=8c360876  C[2]=54b1ec96  D[2]=373b83e9
A[3]=411bbde2  B[3]=7cb8fecd  C[3]=5e771def  D[3]=d09999f8
A[4]=1ff1b3d8  B[4]=5b95d117  C[4]=b85b5d45  D[4]=f5ba8e82
A[5]=0ae7a8e7  B[5]=cba349fb  C[5]=c16efdea  D[5]=c65440a4
A[6]=698764c9  B[6]=e8d24224  C[6]=e486cdd9  D[6]=df98fbd6
A[7]=9661ead8  B[7]=7de9ea03  C[7]=50f46f06  D[7]=be4c005c

Step 23: (r=22, s=19)
A[0]=1f376392  B[0]=2eb28188  C[0]=00e74724  D[0]=487ee0ab
A[1]=bb831c81  B[1]=194dd986  C[1]=5bd24ed3  D[1]=5c27a41b
A[2]=3180871c  B[2]=adff206f  C[2]=8c360876  D[2]=54b1ec96
A[3]=b7ccbcbf  B[3]=789046ef  C[3]=7cb8fecd  D[3]=5e771def
A[4]=9ec99c94  B[4]=f607fc6c  C[4]=5b95d117  D[4]=b85b5d45
A[5]=325ca6dd  B[5]=39c2b9ea  C[5]=cba349fb  D[5]=c16efdea
```

```
A[6]=0f000566  B[6]=325a61d9  C[6]=e8d24224  D[6]=e486cdd9
A[7]=8af220f5  B[7]=b625987a  C[7]=7de9ea03  D[7]=50f46f06

Step 24: (r=15, s= 5)
A[0]=e7673ca2  B[0]=b1c90f9b  C[0]=2eb28188  D[0]=00e74724
A[1]=87b5c684  B[1]=8e40ddc1  C[1]=194dd986  D[1]=5bd24ed3
A[2]=68d1bf13  B[2]=438e18c0  C[2]=adff206f  D[2]=8c360876
A[3]=533289e3  B[3]=5e5fdbe6  C[3]=789046ef  D[3]=7cb8fecd
A[4]=fa9329e2  B[4]=ce4a4f64  C[4]=f607fc6c  D[4]=5b95d117
A[5]=7a1e0884  B[5]=536e992e  C[5]=39c2b9ea  D[5]=cba349fb
A[6]=a0164458  B[6]=02b30780  C[6]=325a61d9  D[6]=e8d24224
A[7]=b2da8a28  B[7]=107ac579  C[7]=b625987a  D[7]=7de9ea03

Step 25: (r= 5, s=29)
A[0]=2394c8fd  B[0]=ece7945c  C[0]=b1c90f9b  D[0]=2eb28188
A[1]=c8d8feb0  B[1]=f6b8d090  C[1]=8e40ddc1  D[1]=194dd986
A[2]=31ea1db2  B[2]=1a37e26d  C[2]=438e18c0  D[2]=adff206f
A[3]=3ffa800f  B[3]=66513c6a  C[3]=5e5fdbe6  D[3]=789046ef
A[4]=b1c8f717  B[4]=52653c5f  C[4]=ce4a4f64  D[4]=f607fc6c
A[5]=3c6ac857  B[5]=43c1108f  C[5]=536e992e  D[5]=39c2b9ea
A[6]=1ef7bc26  B[6]=02c88b14  C[6]=02b30780  D[6]=325a61d9
A[7]=54a3e149  B[7]=5b514516  C[7]=107ac579  D[7]=b625987a

Step 26: (r=29, s= 9)
A[0]=a4d8cfb5  B[0]=a472991f  C[0]=ece7945c  D[0]=b1c90f9b
A[1]=8885aff3  B[1]=191b1fd6  C[1]=f6b8d090  D[1]=8e40ddc1
A[2]=c36d676b  B[2]=463d43b6  C[2]=1a37e26d  D[2]=438e18c0
A[3]=531d4101  B[3]=e7ff5001  C[3]=66513c6a  D[3]=5e5fdbe6
A[4]=c11bd3fe  B[4]=f6391ee2  C[4]=52653c5f  D[4]=ce4a4f64
A[5]=b25d1826  B[5]=e78d590a  C[5]=43c1108f  D[5]=536e992e
A[6]=0ef41c41  B[6]=c3def784  C[6]=02c88b14  D[6]=02b30780
A[7]=5c9834c1  B[7]=2a947c29  C[7]=5b514516  D[7]=107ac579

Step 27: (r= 9, s=15)
A[0]=1edeb9e7  B[0]=b19f6b49  C[0]=a472991f  D[0]=ece7945c
A[1]=667ac620  B[1]=0b5fe711  C[1]=191b1fd6  D[1]=f6b8d090
A[2]=ea34bcfb  B[2]=daced786  C[2]=463d43b6  D[2]=1a37e26d
A[3]=7efac32f  B[3]=3a8202a6  C[3]=e7ff5001  D[3]=66513c6a
A[4]=86b32dbc  B[4]=37a7fd82  C[4]=f6391ee2  D[4]=52653c5f
A[5]=0eebd7e0  B[5]=ba304d64  C[5]=e78d590a  D[5]=43c1108f
A[6]=80b883ae  B[6]=e838821d  C[6]=c3def784  D[6]=02c88b14
A[7]=e62a026c  B[7]=306982b9  C[7]=2a947c29  D[7]=5b514516

Step 28: (r=15, s= 5)
A[0]=1f526558  B[0]=5cf38f6f  C[0]=b19f6b49  D[0]=a472991f
A[1]=9309900c  B[1]=6310333d  C[1]=0b5fe711  D[1]=191b1fd6
A[2]=5aad999a  B[2]=5e7df51a  C[2]=daced786  D[2]=463d43b6
A[3]=3ce7925c  B[3]=6197bf7d  C[3]=3a8202a6  D[3]=e7ff5001
A[4]=a786af2e  B[4]=96de4359  C[4]=37a7fd82  D[4]=f6391ee2
```

```
A[5]=0a4ddb35  B[5]=ebf00775  C[5]=ba304d64  D[5]=e78d590a
A[6]=bb60fd24  B[6]=41d7405c  C[6]=e838821d  D[6]=c3def784
A[7]=67fbb170  B[7]=01367315  C[7]=306982b9  D[7]=2a947c29

Step 29: (r= 5, s=29)
A[0]=57910ac3  B[0]=ea4cab03  C[0]=5cf38f6f  D[0]=b19f6b49
A[1]=fa440c1a  B[1]=61320192  C[1]=6310333d  D[1]=0b5fe711
A[2]=f1611b3e  B[2]=55b3334b  C[2]=5e7df51a  D[2]=daced786
A[3]=0700fc23  B[3]=9cf24b87  C[3]=6197bf7d  D[3]=3a8202a6
A[4]=cb34fcf7  B[4]=f0d5e5d4  C[4]=96de4359  D[4]=37a7fd82
A[5]=2bd4a8fd  B[5]=49bb66a1  C[5]=ebf00775  D[5]=ba304d64
A[6]=d3750fd2  B[6]=6c1fa497  C[6]=41d7405c  D[6]=e838821d
A[7]=00a21f27  B[7]=ff762e0c  C[7]=01367315  D[7]=306982b9

Step 30: (r=29, s= 9)
A[0]=1d3902cd  B[0]=6af22158  C[0]=ea4cab03  D[0]=5cf38f6f
A[1]=4882ea92  B[1]=5f488183  C[1]=61320192  D[1]=6310333d
A[2]=3160cbae  B[2]=de2c2367  C[2]=55b3334b  D[2]=5e7df51a
A[3]=c34c9c3b  B[3]=60e01f84  C[3]=9cf24b87  D[3]=6197bf7d
A[4]=e7d2426d  B[4]=f9669f9e  C[4]=f0d5e5d4  D[4]=96de4359
A[5]=876f6f58  B[5]=a57a951f  C[5]=49bb66a1  D[5]=ebf00775
A[6]=53c0946b  B[6]=5a6ea1fa  C[6]=6c1fa497  D[6]=41d7405c
A[7]=aee89b48  B[7]=e01443e4  C[7]=ff762e0c  D[7]=01367315

Step 31: (r= 9, s=15)
A[0]=23c599a0  B[0]=72059a3a  C[0]=6af22158  D[0]=ea4cab03
A[1]=1b392525  B[1]=05d52491  C[1]=5f488183  D[1]=61320192
A[2]=83693a7b  B[2]=c1975c62  C[2]=de2c2367  D[2]=55b3334b
A[3]=c7b09ba0  B[3]=99387786  C[3]=60e01f84  D[3]=9cf24b87
A[4]=ff7756bd  B[4]=a484dbcf  C[4]=f9669f9e  D[4]=f0d5e5d4
A[5]=134c8717  B[5]=dedeb10e  C[5]=a57a951f  D[5]=49bb66a1
A[6]=8687d830  B[6]=8128d6a7  C[6]=5a6ea1fa  D[6]=6c1fa497
A[7]=2bfc1bc8  B[7]=d136915d  C[7]=e01443e4  D[7]=ff762e0c

Feed-Forward Step 0: (r=15, s= 5)
A[0]=17ff883c  B[0]=ccd011e2  C[0]=72059a3a  D[0]=6af22158
A[1]=692b0847  B[1]=92928d9c  C[1]=05d52491  D[1]=5f488183
A[2]=3535ed4f  B[2]=9d3dc1b4  C[2]=c1975c62  D[2]=de2c2367
A[3]=ff38b3b5  B[3]=4dd063d8  C[3]=99387786  D[3]=60e01f84
A[4]=e5d61771  B[4]=ab5effbb  C[4]=a484dbcf  D[4]=f9669f9e
A[5]=f6ebb3a4  B[5]=438b89a6  C[5]=dedeb10e  D[5]=a57a951f
A[6]=f7cde977  B[6]=ec184343  C[6]=8128d6a7  D[6]=5a6ea1fa
A[7]=ba34dd1e  B[7]=0de415fe  C[7]=d136915d  D[7]=e01443e4

Feed-Forward Step 1: (r= 5, s=29)
A[0]=812c9237  B[0]=fff10782  C[0]=ccd011e2  D[0]=72059a3a
A[1]=ffc2955b  B[1]=256108ed  C[1]=92928d9c  D[1]=05d52491
A[2]=fde8e2ff  B[2]=a6bda9e6  C[2]=9d3dc1b4  D[2]=c1975c62
A[3]=d11fe467  B[3]=e71676bf  C[3]=4dd063d8  D[3]=99387786
```

```
A[4]=d3237532  B[4]=bac2ee3c  C[4]=ab5effbb  D[4]=a484dbcf
A[5]=326d594b  B[5]=dd76749e  C[5]=438b89a6  D[5]=dedeb10e
A[6]=7401bf7e  B[6]=f9bd2efe  C[6]=ec184343  D[6]=8128d6a7
A[7]=d1e388ce  B[7]=469ba3d7  C[7]=0de415fe  D[7]=d136915d

Feed-Forward Step 2: (r=29, s= 9)
A[0]=52772a13  B[0]=f0259246  C[0]=fff10782  D[0]=ccd011e2
A[1]=d6fa4874  B[1]=7ff852ab  C[1]=256108ed  D[1]=92928d9c
A[2]=3966c160  B[2]=ffbd1c5f  C[2]=a6bda9e6  D[2]=9d3dc1b4
A[3]=7eda065b  B[3]=fa23fc8c  C[3]=e71676bf  D[3]=4dd063d8
A[4]=4d40f9d1  B[4]=5a646ea6  C[4]=bac2ee3c  D[4]=ab5effbb
A[5]=7d4772d0  B[5]=664dab29  C[5]=dd76749e  D[5]=438b89a6
A[6]=23f7e18c  B[6]=ce8037ef  C[6]=f9bd2efe  D[6]=ec184343
A[7]=6c9db736  B[7]=da3c7119  C[7]=469ba3d7  D[7]=0de415fe

Feed-Forward Step 3: (r= 9, s=15)
A[0]=b1230f3f  B[0]=ee5426a4  C[0]=f0259246  D[0]=fff10782
A[1]=c8b8a4e6  B[1]=f490e9ad  C[1]=7ff852ab  D[1]=256108ed
A[2]=f25d5289  B[2]=cd82c072  C[2]=ffbd1c5f  D[2]=a6bda9e6
A[3]=f9105d30  B[3]=b40cb6fd  C[3]=fa23fc8c  D[3]=e71676bf
A[4]=bac54e8a  B[4]=81f3a29a  C[4]=5a646ea6  D[4]=bac2ee3c
A[5]=75c5c83d  B[5]=8ee5a0fa  C[5]=664dab29  D[5]=dd76749e
A[6]=b27c2719  B[6]=efc31847  C[6]=ce8037ef  D[6]=f9bd2efe
A[7]=1ff6826f  B[7]=3b6e6cd9  C[7]=da3c7119  D[7]=469ba3d7
```

Compression Function Output

```
A[0]=b1230f3f  B[0]=ee5426a4  C[0]=f0259246  D[0]=fff10782
A[1]=c8b8a4e6  B[1]=f490e9ad  C[1]=7ff852ab  D[1]=256108ed
A[2]=f25d5289  B[2]=cd82c072  C[2]=ffbd1c5f  D[2]=a6bda9e6
A[3]=f9105d30  B[3]=b40cb6fd  C[3]=fa23fc8c  D[3]=e71676bf
A[4]=bac54e8a  B[4]=81f3a29a  C[4]=5a646ea6  D[4]=bac2ee3c
A[5]=75c5c83d  B[5]=8ee5a0fa  C[5]=664dab29  D[5]=dd76749e
A[6]=b27c2719  B[6]=efc31847  C[6]=ce8037ef  D[6]=f9bd2efe
A[7]=1ff6826f  B[7]=3b6e6cd9  C[7]=da3c7119  D[7]=469ba3d7
```

Hash Function Output

```
3f 0f 23 b1 e6 a4 b8 c8 89 52 5d f2 30 5d 10 f9
8a 4e c5 ba 3d c8 c5 75 19 27 7c b2 6f 82 f6 1f
a4 26 54 ee ad e9 90 f4 72 c0 82 cd fd b6 0c b4
9a a2 f3 81 fa a0 e5 8e 47 18 c3 ef d9 6c 6e 3b
```

6.4.3 Two blocks message

We use the message made of 1079 1 bits.

First message block

```
M[  0..  7] = ff ff ff ff ff ff ff ff
```

```
M[  8.. 15] = ff ff ff ff ff ff ff ff
M[ 16.. 23] = ff ff ff ff ff ff ff ff
M[ 24.. 31] = ff ff ff ff ff ff ff ff
M[ 32.. 39] = ff ff ff ff ff ff ff ff
M[ 40.. 47] = ff ff ff ff ff ff ff ff
M[ 48.. 55] = ff ff ff ff ff ff ff ff
M[ 56.. 63] = ff ff ff ff ff ff ff ff
M[ 64.. 71] = ff ff ff ff ff ff ff ff
M[ 72.. 79] = ff ff ff ff ff ff ff ff
M[ 80.. 87] = ff ff ff ff ff ff ff ff
M[ 88.. 95] = ff ff ff ff ff ff ff ff
M[ 96..103] = ff ff ff ff ff ff ff ff
M[104..111] = ff ff ff ff ff ff ff ff
M[112..119] = ff ff ff ff ff ff ff ff
M[120..127] = ff ff ff ff ff ff ff ff
```

NTT Output

```
y[  0..  7] =    2   86   98  227   95   77   58  143
y[  8.. 15] =   30   88  113  180   23   99  198   13
y[ 16.. 23] =  129   99   49  124  176  112   29   25
y[ 24.. 31] =   15   75  185   88  140  162   99  143
y[ 32.. 39] =  193   12  153  234   88   32  143  123
y[ 40.. 47] =  136  228  221  198   70  243  178  116
y[ 48.. 55] =  225  137  205    0   44    3  200  137
y[ 56.. 63] =   68   61  239  127   35  160   89  129
y[ 64.. 71] =  241   24  231  210   22  182  100  124
y[ 72.. 79] =   34   91  248   64  146  239  173   25
y[ 80.. 87] =  249   80  244  174   11   64   50   18
y[ 88.. 95] =   17  161  124   95   73  100  215  156
y[ 96..103] =  253  250  122   18  134  251   25  162
y[104..111] =  137  234   62   10  165  228  236   41
y[112..119] =  255  140   61   62   67  176  141  238
y[120..127] =  197  205   31  131  211   74  118   53
y[128..135] =  256  253  159   94  162  227  199   89
y[136..143] =  227  118  144   32  234  217   59  152
y[144..151] =  128  177  208  172   81  165  228  147
y[152..159] =  242  179   72  170  117  128  158  176
y[160..167] =   64   85  104  220  169  115  114  114
y[168..175] =  121   95   36  140  187  171   79  181
y[176..183] =   32  233   52  163  213   31   57   89
y[184..191] =  189  205   18  166  222  123  168   76
y[192..199] =   16   20   26   13  235   31  157  116
y[200..207] =  223  189    9  151  111  104   84  111
y[208..215] =    8  129   13  175  246  104  207  165
y[216..223] =  240  108  133    7  184  209   42  253
y[224..231] =    4  194  135  198  123  254  232   90
y[232..239] =  120  100  195  219   92  239   21  189
y[240..247] =    2  201  196  128  190  118  116   62
y[248..255] =   60   69  226   71   46  111  139  114
```

Intermediate Expanded Message

```
Z[ 0] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
Z[ 1] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
Z[ 2] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
Z[ 3] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
Z[ 4] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
Z[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
Z[ 6] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
Z[ 7] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
Z[ 8] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
Z[ 9] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
Z[10] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
Z[11] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
Z[12] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
Z[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
Z[14] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
Z[15] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
Z[16] = ff2101be  aaa2555e  ad3f52c1  cd7a3286
        e5de1a22  9d91626f  ebf71409  3365cc9b
Z[17] = 6f809080  d5512aaf  468fb971  e6bd1943
        f2ef0d11  3eb8c148  65eb9a15  a9c3563d
Z[18] = 37c0c840  5a98a568  b3584ca8  634e9cb2
        69679699  1f5ce0a4  c3063cfa  44d1bb2f
Z[19] = 1be0e420  2d4cd2b4  d9ac2654  31a7ce59
        c4c43b3c  0faef052  e1831e7d  b2794d87
Z[20] = 0df0f210  16a6e95a  ecd6132a  a8e4571c
        e2621d9e  07d7f829  60b19f4f  492cb6d4
Z[21] = 06f8f908  0b53f4ad  f66b0995  d4722b8e
        f1310ecf  93fc6c04  c0693f97  2496db6a
Z[22] = 037cfc84  95ba6a46  6b2594db  ea3915c7
        68889778  c9fe3602  5024afdc  124bedb5
Z[23] = 01befe42  cadd3523  c5a33a5d  650c9af4
        3444cbbc  e4ff1b01  2812d7ee  993666ca
```

```
Z[24] = fc844aea  51e2e5de  e5de4313  4d879cb2
        66ca4ca8  1be0bced  dd28563d  a4890b53
Z[25] = ba50563d  b5f56c04  afdc6190  a02e15c7
        bc0e4155  b4374ca8  6f80ad3f  b9719cb2
Z[26] = 4a0b0a74  dfc5ebf7  642d1be0  634e6b25
        52c1e6bd  9a15cc9b  b516f3ce  bdcc650c
Z[27] = eb189778  ae1e0000  1b01029d  4d879778
        d2b43523  b0bb6ea1  6b25ab81  42349080
Z[28] = 116c14e8  0b53d70f  1b01beab  650c6c04
        c4c44f45  a3aa37c0  5a98f052  60b115c7
Z[29] = 908045b0  b892b7b3  5a9837c0  afdc0fae
        5e14ac60  061952c1  d630571c  fc84a805
Z[30] = c91ff9e7  cc9b0fae  fd63fac6  4e66ad3f
        571cebf7  dee608b6  f052e6bd  c4c423b7
Z[31] = cf389a15  6f803602  66cab971  3602ef73
        3c1bd2b4  3dd9923e  60b14076  634e2e2b
```

Expanded Message

```
W[ 0] = 1158f470  de09ed36  c9cd0fe6  599c4844
        41c31892  2e40f97f  f2feafc9  1211c34c
W[ 1] = faf1fd1c  0d02582a  fbaaa71d  bb591211
        ef61a948  073a2cce  eb0bbd84  1da1f0d3
W[ 2] = 3e260172  ea5246d2  37a544a7  ad9e29ea
        3f9815ae  c85b51a9  478b109f  0965d55d
W[ 3] = 08acd1c0  ef61b4d8  17203f98  58e3ad9e
        eb0ba88f  d55de5fc  f5e23296  53d4c6e9
W[ 4] = ab73fe8e  2cce2c15  c577306b  f245ac2c
        da6cd4a4  a4f21667  357adec2  264d5546
W[ 5] = 39d0fa38  c405f69b  2e4007f3  0d022422
        baa00c49  44a7599c  484434c1  b703e1a6
W[ 6] = a948e8e0  0000da6c  022b1fcc  a948d6cf
        2c153124  5bc7f2fe  b9e7194b  a3804051
W[ 7] = 478ba380  599c2369  50f0c577  121114f5
        36330ad7  3f98cbf8  bb59ab73  ad9e478b
W[ 8] = d7880172  5c80d3eb  5546cf95  2cce53d4
        31dd2b5c  334fe999  5037213e  5262aaba
W[ 9] = eea81720  bc122594  1667e034  40512931
        da6ccedc  be3d0d02  58e3e6b5  36ecbfaf
W[10] = 0e740b90  096512ca  1667f01a  53d4b7bc
        cedce76e  b3660681  4b285037  50373cb4
W[11] = fd1cff47  43eeb92e  ea52bb59  4051d616
        5546ea52  1720ae57  e318ef61  b41f2aa3
W[12] = c6305c80  c293dc97  bd843a89  b082eb0b
        c7a2f529  c1213408  5c80548d  c577b875
W[13] = a38005c8  c4be0965  4b28f80d  bd84dbde
        4e0cf3b7  050fa664  dd50cb3f  fd1c1e5a
W[14] = 3d6d2e40  e5434b28  531bc068  52625262
        44a75771  ab731a04  c1dacd6a  c9143917
```

```
W[15] = d27902e4  d55da7d6  fdd558e3  410aedef
        484456b8  e48ad332  f2fe427c  cedc0f2d
W[16] = 6f809080  d5512aaf  468fb971  e6bd1943
        f2ef0d11  3eb8c148  65eb9a15  a9c3563d
W[17] = 37c0c840  5a98a568  b3584ca8  634e9cb2
        69679699  1f5ce0a4  c3063cfa  44d1bb2f
W[18] = 01befe42  cadd3523  c5a33a5d  650c9af4
        3444cbbc  e4ff1b01  2812d7ee  993666ca
W[19] = 0df0f210  16a6e95a  ecd6132a  a8e4571c
        e2621d9e  07d7f829  60b19f4f  492cb6d4
W[20] = 037cfc84  95ba6a46  6b2594db  ea3915c7
        68889778  c9fe3602  5024afdc  124bedb5
W[21] = 06f8f908  0b53f4ad  f66b0995  d4722b8e
        f1310ecf  93fc6c04  c0693f97  2496db6a
W[22] = ff2101be  aaa2555e  ad3f52c1  cd7a3286
        e5de1a22  9d91626f  ebf71409  3365cc9b
W[23] = 1be0e420  2d4cd2b4  d9ac2654  31a7ce59
        c4c43b3c  0faef052  e1831e7d  b2794d87
W[24] = c91ff9e7  cc9b0fae  fd63fac6  4e66ad3f
        571cebf7  dee608b6  f052e6bd  c4c423b7
W[25] = fc844aea  51e2e5de  e5de4313  4d879cb2
        66ca4ca8  1be0bced  dd28563d  a4890b53
W[26] = ba50563d  b5f56c04  afdc6190  a02e15c7
        bc0e4155  b4374ca8  6f80ad3f  b9719cb2
W[27] = cf389a15  6f803602  66cab971  3602ef73
        3c1bd2b4  3dd9923e  60b14076  634e2e2b
W[28] = eb189778  ae1e0000  1b01029d  4d879778
        d2b43523  b0bb6ea1  6b25ab81  42349080
W[29] = 908045b0  b892b7b3  5a9837c0  afdc0fae
        5e14ac60  061952c1  d630571c  fc84a805
W[30] = 116c14e8  0b53d70f  1b01beab  650c6c04
        c4c44f45  a3aa37c0  5a98f052  60b115c7
W[31] = 4a0b0a74  dfc5ebf7  642d1be0  634e6b25
        52c1e6bd  9a15cc9b  b516f3ce  bdcc650c
```

Feistel Steps

```
IV :
A[0]=b314b806  B[0]=f778d95b  C[0]=14c1303a  D[0]=d10eca9e
A[1]=676cf96e  B[1]=6e5e21da  C[1]=b5b890d5  D[1]=ea3c1b82
A[2]=ed91a471  B[2]=ad570671  C[2]=82e61e95  D[2]=5061c319
A[3]=5f306791  B[3]=4584c064  C[3]=94f47683  D[3]=0c2a9f5c
A[4]=4ea515ee  B[4]=ac201a0f  C[4]=6ebc9ce7  D[4]=fcfc980e
A[5]=de2a06cf  B[5]=d4ce2a86  C[5]=f9af5b29  D[5]=bab373c6
A[6]=c9c96851  B[6]=c6d663f4  C[6]=f4177798  D[6]=1699d7c9
A[7]=4f49a403  B[7]=8ec5d766  C[7]=f6cec3ee  D[7]=0822d6af

IV XOR M :
A[0]=4ceb47f9  B[0]=088726a4  C[0]=eb3ecfc5  D[0]=2ef13561
```

```
A[1]=98930691  B[1]=91a1de25  C[1]=4a476f2a  D[1]=15c3e47d
A[2]=126e5b8e  B[2]=52a8f98e  C[2]=7d19e16a  D[2]=af9e3ce6
A[3]=a0cf986e  B[3]=ba7b3f9b  C[3]=6b0b897c  D[3]=f3d560a3
A[4]=b15aea11  B[4]=53dfe5f0  C[4]=91436318  D[4]=030367f1
A[5]=21d5f930  B[5]=2b31d579  C[5]=0650a4d6  D[5]=454c8c39
A[6]=363697ae  B[6]=39299c0b  C[6]=0be88867  D[6]=e9662836
A[7]=b0b65bfc  B[7]=713a2899  C[7]=09313c11  D[7]=f7dd2950

Step  0: (r= 3, s=20)
A[0]=4bf6f2a7  B[0]=675a3fca  C[0]=088726a4  D[0]=eb3ecfc5
A[1]=7546a8fe  B[1]=c498348c  C[1]=91a1de25  D[1]=4a476f2a
A[2]=722c4dc9  B[2]=9372dc70  C[2]=52a8f98e  D[2]=7d19e16a
A[3]=b386683c  B[3]=067cc375  C[3]=ba7b3f9b  D[3]=6b0b897c
A[4]=28652ba7  B[4]=8ad7508d  C[4]=53dfe5f0  D[4]=91436318
A[5]=45c0fa82  B[5]=0eafc981  C[5]=2b31d579  D[5]=0650a4d6
A[6]=ca5444bc  B[6]=b1b4bd71  C[6]=39299c0b  D[6]=0be88867
A[7]=4508ef92  B[7]=85b2dfe5  C[7]=713a2899  D[7]=09313c11

Step  1: (r=20, s=14)
A[0]=dd6fed25  B[0]=2a74bf6f  C[0]=675a3fca  D[0]=088726a4
A[1]=53437f60  B[1]=8fe7546a  C[1]=c498348c  D[1]=91a1de25
A[2]=8ba82248  B[2]=dc9722c4  C[2]=9372dc70  D[2]=52a8f98e
A[3]=0cb860a2  B[3]=83cb3866  C[3]=067cc375  D[3]=ba7b3f9b
A[4]=801a1c65  B[4]=ba728652  C[4]=8ad7508d  D[4]=53dfe5f0
A[5]=210b9f9d  B[5]=a8245c0f  C[5]=0eafc981  D[5]=2b31d579
A[6]=32fa305e  B[6]=4bcca544  C[6]=b1b4bd71  D[6]=39299c0b
A[7]=273fb310  B[7]=f924508e  C[7]=85b2dfe5  D[7]=713a2899

Step  2: (r=14, s=27)
A[0]=184d190f  B[0]=fb49775b  C[0]=2a74bf6f  D[0]=675a3fca
A[1]=a436088d  B[1]=dfd814d0  C[1]=8fe7546a  D[1]=c498348c
A[2]=11005227  B[2]=089222ea  C[2]=dc9722c4  D[2]=9372dc70
A[3]=6a70906d  B[3]=1828832e  C[3]=83cb3866  D[3]=067cc375
A[4]=491afd31  B[4]=87196006  C[4]=ba728652  D[4]=8ad7508d
A[5]=81a3af03  B[5]=e7e74842  C[5]=a8245c0f  D[5]=0eafc981
A[6]=57fc1fa0  B[6]=8c178cbe  C[6]=4bcca544  D[6]=b1b4bd71
A[7]=d42b9a31  B[7]=ecc409cf  C[7]=f924508e  D[7]=85b2dfe5

Step  3: (r=27, s= 3)
A[0]=de4f1f96  B[0]=78c268c8  C[0]=fb49775b  D[0]=2a74bf6f
A[1]=3a670faa  B[1]=6d21b044  C[1]=dfd814d0  D[1]=8fe7546a
A[2]=bc11d850  B[2]=38880291  C[2]=089222ea  D[2]=dc9722c4
A[3]=d70226e0  B[3]=6b538483  C[3]=1828832e  D[3]=83cb3866
A[4]=c39d43b9  B[4]=8a48d7e9  C[4]=87196006  D[4]=ba728652
A[5]=dac9eca0  B[5]=1c0d1d78  C[5]=e7e74842  D[5]=a8245c0f
A[6]=d5e4e9ee  B[6]=02bfe0fd  C[6]=8c178cbe  D[6]=4bcca544
A[7]=9fb2ff71  B[7]=8ea15cd1  C[7]=ecc409cf  D[7]=f924508e

Step  4: (r= 3, s=20)
```

```
A[0]=b0b58094  B[0]=f278fcb6  C[0]=78c268c8  D[0]=fb49775b
A[1]=466cbe1f  B[1]=d3387d51  C[1]=6d21b044  D[1]=dfd814d0
A[2]=180ee0eb  B[2]=e08ec285  C[2]=38880291  D[2]=089222ea
A[3]=93dbd3bb  B[3]=b8113706  C[3]=6b538483  D[3]=1828832e
A[4]=c040e48f  B[4]=1cea1dce  C[4]=8a48d7e9  D[4]=87196006
A[5]=0a4cdc09  B[5]=d64f6506  C[5]=1c0d1d78  D[5]=e7e74842
A[6]=cdd85b82  B[6]=af274f76  C[6]=02bfe0fd  D[6]=8c178cbe
A[7]=e9823096  B[7]=fd97fb8c  C[7]=8ea15cd1  D[7]=ecc409cf

Step  5: (r=20, s=14)
A[0]=e53b4a70  B[0]=094b0b58  C[0]=f278fcb6  D[0]=78c268c8
A[1]=eda9787e  B[1]=e1f466cb  C[1]=d3387d51  D[1]=6d21b044
A[2]=44a2a730  B[2]=0eb180ee  C[2]=e08ec285  D[2]=38880291
A[3]=71a95eea  B[3]=3bb93dbd  C[3]=b8113706  D[3]=6b538483
A[4]=48b49005  B[4]=48fc040e  C[4]=1cea1dce  D[4]=8a48d7e9
A[5]=09282ad9  B[5]=c090a4cd  C[5]=d64f6506  D[5]=1c0d1d78
A[6]=0c595d14  B[6]=b82cdd85  C[6]=af274f76  D[6]=02bfe0fd
A[7]=9993091f  B[7]=096e9823  C[7]=fd97fb8c  D[7]=8ea15cd1

Step  6: (r=14, s=27)
A[0]=82641b44  B[0]=d29c394e  C[0]=094b0b58  D[0]=f278fcb6
A[1]=b1bbdb4e  B[1]=5e1fbb6a  C[1]=e1f466cb  D[1]=d3387d51
A[2]=16b0ef72  B[2]=a9cc1128  C[2]=0eb180ee  D[2]=e08ec285
A[3]=2673ff05  B[3]=57ba9c6a  C[3]=3bb93dbd  D[3]=b8113706
A[4]=37b56d52  B[4]=2401522d  C[4]=48fc040e  D[4]=1cea1dce
A[5]=c38afad2  B[5]=0ab6424a  C[5]=c090a4cd  D[5]=d64f6506
A[6]=41665e24  B[6]=57450316  C[6]=b82cdd85  D[6]=af274f76
A[7]=60fa02ff  B[7]=c247e664  C[7]=096e9823  D[7]=fd97fb8c

Step  7: (r=27, s= 3)
A[0]=7443877f  B[0]=241320da  C[0]=d29c394e  D[0]=094b0b58
A[1]=8ac137f6  B[1]=758ddeda  C[1]=5e1fbb6a  D[1]=e1f466cb
A[2]=238b7e23  B[2]=90b5877b  C[2]=a9cc1128  D[2]=0eb180ee
A[3]=09f81957  B[3]=29339ff8  C[3]=57ba9c6a  D[3]=3bb93dbd
A[4]=e2a68675  B[4]=91bdab6a  C[4]=2401522d  D[4]=48fc040e
A[5]=39667d20  B[5]=961c57d6  C[5]=0ab6424a  D[5]=c090a4cd
A[6]=6fe056e8  B[6]=220b32f1  C[6]=57450316  D[6]=b82cdd85
A[7]=8659cbef  B[7]=fb07d017  C[7]=c247e664  D[7]=096e9823

Step  8: (r=26, s= 4)
A[0]=514f5727  B[0]=fdd10e1d  C[0]=241320da  D[0]=d29c394e
A[1]=2f1ea726  B[1]=da2b04df  C[1]=758ddeda  D[1]=5e1fbb6a
A[2]=27fd5b53  B[2]=8c8e2df8  C[2]=90b5877b  D[2]=a9cc1128
A[3]=08311e94  B[3]=5c27e065  C[3]=29339ff8  D[3]=57ba9c6a
A[4]=78d5b723  B[4]=d78a9a19  C[4]=91bdab6a  D[4]=2401522d
A[5]=3ed8f519  B[5]=80e599f4  C[5]=961c57d6  D[5]=0ab6424a
A[6]=64aa92c2  B[6]=a1bf815b  C[6]=220b32f1  D[6]=57450316
A[7]=7f51ef9c  B[7]=be19672f  C[7]=fb07d017  D[7]=c247e664
```

```
Step  9: (r= 4, s=23)
A[0]=2570ffed  B[0]=14f57275  C[0]=fdd10e1d  D[0]=241320da
A[1]=714c47de  B[1]=f1ea7262  C[1]=da2b04df  D[1]=758ddeda
A[2]=7f1fd2b4  B[2]=7fd5b532  C[2]=8c8e2df8  D[2]=90b5877b
A[3]=75cb0a05  B[3]=8311e940  C[3]=5c27e065  D[3]=29339ff8
A[4]=f4113783  B[4]=8d5b7237  C[4]=d78a9a19  D[4]=91bdab6a
A[5]=8643d5b8  B[5]=ed8f5193  C[5]=80e599f4  D[5]=961c57d6
A[6]=acc4dc7c  B[6]=4aa92c26  C[6]=a1bf815b  D[6]=220b32f1
A[7]=7eeaf7a1  B[7]=f51ef9c7  C[7]=be19672f  D[7]=fb07d017

Step 10: (r=23, s=11)
A[0]=95b66df6  B[0]=f692b87f  C[0]=14f57275  D[0]=fdd10e1d
A[1]=2ff59e40  B[1]=ef38a623  C[1]=f1ea7262  D[1]=da2b04df
A[2]=75eb8f1f  B[2]=5a3f8fe9  C[2]=7fd5b532  D[2]=8c8e2df8
A[3]=33faaccc  B[3]=02bae585  C[3]=8311e940  D[3]=5c27e065
A[4]=b52284c6  B[4]=c1fa089b  C[4]=8d5b7237  D[4]=d78a9a19
A[5]=a800ee5a  B[5]=dc4321ea  C[5]=ed8f5193  D[5]=80e599f4
A[6]=63bb21da  B[6]=3e56626e  C[6]=4aa92c26  D[6]=a1bf815b
A[7]=ce858a79  B[7]=d0bf757b  C[7]=f51ef9c7  D[7]=be19672f

Step 11: (r=11, s=26)
A[0]=82653ac8  B[0]=b36fb4ad  C[0]=f692b87f  D[0]=14f57275
A[1]=c3e827d0  B[1]=acf2017f  C[1]=ef38a623  D[1]=f1ea7262
A[2]=c45355be  B[2]=5c78fbaf  C[2]=5a3f8fe9  D[2]=7fd5b532
A[3]=28d0a4e3  B[3]=d566619f  C[3]=02bae585  D[3]=8311e940
A[4]=2e48e889  B[4]=142635a9  C[4]=c1fa089b  D[4]=8d5b7237
A[5]=06885767  B[5]=0772d540  C[5]=dc4321ea  D[5]=ed8f5193
A[6]=0734a623  B[6]=d90ed31d  C[6]=3e56626e  D[6]=4aa92c26
A[7]=1af5c1ae  B[7]=2c53ce74  C[7]=d0bf757b  D[7]=f51ef9c7

Step 12: (r=26, s= 4)
A[0]=1be81ec7  B[0]=220994eb  C[0]=b36fb4ad  D[0]=f692b87f
A[1]=6970fbb5  B[1]=430fa09f  C[1]=acf2017f  D[1]=ef38a623
A[2]=2a00393c  B[2]=fb114d56  C[2]=5c78fbaf  D[2]=5a3f8fe9
A[3]=438cea79  B[3]=8ca34293  C[3]=d566619f  D[3]=02bae585
A[4]=32a31ff2  B[4]=24b923a2  C[4]=142635a9  D[4]=c1fa089b
A[5]=73e6d37d  B[5]=9c1a215d  C[5]=0772d540  D[5]=dc4321ea
A[6]=1c720532  B[6]=8c1cd298  C[6]=d90ed31d  D[6]=3e56626e
A[7]=c5044e45  B[7]=b86bd706  C[7]=2c53ce74  D[7]=d0bf757b

Step 13: (r= 4, s=23)
A[0]=3b6a51eb  B[0]=be81ec71  C[0]=220994eb  D[0]=b36fb4ad
A[1]=dc5d5c3c  B[1]=970fbb56  C[1]=430fa09f  D[1]=acf2017f
A[2]=5891a8f1  B[2]=a00393c2  C[2]=fb114d56  D[2]=5c78fbaf
A[3]=9652ae67  B[3]=38cea794  C[3]=8ca34293  D[3]=d566619f
A[4]=c142a83a  B[4]=2a31ff23  C[4]=24b923a2  D[4]=142635a9
A[5]=26414728  B[5]=3e6d37d7  C[5]=9c1a215d  D[5]=0772d540
A[6]=8d0de223  B[6]=c7205321  C[6]=8c1cd298  D[6]=d90ed31d
A[7]=4b2a4788  B[7]=5044e45c  C[7]=b86bd706  D[7]=2c53ce74
```

```
Step 14: (r=23, s=11)
A[0]=f9e4567a  B[0]=f59db528  C[0]=be81ec71  D[0]=220994eb
A[1]=39ecb23b  B[1]=1e6e2eae  C[1]=970fbb56  D[1]=430fa09f
A[2]=c6426de0  B[2]=78ac48d4  C[2]=a00393c2  D[2]=fb114d56
A[3]=78356778  B[3]=33cb2957  C[3]=38cea794  D[3]=8ca34293
A[4]=2d8d0d1e  B[4]=1d60a154  C[4]=2a31ff23  D[4]=24b923a2
A[5]=f161585d  B[5]=941320a3  C[5]=3e6d37d7  D[5]=9c1a215d
A[6]=d2036fed  B[6]=11c686f1  C[6]=c7205321  D[6]=8c1cd298
A[7]=8c126f96  B[7]=c4259523  C[7]=5044e45c  D[7]=b86bd706

Step 15: (r=11, s=26)
A[0]=8831139d  B[0]=22b3d7cf  C[0]=f59db528  D[0]=be81ec71
A[1]=d7a25f95  B[1]=6591d9cf  C[1]=1e6e2eae  D[1]=970fbb56
A[2]=02e3124f  B[2]=136f0632  C[2]=78ac48d4  D[2]=a00393c2
A[3]=eb96a9bf  B[3]=ab3bc3c1  C[3]=33cb2957  D[3]=38cea794
A[4]=e51c546c  B[4]=6868f16c  C[4]=1d60a154  D[4]=2a31ff23
A[5]=fe65f264  B[5]=0ac2ef8b  C[5]=941320a3  D[5]=3e6d37d7
A[6]=e8b77ba5  B[6]=1b7f6e90  C[6]=11c686f1  D[6]=c7205321
A[7]=d068f6ee  B[7]=937cb460  C[7]=c4259523  D[7]=5044e45c

Step 16: (r=19, s=28)
A[0]=e6eac05b  B[0]=9cec4188  C[0]=22b3d7cf  D[0]=f59db528
A[1]=e88f1783  B[1]=fcaebd12  C[1]=6591d9cf  D[1]=1e6e2eae
A[2]=a40f8631  B[2]=92781718  C[2]=136f0632  D[2]=78ac48d4
A[3]=20268b41  B[3]=4dff5cb5  C[3]=ab3bc3c1  D[3]=33cb2957
A[4]=9c80930a  B[4]=a36728e2  C[4]=6868f16c  D[4]=1d60a154
A[5]=cbdeb69c  B[5]=9327f32f  C[5]=0ac2ef8b  D[5]=941320a3
A[6]=1bdec107  B[6]=dd2f45bb  C[6]=1b7f6e90  D[6]=11c686f1
A[7]=8616a4ba  B[7]=b7768347  C[7]=937cb460  D[7]=c4259523

Step 17: (r=28, s= 7)
A[0]=462b72bc  B[0]=be6eac05  C[0]=9cec4188  D[0]=22b3d7cf
A[1]=64db1ae7  B[1]=3e88f178  C[1]=fcaebd12  D[1]=6591d9cf
A[2]=74bc7364  B[2]=1a40f863  C[2]=92781718  D[2]=136f0632
A[3]=6b103689  B[3]=120268b4  C[3]=4dff5cb5  D[3]=ab3bc3c1
A[4]=0a0a15c3  B[4]=a9c80930  C[4]=a36728e2  D[4]=6868f16c
A[5]=e3df9566  B[5]=ccbdeb69  C[5]=9327f32f  D[5]=0ac2ef8b
A[6]=a7e1c8a6  B[6]=71bdec10  C[6]=dd2f45bb  D[6]=1b7f6e90
A[7]=07ae35b9  B[7]=a8616a4b  C[7]=b7768347  D[7]=937cb460

Step 18: (r= 7, s=22)
A[0]=9c8bb4c0  B[0]=15b95e23  C[0]=be6eac05  D[0]=9cec4188
A[1]=099f9a44  B[1]=6d8d73b2  C[1]=3e88f178  D[1]=fcaebd12
A[2]=31a5881e  B[2]=5e39b23a  C[2]=1a40f863  D[2]=92781718
A[3]=df50af76  B[3]=881b44b5  C[3]=120268b4  D[3]=4dff5cb5
A[4]=1a2ccb6e  B[4]=050ae185  C[4]=a9c80930  D[4]=a36728e2
A[5]=dba9d235  B[5]=efcab371  C[5]=ccbdeb69  D[5]=9327f32f
A[6]=537cc436  B[6]=f0e45353  C[6]=71bdec10  D[6]=dd2f45bb
```

```
A[7]=7430a712  B[7]=d71adc83  C[7]=a8616a4b  D[7]=b7768347

Step 19: (r=22, s=19)
A[0]=58759984  B[0]=302722ed  C[0]=15b95e23  D[0]=be6eac05
A[1]=5a99818c  B[1]=910267e6  C[1]=6d8d73b2  D[1]=3e88f178
A[2]=e381acb1  B[2]=078c6962  C[2]=5e39b23a  D[2]=1a40f863
A[3]=88c903d8  B[3]=ddb7d42b  C[3]=881b44b5  D[3]=120268b4
A[4]=6cc85f7d  B[4]=db868b32  C[4]=050ae185  D[4]=a9c80930
A[5]=c78dbccb  B[5]=8d76ea74  C[5]=efcab371  D[5]=ccbdeb69
A[6]=7071df94  B[6]=0d94df31  C[6]=f0e45353  D[6]=71bdec10
A[7]=10eebbd3  B[7]=c49d0c29  C[7]=d71adc83  D[7]=a8616a4b

Step 20: (r=19, s=28)
A[0]=f984e0fe  B[0]=cc22c3ac  C[0]=302722ed  D[0]=15b95e23
A[1]=0eff8fa2  B[1]=0c62d4cc  C[1]=910267e6  D[1]=6d8d73b2
A[2]=2b93499f  B[2]=658f1c0d  C[2]=078c6962  D[2]=5e39b23a
A[3]=addc8840  B[3]=1ec44648  C[3]=ddb7d42b  D[3]=881b44b5
A[4]=bc5bf32a  B[4]=fbeb6642  C[4]=db868b32  D[4]=050ae185
A[5]=c25413ff  B[5]=e65e3c6d  C[5]=8d76ea74  D[5]=efcab371
A[6]=b1c5ff24  B[6]=fca3838e  C[6]=0d94df31  D[6]=f0e45353
A[7]=359842d6  B[7]=de988775  C[7]=c49d0c29  D[7]=d71adc83

Step 21: (r=28, s= 7)
A[0]=5f564023  B[0]=ef984e0f  C[0]=cc22c3ac  D[0]=302722ed
A[1]=acf5eb46  B[1]=20eff8fa  C[1]=0c62d4cc  D[1]=910267e6
A[2]=099abd4d  B[2]=f2b93499  C[2]=658f1c0d  D[2]=078c6962
A[3]=520a3ef7  B[3]=0addc884  C[3]=1ec44648  D[3]=ddb7d42b
A[4]=4f061b6b  B[4]=abc5bf32  C[4]=fbeb6642  D[4]=db868b32
A[5]=72067d52  B[5]=fc25413f  C[5]=e65e3c6d  D[5]=8d76ea74
A[6]=157ec669  B[6]=4b1c5ff2  C[6]=fca3838e  D[6]=0d94df31
A[7]=210472a7  B[7]=6359842d  C[7]=de988775  D[7]=c49d0c29

Step 22: (r= 7, s=22)
A[0]=38f8ea29  B[0]=ab2011af  C[0]=ef984e0f  D[0]=cc22c3ac
A[1]=43fd57b7  B[1]=7af5a356  C[1]=20eff8fa  D[1]=0c62d4cc
A[2]=0f4442f7  B[2]=cd5ea684  C[2]=f2b93499  D[2]=658f1c0d
A[3]=e07f353c  B[3]=051f7ba9  C[3]=0addc884  D[3]=1ec44648
A[4]=32cac6a2  B[4]=830db5a7  C[4]=abc5bf32  D[4]=fbeb6642
A[5]=65e6ea36  B[5]=033ea939  C[5]=fc25413f  D[5]=e65e3c6d
A[6]=440b5604  B[6]=bf63348a  C[6]=4b1c5ff2  D[6]=fca3838e
A[7]=6576d886  B[7]=82395390  C[7]=6359842d  D[7]=de988775

Step 23: (r=22, s=19)
A[0]=38695090  B[0]=8a4e3e3a  C[0]=ab2011af  D[0]=ef984e0f
A[1]=694e5f26  B[1]=edd0ff55  C[1]=7af5a356  D[1]=20eff8fa
A[2]=c8c17790  B[2]=bdc3d110  C[2]=cd5ea684  D[2]=f2b93499
A[3]=9403e412  B[3]=4f381fcd  C[3]=051f7ba9  D[3]=0addc884
A[4]=53516224  B[4]=a88cb2b1  C[4]=830db5a7  D[4]=abc5bf32
A[5]=9dc3d8f5  B[5]=8d9979ba  C[5]=033ea939  D[5]=fc25413f
```

```
A[6]=822d3a9f  B[6]=811102d5  C[6]=bf63348a  D[6]=4b1c5ff2
A[7]=7b3fc42a  B[7]=21995db6  C[7]=82395390  D[7]=6359842d

Step 24: (r=15, s= 5)
A[0]=af9e5b4f  B[0]=a8481c34  C[0]=8a4e3e3a  D[0]=ab2011af
A[1]=d7e91bc1  B[1]=2f9334a7  C[1]=edd0ff55  D[1]=7af5a356
A[2]=b1a95870  B[2]=bbc86460  C[2]=bdc3d110  D[2]=cd5ea684
A[3]=87db11eb  B[3]=f2094a01  C[3]=4f381fcd  D[3]=051f7ba9
A[4]=4a672871  B[4]=b11229a8  C[4]=a88cb2b1  D[4]=830db5a7
A[5]=0a2a9f55  B[5]=ec7acee1  C[5]=8d9979ba  D[5]=033ea939
A[6]=f85ee63e  B[6]=9d4fc116  C[6]=811102d5  D[6]=bf63348a
A[7]=c42fb3ef  B[7]=e2153d9f  C[7]=21995db6  D[7]=82395390

Step 25: (r= 5, s=29)
A[0]=df28a12f  B[0]=f3cb69f5  C[0]=a8481c34  D[0]=8a4e3e3a
A[1]=3aef8d29  B[1]=fd23783a  C[1]=2f9334a7  D[1]=edd0ff55
A[2]=e1ec5f53  B[2]=352b0e16  C[2]=bbc86460  D[2]=bdc3d110
A[3]=00bd7d06  B[3]=fb623d70  C[3]=f2094a01  D[3]=4f381fcd
A[4]=fd291f7c  B[4]=4ce50e29  C[4]=b11229a8  D[4]=a88cb2b1
A[5]=bb91e89a  B[5]=4553eaa1  C[5]=ec7acee1  D[5]=8d9979ba
A[6]=13a0779c  B[6]=0bdcc7df  C[6]=9d4fc116  D[6]=811102d5
A[7]=865ee631  B[7]=85f67df8  C[7]=e2153d9f  D[7]=21995db6

Step 26: (r=29, s= 9)
A[0]=fe6f3535  B[0]=fbe51425  C[0]=f3cb69f5  D[0]=a8481c34
A[1]=75bc1eb4  B[1]=275df1a5  C[1]=fd23783a  D[1]=2f9334a7
A[2]=e833e264  B[2]=7c3d8bea  C[2]=352b0e16  D[2]=bbc86460
A[3]=ac8e4fb2  B[3]=c017afa0  C[3]=fb623d70  D[3]=f2094a01
A[4]=5c5d0d01  B[4]=9fa523ef  C[4]=4ce50e29  D[4]=b11229a8
A[5]=15a812f8  B[5]=57723d13  C[5]=4553eaa1  D[5]=ec7acee1
A[6]=ea4d56a5  B[6]=82740ef3  C[6]=0bdcc7df  D[6]=9d4fc116
A[7]=c0d561a3  B[7]=30cbdcc6  C[7]=85f67df8  D[7]=e2153d9f

Step 27: (r= 9, s=15)
A[0]=c3b13c6b  B[0]=de6a6bfc  C[0]=fbe51425  D[0]=f3cb69f5
A[1]=bdd19644  B[1]=783d68eb  C[1]=275df1a5  D[1]=fd23783a
A[2]=f0cf1bba  B[2]=67c4c9d0  C[2]=7c3d8bea  D[2]=352b0e16
A[3]=e76dc53a  B[3]=1c9f6559  C[3]=c017afa0  D[3]=fb623d70
A[4]=5e2cf0e5  B[4]=ba1a02b8  C[4]=9fa523ef  D[4]=4ce50e29
A[5]=a4d5a8cf  B[5]=5025f02b  C[5]=57723d13  D[5]=4553eaa1
A[6]=2c888aba  B[6]=9aad4bd4  C[6]=82740ef3  D[6]=0bdcc7df
A[7]=80f18afc  B[7]=aac34781  C[7]=30cbdcc6  D[7]=85f67df8

Step 28: (r=15, s= 5)
A[0]=23ca1a3f  B[0]=9e35e1d8  C[0]=de6a6bfc  D[0]=fbe51425
A[1]=b22305d5  B[1]=cb225ee8  C[1]=783d68eb  D[1]=275df1a5
A[2]=81d1096e  B[2]=8ddd7867  C[2]=67c4c9d0  D[2]=7c3d8bea
A[3]=2f14bc68  B[3]=e29d73b6  C[3]=1c9f6559  D[3]=c017afa0
A[4]=8d1499a1  B[4]=7872af16  C[4]=ba1a02b8  D[4]=9fa523ef
```

```
A[5]=c914d8bf  B[5]=d467d26a  C[5]=5025f02b  D[5]=57723d13
A[6]=fb4e0ab8  B[6]=455d1644  C[6]=9aad4bd4  D[6]=82740ef3
A[7]=6338bdd1  B[7]=c57e4078  C[7]=aac34781  D[7]=30cbdcc6

Step 29: (r= 5, s=29)
A[0]=5f7b268a  B[0]=794347e4  C[0]=9e35e1d8  D[0]=de6a6bfc
A[1]=1dda0bcd  B[1]=4460bab6  C[1]=cb225ee8  D[1]=783d68eb
A[2]=84d8a986  B[2]=3a212dd0  C[2]=8ddd7867  D[2]=67c4c9d0
A[3]=1832e14e  B[3]=e2978d05  C[3]=e29d73b6  D[3]=1c9f6559
A[4]=607ae29e  B[4]=a2933431  C[4]=7872af16  D[4]=ba1a02b8
A[5]=4ccde62b  B[5]=229b17f9  C[5]=d467d26a  D[5]=5025f02b
A[6]=0911624d  B[6]=69c1571f  C[6]=455d1644  D[6]=9aad4bd4
A[7]=a4b4714c  B[7]=6717ba2c  C[7]=c57e4078  D[7]=aac34781

Step 30: (r=29, s= 9)
A[0]=2867e6c7  B[0]=4bef64d1  C[0]=794347e4  D[0]=9e35e1d8
A[1]=87d7f9ea  B[1]=a3bb4179  C[1]=4460bab6  D[1]=cb225ee8
A[2]=a8fe3ee4  B[2]=d09b1530  C[2]=3a212dd0  D[2]=8ddd7867
A[3]=5374231b  B[3]=c3065c29  C[3]=e2978d05  D[3]=e29d73b6
A[4]=64f683e7  B[4]=cc0f5c53  C[4]=a2933431  D[4]=7872af16
A[5]=1097c1a1  B[5]=6999bcc5  C[5]=229b17f9  D[5]=d467d26a
A[6]=d2e027f6  B[6]=a1222c49  C[6]=69c1571f  D[6]=455d1644
A[7]=a18aceb2  B[7]=94968e29  C[7]=6717ba2c  D[7]=c57e4078

Step 31: (r= 9, s=15)
A[0]=1690779d  B[0]=cfcd8e50  C[0]=4bef64d1  D[0]=794347e4
A[1]=51efdb8f  B[1]=aff3d50f  C[1]=a3bb4179  D[1]=4460bab6
A[2]=a96bc307  B[2]=fc7dc951  C[2]=d09b1530  D[2]=3a212dd0
A[3]=0b8f69c3  B[3]=e84636a6  C[3]=c3065c29  D[3]=e2978d05
A[4]=a4f0e635  B[4]=ed07cec9  C[4]=cc0f5c53  D[4]=a2933431
A[5]=4a671c9b  B[5]=2f834221  C[5]=6999bcc5  D[5]=229b17f9
A[6]=1536b77b  B[6]=c04feda5  C[6]=a1222c49  D[6]=69c1571f
A[7]=821c4b16  B[7]=159d6543  C[7]=94968e29  D[7]=6717ba2c

Feed-Forward Step 0: (r=15, s= 5)
A[0]=76a87046  B[0]=3bce8b48  C[0]=cfcd8e50  D[0]=4bef64d1
A[1]=33ff3fb1  B[1]=edc7a8f7  C[1]=aff3d50f  D[1]=a3bb4179
A[2]=ca76740b  B[2]=e183d4b5  C[2]=fc7dc951  D[2]=d09b1530
A[3]=1b48fcb6  B[3]=b4e185c7  C[3]=e84636a6  D[3]=c3065c29
A[4]=3752b18e  B[4]=731ad278  C[4]=ed07cec9  D[4]=cc0f5c53
A[5]=ff32b41d  B[5]=8e4da533  C[5]=2f834221  D[5]=6999bcc5
A[6]=97b8d348  B[6]=5bbd8a9b  C[6]=c04feda5  D[6]=a1222c49
A[7]=bbc1f5f4  B[7]=258b410e  C[7]=159d6543  D[7]=94968e29

Feed-Forward Step 1: (r= 5, s=29)
A[0]=eeb53b08  B[0]=d50e08ce  C[0]=3bce8b48  D[0]=cfcd8e50
A[1]=c11bc045  B[1]=7fe7f626  C[1]=edc7a8f7  D[1]=aff3d50f
A[2]=234dc7ec  B[2]=4ece8179  C[2]=e183d4b5  D[2]=fc7dc951
A[3]=ff022a88  B[3]=691f96c3  C[3]=b4e185c7  D[3]=e84636a6
```

```
A[4]=658353a7  B[4]=ea5631c6  C[4]=731ad278  D[4]=ed07cec9
A[5]=11dbf846  B[5]=e65683bf  C[5]=8e4da533  D[5]=2f834221
A[6]=41d539a3  B[6]=f71a6912  C[6]=5bbd8a9b  D[6]=c04feda5
A[7]=af75b891  B[7]=783ebe97  C[7]=258b410e  D[7]=159d6543

Feed-Forward Step 2: (r=29, s= 9)
A[0]=f07c5c85  B[0]=1dd6a761  C[0]=d50e08ce  D[0]=3bce8b48
A[1]=50d7dcda  B[1]=b8237808  C[1]=7fe7f626  D[1]=edc7a8f7
A[2]=272e3d8c  B[2]=8469b8fd  C[2]=4ece8179  D[2]=e183d4b5
A[3]=291a4c42  B[3]=1fe04551  C[3]=691f96c3  D[3]=b4e185c7
A[4]=dddb62ec  B[4]=ecb06a74  C[4]=ea5631c6  D[4]=731ad278
A[5]=96aebc6c  B[5]=c23b7f08  C[5]=e65683bf  D[5]=8e4da533
A[6]=f8442627  B[6]=683aa734  C[6]=f71a6912  D[6]=5bbd8a9b
A[7]=741c47cb  B[7]=35eeb712  C[7]=783ebe97  D[7]=258b410e

Feed-Forward Step 3: (r= 9, s=15)
A[0]=63de6ad4  B[0]=f8b90be0  C[0]=1dd6a761  D[0]=d50e08ce
A[1]=fccb64c0  B[1]=afb9b4a1  C[1]=b8237808  D[1]=7fe7f626
A[2]=b0b20f57  B[2]=5c7b184e  C[2]=8469b8fd  D[2]=4ece8179
A[3]=36819bf0  B[3]=34988452  C[3]=1fe04551  D[3]=691f96c3
A[4]=e7af3b35  B[4]=b6c5d9bb  C[4]=ecb06a74  D[4]=ea5631c6
A[5]=5c03ca5e  B[5]=5d78d92d  C[5]=c23b7f08  D[5]=e65683bf
A[6]=45478906  B[6]=884c4ff0  C[6]=683aa734  D[6]=f71a6912
A[7]=a0023940  B[7]=388f96e8  C[7]=35eeb712  D[7]=783ebe97
```

Second message block

```
M[  0..  7] = ff ff ff ff ff ff fe 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =  243   52  151  163  238  141  176    4
y[  8.. 15] =  180  170  128   28   36   36  157   38
y[ 16.. 23] =   68  208   55  168  117  214   88  115
y[ 24.. 31] =   88   14   70  255  173  206  169   46
```

```
y[ 32.. 39] =   81  175  138  212   24   95  231  105
y[ 40.. 47] =  163  164  237  239  114   30  101  108
y[ 48.. 55] =  102  116  229   89  170  203   57    2
y[ 56.. 63] =  150  206  145   68  168   96   16  188
y[ 64.. 71] =  210  224  100   35  104  221  190  234
y[ 72.. 79] =  203  159  117   35  162  121   51  137
y[ 80.. 87] =   97   84   41   28  139  160   93  199
y[ 88.. 95] =  238  155  235   82  216  157   67  105
y[ 96..103] =  229  108  176  114  150  225   87  208
y[104..111] =   58   82  135   16    6  210  241  166
y[112..119] =   89  198  134   39   32  224  244  138
y[120..127] =    9  162  101  242  177   36   78  190
y[128..135] =  253  161   80   99   75   12   46   44
y[136..143] =    1  237  214   23  113   75  160  107
y[144..151] =  235   99   19  146  256   79    1  106
y[152..159] =  146   91   23  147  116  103  187  140
y[160..167] =  208  212  231  175  207  151   95    1
y[168..175] =  232   88  172   20   98   63   73   48
y[176..183] =  192  109  121  224  218  244   52   10
y[184..191] =  169   63  154   13   36   77  121  168
y[192..199] =   49  215  209  231   73  167  162   11
y[200..207] =   90   10  183  251  131  157  153  143
y[208..215] =  235  138  164    2  252   99  127   19
y[216..223] =   36   81   41  145    5  224   66  204
y[224..231] =  253  122  184  240  141    0   25  148
y[232..239] =   85  102   83  143   95   63   76    8
y[240..247] =  251   60  249   59   85   46   93  166
y[248..255] =  176  240  243   60  121  113   51  228
```

Intermediate Expanded Message

```
Z[ 0] = 2594f5e2  bc12b366  ac2cf245  02e4c577
        c121c85b  143c5c80  1a041a04  1b76b7bc
Z[ 1] = dc973124  bfaf27bf  e0ed548d  531b3f98
        0a1e3f98  fe8e3296  db25c34c  213ec068
Z[ 2] = c4be3a89  df7baa01  44a71158  4be1ed36
        bccbbc12  f2fef18c  15ae5262  4e0c48fd
Z[ 3] = 53d449b6  4051ebc4  d8fac121  01722931
        db25b2ad  3124af10  4560bfaf  ce230b90
Z[ 4] = e827de09  194b4844  e5fc4b28  ef61cf95
        b92ed8fa  194b548d  5771bb59  a94824db
Z[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
        b64af245  3b42f01a  b7bce25f  4be1306b
Z[ 6] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
        3b4229ea  0b90a7d6  de090456  be3df470
Z[ 7] = d55d4051  1c2fa71d  e8271720  aa01f69b
        bb590681  f52948fd  1a04c630  cf95385e
Z[ 8] = baa0fd1c  478b39d0  08ac3633  1fcc213e
        f18c00b9  109fe0ed  363351a9  4d53b9e7
```

```
Z[ 9] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
        41c3afc9  b082109f  4a6f53d4  ab73cd6a
Z[10] = df7bdc97  c4beed36  b366dbde  00b944a7
        3f98edef  0e74c293  2d8746d2  22b034c1
Z[11] = 4ec5d107  e8275771  f69be3d1  073a2594
        2d87c068  0965b591  37a51a04  bfaf5771
Z[12] = e1a62369  ed36dd50  bef634c1  07f3bb59
        073a410a  fbaaca86  b7bca4f2  ad9eb4d8
Z[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
        3a891a04  af101da1  e827039d  d9b32fb2
Z[14] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
        49b63d6d  ad9e3bfb  2d8744a7  05c836ec
Z[15] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
        f3b7c577  2b5cf5e2  51a95771  eb0b24db
Z[16] = fc84f3ce  45b0a3aa  4155ef73  2812b971
        00dfbced  da8b6f80  626f1f5c  ab81a8e4
Z[17] = ecd63b3c  108d2fe9  ff2165eb  00df4ca8
        9f4f4ca8  14093cfa  650cb6d4  c306b358
Z[18] = d551468f  e95a9857  d47214e8  52c1e95a
        ea39ae1e  b5f5ee94  555e634e  3f9757fb
Z[19] = c76158da  6967e79c  de07b437  2d4c31a7
        b358a2cb  a6479e70  1f5cb279  69670df0
Z[20] = 2aafd70f  d630571c  3f975a98  ad3fc5a3
        4e66d0f6  bf8a65eb  923ead3f  a5682c6d
Z[21] = ecd6547f  aefd23b7  fba59936  6ea15103
        1f5cef73  23b7ecd6  045bdc49  397e3a5d
Z[22] = fc84e79c  c069b971  9af4a2cb  15c74bc9
        4a0b3286  484d95ba  52c1053a  4234f210
Z[23] = fac64d87  f90894db  4a0b1be0  5103f4ad
        b97107d7  f3ce57fb  6967ba50  2c6d43f2
Z[24] = ac602d4c  563dae1e  0a749af4  2654037c
        ee94b437  14091864  41551f5c  5d35211a
Z[25] = 563dd551  9f4fb279  44d1da8b  5c56642d
        4f450c32  a02efe42  59b9d393  9a152812
Z[26] = d8cdb892  b892d8cd  a3aa52c1  00df5b77
        4ca8aefd  116cf052  36e11a22  29d05e14
Z[27] = 5ef3650c  e3414d87  f4add0f6  08b601be
        36e1d393  0b533b3c  431353a0  b279c3e5
Z[28] = db6ae341  e95a1e7d  b19ae0a4  0995ebf7
        08b6aaa2  fac61e7d  a8e46967  9cb29778
Z[29] = 9857492c  01be1864  563dab81  108dcd7a
        468fa726  9e70476e  e341a8e4  d1d55b77
Z[30] = 6a465e14  f131634e  0000e420  a10dd551
        58da476e  9cb20df0  36e1d70f  06f8b0bb
Z[31] = 3444cc9b  336521f9  2812e341  b0bb9857
        f131ad3f  3444f2ef  626f1f5c  e6bdc5a3
```

Expanded Message

```
W[ 0] = e827de09  194b4844  e5fc4b28  ef61cf95
```

```
          b92ed8fa  194b548d  5771bb59  a94824db
W[ 1] = 4e0cebc4  5262c577  e8e0b2ad  dc973edf
          3b4229ea  0b90a7d6  de090456  be3df470
W[ 2] = 2594f5e2  bc12b366  ac2cf245  02e4c577
          c121c85b  143c5c80  1a041a04  1b76b7bc
W[ 3] = c4be3a89  df7baa01  44a71158  4be1ed36
          bccbbc12  f2fef18c  15ae5262  4e0c48fd
W[ 4] = d55d4051  1c2fa71d  e8271720  aa01f69b
          bb590681  f52948fd  1a04c630  cf95385e
W[ 5] = 3cb44619  143c1da1  b9e7aaba  d6164335
          b64af245  3b42f01a  b7bce25f  4be1306b
W[ 6] = 53d449b6  4051ebc4  d8fac121  01722931
          db25b2ad  3124af10  4560bfaf  ce230b90
W[ 7] = dc973124  bfaf27bf  e0ed548d  531b3f98
          0a1e3f98  fe8e3296  db25c34c  213ec068
W[ 8] = 2b5cfbaa  2aa3fa38  213e3d6d  be3d4335
          f3b7c577  2b5cf5e2  51a95771  eb0b24db
W[ 9] = 4ec5d107  e8275771  f69be3d1  073a2594
          2d87c068  0965b591  37a51a04  bfaf5771
W[10] = e1a62369  ed36dd50  bef634c1  07f3bb59
          073a410a  fbaaca86  b7bca4f2  ad9eb4d8
W[11] = baa0fd1c  478b39d0  08ac3633  1fcc213e
          f18c00b9  109fe0ed  363351a9  4d53b9e7
W[12] = 478bf01a  afc90dbb  3917ff47  4c9a00b9
          41c3afc9  b082109f  4a6f53d4  ab73cd6a
W[13] = aa01f01a  0172bccb  478bfc63  0dbb5bc7
          3a891a04  af101da1  e827039d  d9b32fb2
W[14] = df7bdc97  c4beed36  b366dbde  00b944a7
          3f98edef  0e74c293  2d8746d2  22b034c1
W[15] = 582afd1c  f3b7cb3f  0000ac2c  b13b1211
          49b63d6d  ad9e3bfb  2d8744a7  05c836ec
W[16] = ecd63b3c  108d2fe9  ff2165eb  00df4ca8
          9f4f4ca8  14093cfa  650cb6d4  c306b358
W[17] = d551468f  e95a9857  d47214e8  52c1e95a
          ea39ae1e  b5f5ee94  555e634e  3f9757fb
W[18] = fac64d87  f90894db  4a0b1be0  5103f4ad
          b97107d7  f3ce57fb  6967ba50  2c6d43f2
W[19] = 2aafd70f  d630571c  3f975a98  ad3fc5a3
          4e66d0f6  bf8a65eb  923ead3f  a5682c6d
W[20] = fc84e79c  c069b971  9af4a2cb  15c74bc9
          4a0b3286  484d95ba  52c1053a  4234f210
W[21] = ecd6547f  aefd23b7  fba59936  6ea15103
          1f5cef73  23b7ecd6  045bdc49  397e3a5d
W[22] = fc84f3ce  45b0a3aa  4155ef73  2812b971
          00dfbced  da8b6f80  626f1f5c  ab81a8e4
W[23] = c76158da  6967e79c  de07b437  2d4c31a7
          b358a2cb  a6479e70  1f5cb279  69670df0
W[24] = 6a465e14  f131634e  0000e420  a10dd551
          58da476e  9cb20df0  36e1d70f  06f8b0bb
```

```
W[25] = ac602d4c  563dae1e  0a749af4  2654037c
        ee94b437  14091864  41551f5c  5d35211a
W[26] = 563dd551  9f4fb279  44d1da8b  5c56642d
        4f450c32  a02efe42  59b9d393  9a152812
W[27] = 3444cc9b  336521f9  2812e341  b0bb9857
        f131ad3f  3444f2ef  626f1f5c  e6bdc5a3
W[28] = 5ef3650c  e3414d87  f4add0f6  08b601be
        36e1d393  0b533b3c  431353a0  b279c3e5
W[29] = 9857492c  01be1864  563dab81  108dcd7a
        468fa726  9e70476e  e341a8e4  d1d55b77
W[30] = db6ae341  e95a1e7d  b19ae0a4  0995ebf7
        08b6aaa2  fac61e7d  a8e46967  9cb29778
W[31] = d8cdb892  b892d8cd  a3aa52c1  00df5b77
        4ca8aefd  116cf052  36e11a22  29d05e14
```

Feistel Steps

```
IV :
A[0]=63de6ad4  B[0]=f8b90be0  C[0]=1dd6a761  D[0]=d50e08ce
A[1]=fccb64c0  B[1]=afb9b4a1  C[1]=b8237808  D[1]=7fe7f626
A[2]=b0b20f57  B[2]=5c7b184e  C[2]=8469b8fd  D[2]=4ece8179
A[3]=36819bf0  B[3]=34988452  C[3]=1fe04551  D[3]=691f96c3
A[4]=e7af3b35  B[4]=b6c5d9bb  C[4]=ecb06a74  D[4]=ea5631c6
A[5]=5c03ca5e  B[5]=5d78d92d  C[5]=c23b7f08  D[5]=e65683bf
A[6]=45478906  B[6]=884c4ff0  C[6]=683aa734  D[6]=f71a6912
A[7]=a0023940  B[7]=388f96e8  C[7]=35eeb712  D[7]=783ebe97

IV XOR M :
A[0]=9c21952b  B[0]=f8b90be0  C[0]=1dd6a761  D[0]=d50e08ce
A[1]=fc359b3f  B[1]=afb9b4a1  C[1]=b8237808  D[1]=7fe7f626
A[2]=b0b20f57  B[2]=5c7b184e  C[2]=8469b8fd  D[2]=4ece8179
A[3]=36819bf0  B[3]=34988452  C[3]=1fe04551  D[3]=691f96c3
A[4]=e7af3b35  B[4]=b6c5d9bb  C[4]=ecb06a74  D[4]=ea5631c6
A[5]=5c03ca5e  B[5]=5d78d92d  C[5]=c23b7f08  D[5]=e65683bf
A[6]=45478906  B[6]=884c4ff0  C[6]=683aa734  D[6]=f71a6912
A[7]=a0023940  B[7]=388f96e8  C[7]=35eeb712  D[7]=783ebe97

Step  0: (r= 3, s=20)
A[0]=85224ccf  B[0]=e10ca95c  C[0]=f8b90be0  D[0]=1dd6a761
A[1]=c9c0ffce  B[1]=e1acd9ff  C[1]=afb9b4a1  D[1]=b8237808
A[2]=0d0173e9  B[2]=85907abd  C[2]=5c7b184e  D[2]=8469b8fd
A[3]=3029e0df  B[3]=b40cdf81  C[3]=34988452  D[3]=1fe04551
A[4]=23337498  B[4]=3d79d9af  C[4]=b6c5d9bb  D[4]=ecb06a74
A[5]=9307b75c  B[5]=e01e52f2  C[5]=5d78d92d  D[5]=c23b7f08
A[6]=39c93a8a  B[6]=2a3c4832  C[6]=884c4ff0  D[6]=683aa734
A[7]=c681bf89  B[7]=0011ca05  C[7]=388f96e8  D[7]=35eeb712

Step  1: (r=20, s=14)
A[0]=66352976  B[0]=ccf85224  C[0]=e10ca95c  D[0]=f8b90be0
```

```
A[1]=13cebf2e  B[1]=fcec9c0f  C[1]=e1acd9ff  D[1]=afb9b4a1
A[2]=068ec2d5  B[2]=3e90d017  C[2]=85907abd  D[2]=5c7b184e
A[3]=0f18e853  B[3]=0df3029e  C[3]=b40cdf81  D[3]=34988452
A[4]=c426140d  B[4]=49823337  C[4]=3d79d9af  D[4]=b6c5d9bb
A[5]=98f04ead  B[5]=75c9307b  C[5]=e01e52f2  D[5]=5d78d92d
A[6]=47c16eca  B[6]=a8a39c93  C[6]=2a3c4832  D[6]=884c4ff0
A[7]=8341fb8a  B[7]=f89c681b  C[7]=0011ca05  D[7]=388f96e8

Step  2: (r=14, s=27)
A[0]=f5fed4df  B[0]=4a5d998d  C[0]=ccf85224  D[0]=e10ca95c
A[1]=8e985c17  B[1]=afcb84f3  C[1]=fcec9c0f  D[1]=e1acd9ff
A[2]=982d2e52  B[2]=b0b541a3  C[2]=3e90d017  D[2]=85907abd
A[3]=64a7fc13  B[3]=3a14c3c6  C[3]=0df3029e  D[3]=b40cdf81
A[4]=299edfa3  B[4]=85037109  C[4]=49823337  D[4]=3d79d9af
A[5]=f7c95bd4  B[5]=13ab663c  C[5]=75c9307b  D[5]=e01e52f2
A[6]=e623f0a8  B[6]=5bb291f0  C[6]=a8a39c93  D[6]=2a3c4832
A[7]=e8fe4f42  B[7]=7ee2a0d0  C[7]=f89c681b  D[7]=0011ca05

Step  3: (r=27, s= 3)
A[0]=8a88ab94  B[0]=ffaff6a6  C[0]=4a5d998d  D[0]=ccf85224
A[1]=a8668bbc  B[1]=bc74c2e0  C[1]=afcb84f3  D[1]=fcec9c0f
A[2]=4e9c0069  B[2]=94c16972  C[2]=b0b541a3  D[2]=3e90d017
A[3]=61646ca3  B[3]=9b253fe0  C[3]=3a14c3c6  D[3]=0df3029e
A[4]=d9f02d57  B[4]=194cf6fd  C[4]=85037109  D[4]=49823337
A[5]=f1a9f8cf  B[5]=a7be4ade  C[5]=13ab663c  D[5]=75c9307b
A[6]=e92b23ae  B[6]=47311f85  C[6]=5bb291f0  D[6]=a8a39c93
A[7]=d326dabe  B[7]=1747f27a  C[7]=7ee2a0d0  D[7]=f89c681b

Step  4: (r= 3, s=20)
A[0]=22cb2c19  B[0]=54455ca4  C[0]=ffaff6a6  D[0]=4a5d998d
A[1]=b611b4d0  B[1]=43345de5  C[1]=bc74c2e0  D[1]=afcb84f3
A[2]=94cf19ed  B[2]=74e0034a  C[2]=94c16972  D[2]=b0b541a3
A[3]=069f34e0  B[3]=0b23651b  C[3]=9b253fe0  D[3]=3a14c3c6
A[4]=7ea9a839  B[4]=cf816abe  C[4]=194cf6fd  D[4]=85037109
A[5]=14e3549c  B[5]=8d4fc67f  C[5]=a7be4ade  D[5]=13ab663c
A[6]=ffa7b3ad  B[6]=49591d77  C[6]=47311f85  D[6]=5bb291f0
A[7]=808b1700  B[7]=9936d5f6  C[7]=1747f27a  D[7]=7ee2a0d0

Step  5: (r=20, s=14)
A[0]=f5ec0c69  B[0]=c1922cb2  C[0]=54455ca4  D[0]=ffaff6a6
A[1]=6bdd8882  B[1]=4d0b611b  C[1]=43345de5  D[1]=bc74c2e0
A[2]=3f042c89  B[2]=9ed94cf1  C[2]=74e0034a  D[2]=94c16972
A[3]=dc4227ef  B[3]=4e0069f3  C[3]=0b23651b  D[3]=9b253fe0
A[4]=4e62e131  B[4]=8397ea9a  C[4]=cf816abe  D[4]=194cf6fd
A[5]=d7553de8  B[5]=49c14e35  C[5]=8d4fc67f  D[5]=a7be4ade
A[6]=a8950342  B[6]=3adffa7b  C[6]=49591d77  D[6]=47311f85
A[7]=33eca527  B[7]=700808b1  C[7]=9936d5f6  D[7]=1747f27a

Step  6: (r=14, s=27)
```

```
A[0]=0a940f62  B[0]=031a7d7b  C[0]=c1922cb2  D[0]=54455ca4
A[1]=7b0fc9e6  B[1]=62209af7  C[1]=4d0b611b  D[1]=43345de5
A[2]=34de178f  B[2]=0b224fc1  C[2]=9ed94cf1  D[2]=74e0034a
A[3]=1fa12210  B[3]=89fbf710  C[3]=4e0069f3  D[3]=0b23651b
A[4]=b01babb3  B[4]=b84c5398  C[4]=8397ea9a  D[4]=cf816abe
A[5]=68539204  B[5]=4f7a35d5  C[5]=49c14e35  D[5]=8d4fc67f
A[6]=9fcc12cc  B[6]=40d0aa25  C[6]=3adffa7b  D[6]=49591d77
A[7]=0bcf3999  B[7]=2949ccfb  C[7]=700808b1  D[7]=9936d5f6

Step  7: (r=27, s= 3)
A[0]=40f6b72e  B[0]=1054a07b  C[0]=031a7d7b  D[0]=c1922cb2
A[1]=92bd196b  B[1]=33d87e4f  C[1]=62209af7  D[1]=4d0b611b
A[2]=0a3b9d59  B[2]=79a6f0bc  C[2]=0b224fc1  D[2]=9ed94cf1
A[3]=375eb7e7  B[3]=80fd0910  C[3]=89fbf710  D[3]=4e0069f3
A[4]=5e514fff  B[4]=9d80dd5d  C[4]=b84c5398  D[4]=8397ea9a
A[5]=dd60f7a5  B[5]=23429c90  C[5]=4f7a35d5  D[5]=49c14e35
A[6]=7483ca3d  B[6]=64fe6096  C[6]=40d0aa25  D[6]=3adffa7b
A[7]=9ef201cf  B[7]=c85e79cc  C[7]=2949ccfb  D[7]=700808b1

Step  8: (r=26, s= 4)
A[0]=b30c01e4  B[0]=b903dadc  C[0]=1054a07b  D[0]=031a7d7b
A[1]=5d833e0a  B[1]=ae4af465  C[1]=33d87e4f  D[1]=62209af7
A[2]=30834a4b  B[2]=6428ee75  C[2]=79a6f0bc  D[2]=0b224fc1
A[3]=b7d7d1fe  B[3]=9cdd7adf  C[3]=80fd0910  D[3]=89fbf710
A[4]=cd365ac1  B[4]=fd79453f  C[4]=9d80dd5d  D[4]=b84c5398
A[5]=8506d3b6  B[5]=977583de  C[5]=23429c90  D[5]=4f7a35d5
A[6]=5436e816  B[6]=f5d20f28  C[6]=64fe6096  D[6]=40d0aa25
A[7]=3cc1c7a8  B[7]=3e7bc807  C[7]=c85e79cc  D[7]=2949ccfb

Step  9: (r= 4, s=23)
A[0]=b8b63d2a  B[0]=30c01e4b  C[0]=b903dadc  D[0]=1054a07b
A[1]=d439711e  B[1]=d833e0a5  C[1]=ae4af465  D[1]=33d87e4f
A[2]=74758fe2  B[2]=0834a4b3  C[2]=6428ee75  D[2]=79a6f0bc
A[3]=9946fa5f  B[3]=7d7d1feb  C[3]=9cdd7adf  D[3]=80fd0910
A[4]=d25043d1  B[4]=d365ac1c  C[4]=fd79453f  D[4]=9d80dd5d
A[5]=4a1c8cc0  B[5]=506d3b68  C[5]=977583de  D[5]=23429c90
A[6]=285c5402  B[6]=436e8165  C[6]=f5d20f28  D[6]=64fe6096
A[7]=a8dfe7f6  B[7]=cc1c7a83  C[7]=3e7bc807  D[7]=c85e79cc

Step 10: (r=23, s=11)
A[0]=e06a810e  B[0]=955c5b1e  C[0]=30c01e4b  D[0]=b903dadc
A[1]=1b144f06  B[1]=8f6a1cb8  C[1]=d833e0a5  D[1]=ae4af465
A[2]=3076b00c  B[2]=f13a3ac7  C[2]=0834a4b3  D[2]=6428ee75
A[3]=57e2cd57  B[3]=2fcca37d  C[3]=7d7d1feb  D[3]=9cdd7adf
A[4]=50e1d09e  B[4]=e8e92821  C[4]=d365ac1c  D[4]=fd79453f
A[5]=c4cde269  B[5]=60250e46  C[5]=506d3b68  D[5]=977583de
A[6]=d7efa44c  B[6]=01142e2a  C[6]=436e8165  D[6]=f5d20f28
A[7]=622593bf  B[7]=fb546ff3  C[7]=cc1c7a83  D[7]=3e7bc807
```

```
Step 11: (r=11, s=26)
A[0]=2a96a664  B[0]=54087703  C[0]=955c5b1e  D[0]=30c01e4b
A[1]=ca173591  B[1]=a27830d8  C[1]=8f6a1cb8  D[1]=d833e0a5
A[2]=fbb68424  B[2]=b5806183  C[2]=f13a3ac7  D[2]=0834a4b3
A[3]=985017d1  B[3]=166ababf  C[3]=2fcca37d  D[3]=7d7d1feb
A[4]=36d420ca  B[4]=0e84f287  C[4]=e8e92821  D[4]=d365ac1c
A[5]=d2591ad8  B[5]=6f134e26  C[5]=60250e46  D[5]=506d3b68
A[6]=9e34879a  B[6]=7d2266bf  C[6]=01142e2a  D[6]=436e8165
A[7]=9c526a75  B[7]=2c9dfb11  C[7]=fb546ff3  D[7]=cc1c7a83

Step 12: (r=26, s= 4)
A[0]=0db0b38e  B[0]=90aa5a99  C[0]=54087703  D[0]=955c5b1e
A[1]=b81c8a1a  B[1]=47285cd6  C[1]=a27830d8  D[1]=8f6a1cb8
A[2]=764d8872  B[2]=93eeda10  C[2]=b5806183  D[2]=f13a3ac7
A[3]=19ec242e  B[3]=4661405f  C[3]=166ababf  D[3]=2fcca37d
A[4]=a2212aef  B[4]=28db5083  C[4]=0e84f287  D[4]=e8e92821
A[5]=58e0f559  B[5]=6349646b  C[5]=6f134e26  D[5]=60250e46
A[6]=879108e3  B[6]=6a78d21e  C[6]=7d2266bf  D[6]=01142e2a
A[7]=a8c40801  B[7]=d67149a9  C[7]=2c9dfb11  D[7]=fb546ff3

Step 13: (r= 4, s=23)
A[0]=c6828a86  B[0]=db0b38e0  C[0]=90aa5a99  D[0]=54087703
A[1]=cd5bcd5a  B[1]=81c8a1ab  C[1]=47285cd6  D[1]=a27830d8
A[2]=7983825f  B[2]=64d88727  C[2]=93eeda10  D[2]=b5806183
A[3]=437299ba  B[3]=9ec242e1  C[3]=4661405f  D[3]=166ababf
A[4]=cf378812  B[4]=2212aefa  C[4]=28db5083  D[4]=0e84f287
A[5]=b57dbb62  B[5]=8e0f5595  C[5]=6349646b  D[5]=6f134e26
A[6]=653ee4b4  B[6]=79108e38  C[6]=6a78d21e  D[6]=7d2266bf
A[7]=e1504409  B[7]=8c40801a  C[7]=d67149a9  D[7]=2c9dfb11

Step 14: (r=23, s=11)
A[0]=78617852  B[0]=43634145  C[0]=db0b38e0  D[0]=90aa5a99
A[1]=5991e0d5  B[1]=ad66ade6  C[1]=81c8a1ab  D[1]=47285cd6
A[2]=3f5685b2  B[2]=2fbcc1c1  C[2]=64d88727  D[2]=93eeda10
A[3]=3b6aa6b0  B[3]=dd21b94c  C[3]=9ec242e1  D[3]=4661405f
A[4]=6869fd0d  B[4]=09679bc4  C[4]=2212aefa  D[4]=28db5083
A[5]=dbeda2e7  B[5]=b15abedd  C[5]=8e0f5595  D[5]=6349646b
A[6]=c1051685  B[6]=5a329f72  C[6]=79108e38  D[6]=6a78d21e
A[7]=36e219e1  B[7]=04f0a822  C[7]=8c40801a  D[7]=d67149a9

Step 15: (r=11, s=26)
A[0]=24f94e82  B[0]=0bc293c3  C[0]=43634145  D[0]=db0b38e0
A[1]=6029c206  B[1]=8f06aacc  C[1]=ad66ade6  D[1]=81c8a1ab
A[2]=a7c35e37  B[2]=b42d91fa  C[2]=2fbcc1c1  D[2]=64d88727
A[3]=532b058c  B[3]=553581db  C[3]=dd21b94c  D[3]=9ec242e1
A[4]=fe2e68f9  B[4]=4fe86b43  C[4]=09679bc4  D[4]=2212aefa
A[5]=7db78828  B[5]=6d173edf  C[5]=b15abedd  D[5]=8e0f5595
A[6]=8bf1d4cd  B[6]=28b42e08  C[6]=5a329f72  D[6]=79108e38
A[7]=34b9e9fd  B[7]=10cf09b7  C[7]=04f0a822  D[7]=8c40801a
```

```
Step 16: (r=19, s=28)
A[0]=40ed38cc  B[0]=741127ca  C[0]=0bc293c3  D[0]=43634145
A[1]=f60aefe1  B[1]=1033014e  C[1]=8f06aacc  D[1]=ad66ade6
A[2]=6d661148  B[2]=f1bd3e1a  C[2]=b42d91fa  D[2]=2fbcc1c1
A[3]=098972af  B[3]=2c629958  C[3]=553581db  D[3]=dd21b94c
A[4]=b250ad2a  B[4]=47cff173  C[4]=4fe86b43  D[4]=09679bc4
A[5]=10c76e89  B[5]=4143edbc  C[5]=6d173edf  D[5]=b15abedd
A[6]=b3569b13  B[6]=a66c5f8e  C[6]=28b42e08  D[6]=5a329f72
A[7]=3c6d6360  B[7]=4fe9a5cf  C[7]=10cf09b7  D[7]=04f0a822

Step 17: (r=28, s= 7)
A[0]=62ec30c5  B[0]=c40ed38c  C[0]=741127ca  D[0]=0bc293c3
A[1]=d43c5c01  B[1]=1f60aefe  C[1]=1033014e  D[1]=8f06aacc
A[2]=72428586  B[2]=86d66114  C[2]=f1bd3e1a  D[2]=b42d91fa
A[3]=2b7aae44  B[3]=f098972a  C[3]=2c629958  D[3]=553581db
A[4]=004c0c52  B[4]=ab250ad2  C[4]=47cff173  D[4]=4fe86b43
A[5]=55dbfe20  B[5]=910c76e8  C[5]=4143edbc  D[5]=6d173edf
A[6]=e5c5efff  B[6]=3b3569b1  C[6]=a66c5f8e  D[6]=28b42e08
A[7]=4aa17110  B[7]=03c6d636  C[7]=4fe9a5cf  D[7]=10cf09b7

Step 18: (r= 7, s=22)
A[0]=86cf31a3  B[0]=761862b1  C[0]=c40ed38c  D[0]=741127ca
A[1]=205f0c85  B[1]=1e2e00ea  C[1]=1f60aefe  D[1]=1033014e
A[2]=2b9f9e24  B[2]=2142c339  C[2]=86d66114  D[2]=f1bd3e1a
A[3]=8e38bd83  B[3]=bd572215  C[3]=f098972a  D[3]=2c629958
A[4]=e0ab5a70  B[4]=26062900  C[4]=ab250ad2  D[4]=47cff173
A[5]=c6df3ebc  B[5]=edff102a  C[5]=910c76e8  D[5]=4143edbc
A[6]=a09b5342  B[6]=e2f7fff2  C[6]=3b3569b1  D[6]=a66c5f8e
A[7]=1829a3f9  B[7]=50b88825  C[7]=03c6d636  D[7]=4fe9a5cf

Step 19: (r=22, s=19)
A[0]=a86f5125  B[0]=68e1b3cc  C[0]=761862b1  D[0]=c40ed38c
A[1]=8a51e45e  B[1]=214817c3  C[1]=1e2e00ea  D[1]=1f60aefe
A[2]=afbedb8f  B[2]=890ae7e7  C[2]=2142c339  D[2]=86d66114
A[3]=076cbbfc  B[3]=60e38e2f  C[3]=bd572215  D[3]=f098972a
A[4]=c03fbdb2  B[4]=9c382ad6  C[4]=26062900  D[4]=ab250ad2
A[5]=41c6cd30  B[5]=af31b7cf  C[5]=edff102a  D[5]=910c76e8
A[6]=cf128afb  B[6]=d0a826d4  C[6]=e2f7fff2  D[6]=3b3569b1
A[7]=93fbd834  B[7]=fe460a68  C[7]=50b88825  D[7]=03c6d636

Step 20: (r=19, s=28)
A[0]=f584257b  B[0]=892d437a  C[0]=68e1b3cc  D[0]=761862b1
A[1]=27ce6a4d  B[1]=22f4528f  C[1]=214817c3  D[1]=1e2e00ea
A[2]=cc8d97dd  B[2]=dc7d7df6  C[2]=890ae7e7  D[2]=2142c339
A[3]=df39f6c9  B[3]=dfe03b65  C[3]=60e38e2f  D[3]=bd572215
A[4]=1118f4a4  B[4]=ed9601fd  C[4]=9c382ad6  D[4]=26062900
A[5]=ba0b1c19  B[5]=69820e36  C[5]=af31b7cf  D[5]=edff102a
A[6]=96af31bb  B[6]=57de7894  C[6]=d0a826d4  D[6]=e2f7fff2
```

```
A[7]=f96ddd9a  B[7]=c1a49fde  C[7]=fe460a68  D[7]=50b88825

Step 21: (r=28, s= 7)
A[0]=26b62ea3  B[0]=bf584257  C[0]=892d437a  D[0]=68e1b3cc
A[1]=19af57e4  B[1]=d27ce6a4  C[1]=22f4528f  D[1]=214817c3
A[2]=3a8275cb  B[2]=dcc8d97d  C[2]=dc7d7df6  D[2]=890ae7e7
A[3]=bf95a929  B[3]=9df39f6c  C[3]=dfe03b65  D[3]=60e38e2f
A[4]=f707a70c  B[4]=41118f4a  C[4]=ed9601fd  D[4]=9c382ad6
A[5]=0ca46db7  B[5]=9ba0b1c1  C[5]=69820e36  D[5]=af31b7cf
A[6]=4217f729  B[6]=b96af31b  C[6]=57de7894  D[6]=d0a826d4
A[7]=6951e002  B[7]=af96ddd9  C[7]=c1a49fde  D[7]=fe460a68

Step 22: (r= 7, s=22)
A[0]=2c3529ee  B[0]=5b175193  C[0]=bf584257  D[0]=892d437a
A[1]=905a11e5  B[1]=d7abf20c  C[1]=d27ce6a4  D[1]=22f4528f
A[2]=a8a0a5db  B[2]=413ae59d  C[2]=dcc8d97d  D[2]=dc7d7df6
A[3]=471dc07b  B[3]=cad494df  C[3]=9df39f6c  D[3]=dfe03b65
A[4]=8eb520ba  B[4]=83d3867b  C[4]=41118f4a  D[4]=ed9601fd
A[5]=82dfbcf2  B[5]=5236db86  C[5]=9ba0b1c1  D[5]=69820e36
A[6]=2a0d8f9a  B[6]=0bfb94a1  C[6]=b96af31b  D[6]=57de7894
A[7]=a4bc28b7  B[7]=a8f00134  C[7]=af96ddd9  D[7]=c1a49fde

Step 23: (r=22, s=19)
A[0]=20002a66  B[0]=7b8b0d4a  C[0]=5b175193  D[0]=bf584257
A[1]=a31baea8  B[1]=79641684  C[1]=d7abf20c  D[1]=d27ce6a4
A[2]=a6de9cd3  B[2]=76ea2829  C[2]=413ae59d  D[2]=dcc8d97d
A[3]=3a48171a  B[3]=1ed1c770  C[3]=cad494df  D[3]=9df39f6c
A[4]=d59c314b  B[4]=2ea3ad48  C[4]=83d3867b  D[4]=41118f4a
A[5]=aca92a87  B[5]=3ca0b7ef  C[5]=5236db86  D[5]=9ba0b1c1
A[6]=8c2f3d5f  B[6]=e68a8363  C[6]=0bfb94a1  D[6]=b96af31b
A[7]=daf0856d  B[7]=2de92f0a  C[7]=a8f00134  D[7]=af96ddd9

Step 24: (r=15, s= 5)
A[0]=6e139961  B[0]=15331000  C[0]=7b8b0d4a  D[0]=5b175193
A[1]=3f071ec7  B[1]=d754518d  C[1]=79641684  D[1]=d7abf20c
A[2]=a211f26c  B[2]=4e69d36f  C[2]=76ea2829  D[2]=413ae59d
A[3]=892965b2  B[3]=0b8d1d24  C[3]=1ed1c770  D[3]=cad494df
A[4]=ab339c68  B[4]=18a5eace  C[4]=2ea3ad48  D[4]=83d3867b
A[5]=f9dc51e4  B[5]=9543d654  C[5]=3ca0b7ef  D[5]=5236db86
A[6]=47a06f27  B[6]=9eafc617  C[6]=e68a8363  D[6]=0bfb94a1
A[7]=8ca23bb2  B[7]=42b6ed78  C[7]=2de92f0a  D[7]=a8f00134

Step 25: (r= 5, s=29)
A[0]=65e09ff1  B[0]=c2732c2d  C[0]=15331000  D[0]=7b8b0d4a
A[1]=15d66c66  B[1]=e0e3d8e7  C[1]=d754518d  D[1]=79641684
A[2]=96c6978c  B[2]=423e4d94  C[2]=4e69d36f  D[2]=76ea2829
A[3]=43041cde  B[3]=252cb651  C[3]=0b8d1d24  D[3]=1ed1c770
A[4]=43ef2167  B[4]=66738d15  C[4]=18a5eace  D[4]=2ea3ad48
A[5]=d3bb9398  B[5]=3b8a3c9f  C[5]=9543d654  D[5]=3ca0b7ef
```

```
A[6]=04f2fc5d  B[6]=f40de4e8  C[6]=9eafc617  D[6]=e68a8363
A[7]=008c468f  B[7]=94477651  C[7]=42b6ed78  D[7]=2de92f0a

Step 26: (r=29, s= 9)
A[0]=57ef0115  B[0]=2cbc13fe  C[0]=c2732c2d  D[0]=15331000
A[1]=8ce43941  B[1]=c2bacd8c  C[1]=e0e3d8e7  D[1]=d754518d
A[2]=f108a87e  B[2]=92d8d2f1  C[2]=423e4d94  D[2]=4e69d36f
A[3]=52ffff35  B[3]=c860839b  C[3]=252cb651  D[3]=0b8d1d24
A[4]=616a934b  B[4]=e87de42c  C[4]=66738d15  D[4]=18a5eace
A[5]=c6eeeeda  B[5]=1a777273  C[5]=3b8a3c9f  D[5]=9543d654
A[6]=67354f48  B[6]=a09e5f8b  C[6]=f40de4e8  D[6]=9eafc617
A[7]=97492e12  B[7]=e01188d1  C[7]=94477651  D[7]=42b6ed78

Step 27: (r= 9, s=15)
A[0]=da127ddc  B[0]=de022aaf  C[0]=2cbc13fe  D[0]=c2732c2d
A[1]=7c742b3b  B[1]=c8728319  C[1]=c2bacd8c  D[1]=e0e3d8e7
A[2]=28ee952b  B[2]=1150fde2  C[2]=92d8d2f1  D[2]=423e4d94
A[3]=2ec23602  B[3]=fffe6aa5  C[3]=c860839b  D[3]=252cb651
A[4]=7016e2d7  B[4]=d52696c2  C[4]=e87de42c  D[4]=66738d15
A[5]=663f8590  B[5]=ddddb58d  C[5]=1a777273  D[5]=3b8a3c9f
A[6]=fbded67f  B[6]=6a9e90ce  C[6]=a09e5f8b  D[6]=f40de4e8
A[7]=05b4bf63  B[7]=925c252e  C[7]=e01188d1  D[7]=94477651

Step 28: (r=15, s= 5)
A[0]=04b76539  B[0]=3eee6d09  C[0]=de022aaf  D[0]=2cbc13fe
A[1]=d1e49dfa  B[1]=159dbe3a  C[1]=c8728319  D[1]=c2bacd8c
A[2]=139fa509  B[2]=4a959477  C[2]=1150fde2  D[2]=92d8d2f1
A[3]=e330e6ba  B[3]=1b011761  C[3]=fffe6aa5  D[3]=c860839b
A[4]=745120f0  B[4]=716bb80b  C[4]=d52696c2  D[4]=e87de42c
A[5]=1d11659f  B[5]=c2c8331f  C[5]=ddddb58d  D[5]=1a777273
A[6]=97b36dbe  B[6]=6b3ffdef  C[6]=6a9e90ce  D[6]=a09e5f8b
A[7]=45fcf127  B[7]=5fb182da  C[7]=925c252e  D[7]=e01188d1

Step 29: (r= 5, s=29)
A[0]=f06bda6c  B[0]=96eca720  C[0]=3eee6d09  D[0]=de022aaf
A[1]=b8ea8801  B[1]=3c93bf5a  C[1]=159dbe3a  D[1]=c8728319
A[2]=56822d9a  B[2]=73f4a122  C[2]=4a959477  D[2]=1150fde2
A[3]=17179650  B[3]=661cd75c  C[3]=1b011761  D[3]=fffe6aa5
A[4]=8afbdf54  B[4]=8a241e0e  C[4]=716bb80b  D[4]=d52696c2
A[5]=d27642d8  B[5]=a22cb3e3  C[5]=c2c8331f  D[5]=ddddb58d
A[6]=48181ed9  B[6]=f66db7d2  C[6]=6b3ffdef  D[6]=6a9e90ce
A[7]=63692491  B[7]=bf9e24e8  C[7]=5fb182da  D[7]=925c252e

Step 30: (r=29, s= 9)
A[0]=e4675572  B[0]=9e0d7b4d  C[0]=96eca720  D[0]=3eee6d09
A[1]=f9c265b7  B[1]=371d5100  C[1]=3c93bf5a  D[1]=159dbe3a
A[2]=1b563886  B[2]=4ad045b3  C[2]=73f4a122  D[2]=4a959477
A[3]=e53b542b  B[3]=02e2f2ca  C[3]=661cd75c  D[3]=1b011761
A[4]=94a1d79a  B[4]=915f7bea  C[4]=8a241e0e  D[4]=716bb80b
```

```
A[5]=6ae010e9  B[5]=1a4ec85b  C[5]=a22cb3e3  D[5]=c2c8331f
A[6]=b89171fb  B[6]=290303db  C[6]=f66db7d2  D[6]=6b3ffdef
A[7]=2dd078aa  B[7]=2c6d2492  C[7]=bf9e24e8  D[7]=5fb182da

Step 31: (r= 9, s=15)
A[0]=122d0c3d  B[0]=ceaae5c8  C[0]=9e0d7b4d  D[0]=96eca720
A[1]=c62e58b7  B[1]=84cb6ff3  C[1]=371d5100  D[1]=3c93bf5a
A[2]=27511c7b  B[2]=ac710c36  C[2]=4ad045b3  D[2]=73f4a122
A[3]=45829568  B[3]=76a857ca  C[3]=02e2f2ca  D[3]=661cd75c
A[4]=b1f40ce4  B[4]=43af3529  C[4]=915f7bea  D[4]=8a241e0e
A[5]=5ef9ef43  B[5]=c021d2d5  C[5]=1a4ec85b  D[5]=a22cb3e3
A[6]=d2673947  B[6]=22e3f771  C[6]=290303db  D[6]=f66db7d2
A[7]=7974b379  B[7]=a0f1545b  C[7]=2c6d2492  D[7]=bf9e24e8

Feed-Forward Step 0: (r=15, s= 5)
A[0]=4acd0aa8  B[0]=861e8916  C[0]=ceaae5c8  D[0]=9e0d7b4d
A[1]=556c42d3  B[1]=2c5be317  C[1]=84cb6ff3  D[1]=371d5100
A[2]=79b3e833  B[2]=8e3d93a8  C[2]=ac710c36  D[2]=4ad045b3
A[3]=fe1af684  B[3]=4ab422c1  C[3]=76a857ca  D[3]=02e2f2ca
A[4]=67fbbd2a  B[4]=067258fa  C[4]=43af3529  D[4]=915f7bea
A[5]=d17a6c41  B[5]=f7a1af7c  C[5]=c021d2d5  D[5]=1a4ec85b
A[6]=3ccb52e6  B[6]=9ca3e933  C[6]=22e3f771  D[6]=290303db
A[7]=1fd249a3  B[7]=59bcbcba  C[7]=a0f1545b  D[7]=2c6d2492

Feed-Forward Step 1: (r= 5, s=29)
A[0]=da1bb4fc  B[0]=59a15509  C[0]=861e8916  D[0]=ceaae5c8
A[1]=50d31f39  B[1]=ad885a6a  C[1]=2c5be317  D[1]=84cb6ff3
A[2]=0018f14d  B[2]=367d066f  C[2]=8e3d93a8  D[2]=ac710c36
A[3]=7dcdcdc6  B[3]=c35ed09f  C[3]=4ab422c1  D[3]=76a857ca
A[4]=a33dca81  B[4]=ff77a54c  C[4]=067258fa  D[4]=43af3529
A[5]=8366606e  B[5]=2f4d883a  C[5]=f7a1af7c  D[5]=c021d2d5
A[6]=d9760c6b  B[6]=996a5cc7  C[6]=9ca3e933  D[6]=22e3f771
A[7]=b3234348  B[7]=fa493463  C[7]=59bcbcba  D[7]=a0f1545b

Feed-Forward Step 2: (r=29, s= 9)
A[0]=23b8cefa  B[0]=9b43769f  C[0]=59a15509  D[0]=861e8916
A[1]=6af3145f  B[1]=2a1a63e7  C[1]=ad885a6a  D[1]=2c5be317
A[2]=fffd0d8b  B[2]=a0031e29  C[2]=367d066f  D[2]=8e3d93a8
A[3]=3f66ff04  B[3]=cfb9b9b8  C[3]=c35ed09f  D[3]=4ab422c1
A[4]=7e19e967  B[4]=3467b950  C[4]=ff77a54c  D[4]=067258fa
A[5]=e5c54e1d  B[5]=d06ccc0d  C[5]=2f4d883a  D[5]=f7a1af7c
A[6]=2f325439  B[6]=7b2ec18d  C[6]=996a5cc7  D[6]=9ca3e933
A[7]=96d43641  B[7]=16646869  C[7]=fa493463  D[7]=59bcbcba

Feed-Forward Step 3: (r= 9, s=15)
A[0]=2892aa12  B[0]=719df447  C[0]=9b43769f  D[0]=59a15509
A[1]=9c6e697a  B[1]=e628bed5  C[1]=2a1a63e7  D[1]=ad885a6a
A[2]=f66fb0e4  B[2]=fa1b17ff  C[2]=a0031e29  D[2]=367d066f
A[3]=e1fc44b3  B[3]=cdfe087e  C[3]=cfb9b9b8  D[3]=c35ed09f
```

```
A[4]=8da2475f  B[4]=33d2cefc  C[4]=3467b950  D[4]=ff77a54c
A[5]=65de12f7  B[5]=8a9c3bcb  C[5]=d06ccc0d  D[5]=2f4d883a
A[6]=47a53f93  B[6]=64a8725e  C[6]=7b2ec18d  D[6]=996a5cc7
A[7]=1bd830a2  B[7]=a86c832d  C[7]=16646869  D[7]=fa493463
```

Compression Function Output

```
A[0]=2892aa12  B[0]=719df447  C[0]=9b43769f  D[0]=59a15509
A[1]=9c6e697a  B[1]=e628bed5  C[1]=2a1a63e7  D[1]=ad885a6a
A[2]=f66fb0e4  B[2]=fa1b17ff  C[2]=a0031e29  D[2]=367d066f
A[3]=e1fc44b3  B[3]=cdfe087e  C[3]=cfb9b9b8  D[3]=c35ed09f
A[4]=8da2475f  B[4]=33d2cefc  C[4]=3467b950  D[4]=ff77a54c
A[5]=65de12f7  B[5]=8a9c3bcb  C[5]=d06ccc0d  D[5]=2f4d883a
A[6]=47a53f93  B[6]=64a8725e  C[6]=7b2ec18d  D[6]=996a5cc7
A[7]=1bd830a2  B[7]=a86c832d  C[7]=16646869  D[7]=fa493463
```

Final block

```
M[  0..  7] = 37 04 00 00 00 00 00 00
M[  8.. 15] = 00 00 00 00 00 00 00 00
M[ 16.. 23] = 00 00 00 00 00 00 00 00
M[ 24.. 31] = 00 00 00 00 00 00 00 00
M[ 32.. 39] = 00 00 00 00 00 00 00 00
M[ 40.. 47] = 00 00 00 00 00 00 00 00
M[ 48.. 55] = 00 00 00 00 00 00 00 00
M[ 56.. 63] = 00 00 00 00 00 00 00 00
M[ 64.. 71] = 00 00 00 00 00 00 00 00
M[ 72.. 79] = 00 00 00 00 00 00 00 00
M[ 80.. 87] = 00 00 00 00 00 00 00 00
M[ 88.. 95] = 00 00 00 00 00 00 00 00
M[ 96..103] = 00 00 00 00 00 00 00 00
M[104..111] = 00 00 00 00 00 00 00 00
M[112..119] = 00 00 00 00 00 00 00 00
M[120..127] = 00 00 00 00 00 00 00 00
```

NTT Output

```
y[  0..  7] =   61  165  253   25  100  103   38  217
y[  8.. 15] =   83  222  217   81  155  191  230   68
y[ 16.. 23] =  160   84  131  211  120  256   67  256
y[ 24.. 31] =   70  153   56  134  184   54   47  116
y[ 32.. 39] =    3  142  144  243   16   32   20   71
y[ 40.. 47] =   63   73  194  216  243  207  172  210
y[ 48.. 55] =  183  243   53   83  146   42  138  255
y[ 56.. 63] =  108  123  230   72  215  135    9   14
y[ 64.. 71] =  119  197   87   94   48   28  240   38
y[ 72.. 79] =   57  190   59  107  148  226  117  121
y[ 80.. 87] =  177  224  217  112   89  175   90   39
y[ 88.. 95] =   72  226   62  109  209  193  100  189
y[ 96..103] =  243  143  181  173  213  195   59  237
```

```
y[104..111] =  200   30   90  227   52  251   86   58
y[112..119] =   43   98  145   86  103  101  123  134
y[120..127] =   12   87   90  153  210  217   69   88
y[128..135] =   49  202  114   85   10    7   72  150
y[136..143] =   27  145  150   29  212  176  137   42
y[144..151] =  207   26  236  156  247  111   43  111
y[152..159] =   40  214   54  233  183   56   63  251
y[160..167] =  107  225  223  124   94   78   90   39
y[168..175] =   47   37  173  151  124  160  195  157
y[176..183] =  184  124   57   27  221   68  229  112
y[184..191] =    2  244  137   38  152  232  101   96
y[192..199] =  248  170   23   16   62   82  127   72
y[200..207] =   53  177   51    3  219  141  250  246
y[208..215] =  190  143  150  255   21  192   20   71
y[216..223] =   38  141   48    1  158  174   10  178
y[224..231] =  124  224  186  194  154  172   51  130
y[232..239] =  167   80   20  140   58  116   24   52
y[240..247] =   67   12  222   24    7    9  244  233
y[248..255] =   98   23   20  214  157  150   41   22
```

Intermediate Expanded Message

```
Z[ 0] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
Z[ 1] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
        b4d83296  a71d2878  2706cb3f  53d421f7
Z[ 2] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
Z[ 3] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
        58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
Z[ 4] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
Z[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
        e9993408  4ec52cce  d1c0dd50  cedc4844
Z[ 6] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
Z[ 7] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
        3edf08ac  b4d8410a  e318de09  3f9831dd
Z[ 8] = d8412369  3d6d5262  050f073a  b2ad3408
        af101383  14f5b2ad  c577df7b  1e5aa948
Z[ 9] = 12cadbde  b703f0d3  5037f8c6  50371f13
        e0ed1ce8  eea82706  2878ca86  fbaa2d87
Z[10] = e8e04d53  599ce76e  385e43ee  1c2f410a
        1abd21f7  b366c34c  b9e7599c  b7bcd332
Z[11] = 599ccb3f  13832931  3124e5fc  50f0ebc4
        f69b0172  1b76a948  edefb41f  456048fd
Z[12] = c121f97f  0b90109f  3b422cce  34085bc7
        c630264d  022b24db  ac2ce48a  f80dfaf1
Z[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
```

```
        ac2c1b76  00b922b0  c405b875  c6e9073a
Z[14] = e827599c  d279ccb1  c293b591  a43924db
        39d0bef6  ab730e74  53d429ea  25941158
Z[15] = 08ac306b  1158e6b5  0681050f  eea8f69b
        109f46d2  e0ed0e74  b2adb7bc  0fe61da1
Z[16] = 2aaf3523  634efc84  08b6571c  3eb8211a
        1785484d  a2cbdd28  d8cda726  9778e87b
Z[17] = d472ab81  edb5923e  f74a6888  25753a5d
        22d83cfa  2f0a30c8  bf8ac069  36e128f1
Z[18] = 5d35029d  e2629d91  51e20df0  4e66116c
        28f136e1  b6d4c91f  6c04f3ce  c9feb5f5
Z[19] = c069bf8a  31a72e2b  e0a49f4f  e79c9857
        01be5e14  9778e87b  a489db6a  57fb07d7
Z[20] = f82967a9  14094bc9  360229d0  6ea1f131
        2e2b31a7  2c6d3365  dee6a10d  f9e765eb
Z[21] = c5a3ba50  a2cbdd28  124b4d87  116c4e66
        211a3eb8  29d03602  a9c3d630  08b6571c
Z[22] = 6c04f3ce  c227bdcc  a647d9ac  2c6d3365
        b19ace59  116c4e66  32862d4c  14e84aea
Z[23] = 3a5d2575  e1839e70  061959b9  f4ad6b25
        555e0a74  116c4e66  a8e4d70f  23b73c1b
Z[24] = d017afdc  4a0b15c7  061959b9  a2cbdd28
        9e70e183  1943468f  b971c682  24963b3c
Z[25] = 16a6492c  a805d7ee  60b1ff21  60b1ff21
        da8ba568  eb1894db  30c82f0a  fac6650c
Z[26] = e4209bd3  6c04f3ce  43f21be0  21f93dd9
        203b3f97  a3aadc49  ab81d472  a8e4d70f
Z[27] = 6c04f3ce  1785484d  3b3c2496  6190fe42
        f4ad6b25  211a3eb8  ea3995ba  53a00c32
Z[28] = b437cbbc  0df051e2  476e1864  3eb8211a
        ba50c5a3  029d5d35  9af4e4ff  f66b6967
Z[29] = 9cb2e341  fe426190  c761b892  3dd921f9
        9af4e4ff  00df5ef3  b7b3c840  bb2fc4c4
Z[30] = e3419cb2  c91fb6d4  b5f5c9fe  915fee94
        45b01a22  9a15e5de  650cfac6  2d4c3286
Z[31] = 0a74555e  14e84aea  07d757fb  eb1894db
        14094bc9  da8ba568  a2cbdd28  132a4ca8
```

Expanded Message

```
W[ 0] = d4a455ff  43ee3edf  143c22b0  1b76f3b7
        cf952931  4d532aa3  e999b13b  5771548d
W[ 1] = ad9ef5e2  c34cc914  d332e034  f18c2aa3
        15aed6cf  ea52410a  fbaa2594  29ea3e26
W[ 2] = bd842c15  1211fd1c  4a6f4844  e3181b76
        e6b53bfb  3a89e318  d04eb64a  3124ec7d
W[ 3] = ace5022b  f5e2ae57  17200b90  334f0e74
        34c12d87  e25fd279  dbdef5e2  de09c293
W[ 4] = 46d21f13  3e26af10  48fd4a6f  a71d58e3
```

```
          3edf08ac  b4d8410a  e318de09  3f9831dd
W[ 5] = e827c630  50f0e318  c4be4051  1c2f410a
          e9993408  4ec52cce  d1c0dd50  cedc4844
W[ 6] = f5e2ca86  3bfb264d  1e5aafc9  fe8eaa01
          58e34e0c  3408ec7d  a7d6e1a6  0a1e0681
W[ 7] = 3cb4b9e7  dec2a4f2  ff4756b8  ff47306b
          b4d83296  a71d2878  2706cb3f  53d421f7
W[ 8] = 08ac306b  1158e6b5  0681050f  eea8f69b
          109f46d2  e0ed0e74  b2adb7bc  0fe61da1
W[ 9] = 599ccb3f  13832931  3124e5fc  50f0ebc4
          f69b0172  1b76a948  edefb41f  456048fd
W[10] = c121f97f  0b90109f  3b422cce  34085bc7
          c630264d  022b24db  ac2ce48a  f80dfaf1
W[11] = d8412369  3d6d5262  050f073a  b2ad3408
          af101383  14f5b2ad  c577df7b  1e5aa948
W[12] = 12cadbde  b703f0d3  5037f8c6  50371f13
          e0ed1ce8  eea82706  2878ca86  fbaa2d87
W[13] = ad9ecf95  fe8eb2ad  d1070f2d  334f0e74
          ac2c1b76  00b922b0  c405b875  c6e9073a
W[14] = e8e04d53  599ce76e  385e43ee  1c2f410a
          1abd21f7  b366c34c  b9e7599c  b7bcd332
W[15] = e827599c  d279ccb1  c293b591  a43924db
          39d0bef6  ab730e74  53d429ea  25941158
W[16] = d472ab81  edb5923e  f74a6888  25753a5d
          22d83cfa  2f0a30c8  bf8ac069  36e128f1
W[17] = 5d35029d  e2629d91  51e20df0  4e66116c
          28f136e1  b6d4c91f  6c04f3ce  c9feb5f5
W[18] = 3a5d2575  e1839e70  061959b9  f4ad6b25
          555e0a74  116c4e66  a8e4d70f  23b73c1b
W[19] = f82967a9  14094bc9  360229d0  6ea1f131
          2e2b31a7  2c6d3365  dee6a10d  f9e765eb
W[20] = 6c04f3ce  c227bdcc  a647d9ac  2c6d3365
          b19ace59  116c4e66  32862d4c  14e84aea
W[21] = c5a3ba50  a2cbdd28  124b4d87  116c4e66
          211a3eb8  29d03602  a9c3d630  08b6571c
W[22] = 2aaf3523  634efc84  08b6571c  3eb8211a
          1785484d  a2cbdd28  d8cda726  9778e87b
W[23] = c069bf8a  31a72e2b  e0a49f4f  e79c9857
          01be5e14  9778e87b  a489db6a  57fb07d7
W[24] = e3419cb2  c91fb6d4  b5f5c9fe  915fee94
          45b01a22  9a15e5de  650cfac6  2d4c3286
W[25] = d017afdc  4a0b15c7  061959b9  a2cbdd28
          9e70e183  1943468f  b971c682  24963b3c
W[26] = 16a6492c  a805d7ee  60b1ff21  60b1ff21
          da8ba568  eb1894db  30c82f0a  fac6650c
W[27] = 0a74555e  14e84aea  07d757fb  eb1894db
          14094bc9  da8ba568  a2cbdd28  132a4ca8
W[28] = 6c04f3ce  1785484d  3b3c2496  6190fe42
          f4ad6b25  211a3eb8  ea3995ba  53a00c32
```

```
W[29] = 9cb2e341  fe426190  c761b892  3dd921f9
        9af4e4ff  00df5ef3  b7b3c840  bb2fc4c4
W[30] = b437cbbc  0df051e2  476e1864  3eb8211a
        ba50c5a3  029d5d35  9af4e4ff  f66b6967
W[31] = e4209bd3  6c04f3ce  43f21be0  21f93dd9
        203b3f97  a3aadc49  ab81d472  a8e4d70f
```

Feistel Steps

```
IV :
A[0]=2892aa12  B[0]=719df447  C[0]=9b43769f  D[0]=59a15509
A[1]=9c6e697a  B[1]=e628bed5  C[1]=2a1a63e7  D[1]=ad885a6a
A[2]=f66fb0e4  B[2]=fa1b17ff  C[2]=a0031e29  D[2]=367d066f
A[3]=e1fc44b3  B[3]=cdfe087e  C[3]=cfb9b9b8  D[3]=c35ed09f
A[4]=8da2475f  B[4]=33d2cefc  C[4]=3467b950  D[4]=ff77a54c
A[5]=65de12f7  B[5]=8a9c3bcb  C[5]=d06ccc0d  D[5]=2f4d883a
A[6]=47a53f93  B[6]=64a8725e  C[6]=7b2ec18d  D[6]=996a5cc7
A[7]=1bd830a2  B[7]=a86c832d  C[7]=16646869  D[7]=fa493463

IV XOR M :
A[0]=2892ae25  B[0]=719df447  C[0]=9b43769f  D[0]=59a15509
A[1]=9c6e697a  B[1]=e628bed5  C[1]=2a1a63e7  D[1]=ad885a6a
A[2]=f66fb0e4  B[2]=fa1b17ff  C[2]=a0031e29  D[2]=367d066f
A[3]=e1fc44b3  B[3]=cdfe087e  C[3]=cfb9b9b8  D[3]=c35ed09f
A[4]=8da2475f  B[4]=33d2cefc  C[4]=3467b950  D[4]=ff77a54c
A[5]=65de12f7  B[5]=8a9c3bcb  C[5]=d06ccc0d  D[5]=2f4d883a
A[6]=47a53f93  B[6]=64a8725e  C[6]=7b2ec18d  D[6]=996a5cc7
A[7]=1bd830a2  B[7]=a86c832d  C[7]=16646869  D[7]=fa493463

Step  0: (r= 3, s=20)
A[0]=ddf16d4d  B[0]=44957129  C[0]=719df447  D[0]=9b43769f
A[1]=867eec15  B[1]=e3734bd4  C[1]=e628bed5  D[1]=2a1a63e7
A[2]=90a5f1e3  B[2]=b37d8727  C[2]=fa1b17ff  D[2]=a0031e29
A[3]=8c88745e  B[3]=0fe2259f  C[3]=cdfe087e  D[3]=cfb9b9b8
A[4]=fc80a507  B[4]=6d123afc  C[4]=33d2cefc  D[4]=3467b950
A[5]=879310d5  B[5]=2ef097bb  C[5]=8a9c3bcb  D[5]=d06ccc0d
A[6]=e0d18000  B[6]=3d29fc9a  C[6]=64a8725e  D[6]=7b2ec18d
A[7]=52bfdf07  B[7]=dec18510  C[7]=a86c832d  D[7]=16646869

Step  1: (r=20, s=14)
A[0]=359c35bf  B[0]=d4dddf16  C[0]=44957129  D[0]=719df447
A[1]=a7dcbc7d  B[1]=c15867ee  C[1]=e3734bd4  D[1]=e628bed5
A[2]=3644fa73  B[2]=1e390a5f  C[2]=b37d8727  D[2]=fa1b17ff
A[3]=c57eabbd  B[3]=45e8c887  C[3]=0fe2259f  D[3]=cdfe087e
A[4]=3ed4fb72  B[4]=507fc80a  C[4]=6d123afc  D[4]=33d2cefc
A[5]=c2a1de53  B[5]=0d587931  C[5]=2ef097bb  D[5]=8a9c3bcb
A[6]=06dfaeca  B[6]=000e0d18  C[6]=3d29fc9a  D[6]=64a8725e
A[7]=184647f5  B[7]=f0752bfd  C[7]=dec18510  D[7]=a86c832d
```

```
Step  2: (r=14, s=27)
A[0]=261b41bc  B[0]=0d6fcd67  C[0]=d4dddf16  D[0]=44957129
A[1]=d98032d5  B[1]=2f1f69f7  C[1]=c15867ee  D[1]=e3734bd4
A[2]=4e730c24  B[2]=3e9ccd91  C[2]=1e390a5f  D[2]=b37d8727
A[3]=16e48538  B[3]=aaef715f  C[3]=45e8c887  D[3]=0fe2259f
A[4]=d64e67fb  B[4]=3edc8fb5  C[4]=507fc80a  D[4]=6d123afc
A[5]=26288155  B[5]=7794f0a8  C[5]=0d587931  D[5]=2ef097bb
A[6]=3290961d  B[6]=ebb281b7  C[6]=000e0d18  D[6]=3d29fc9a
A[7]=0af28503  B[7]=91fd4611  C[7]=f0752bfd  D[7]=dec18510

Step  3: (r=27, s= 3)
A[0]=11050715  B[0]=e130da0d  C[0]=0d6fcd67  D[0]=d4dddf16
A[1]=bea44561  B[1]=aecc0196  C[1]=2f1f69f7  D[1]=c15867ee
A[2]=2f418d47  B[2]=22739861  C[2]=3e9ccd91  D[2]=1e390a5f
A[3]=514381bc  B[3]=c0b72429  C[3]=aaef715f  D[3]=45e8c887
A[4]=a3b89bb2  B[4]=deb2733f  C[4]=3edc8fb5  D[4]=507fc80a
A[5]=b3d71438  B[5]=a931440a  C[5]=7794f0a8  D[5]=0d587931
A[6]=ffaf74ea  B[6]=e99484b0  C[6]=ebb281b7  D[6]=000e0d18
A[7]=2ebad92e  B[7]=18579428  C[7]=91fd4611  D[7]=f0752bfd

Step  4: (r= 3, s=20)
A[0]=c803f869  B[0]=882838a8  C[0]=e130da0d  D[0]=0d6fcd67
A[1]=1783195d  B[1]=f5222b0d  C[1]=aecc0196  D[1]=2f1f69f7
A[2]=ab156660  B[2]=7a0c6a39  C[2]=22739861  D[2]=3e9ccd91
A[3]=a487490d  B[3]=8a1c0de2  C[3]=c0b72429  D[3]=aaef715f
A[4]=658d833b  B[4]=1dc4dd95  C[4]=deb2733f  D[4]=3edc8fb5
A[5]=03fc39f5  B[5]=9eb8a1c5  C[5]=a931440a  D[5]=7794f0a8
A[6]=7313b747  B[6]=fd7ba757  C[6]=e99484b0  D[6]=ebb281b7
A[7]=1da0382a  B[7]=75d6c971  C[7]=18579428  D[7]=91fd4611

Step  5: (r=20, s=14)
A[0]=88fae0c4  B[0]=869c803f  C[0]=882838a8  D[0]=e130da0d
A[1]=26655658  B[1]=95d17831  C[1]=f5222b0d  D[1]=aecc0196
A[2]=a4ad4b9b  B[2]=660ab156  C[2]=7a0c6a39  D[2]=22739861
A[3]=05b60a1e  B[3]=90da4874  C[3]=8a1c0de2  D[3]=c0b72429
A[4]=1a3652b9  B[4]=33b658d8  C[4]=1dc4dd95  D[4]=deb2733f
A[5]=1270ae87  B[5]=9f503fc3  C[5]=9eb8a1c5  D[5]=a931440a
A[6]=f54e0679  B[6]=7477313b  C[6]=fd7ba757  D[6]=e99484b0
A[7]=a8ef9f6f  B[7]=82a1da03  C[7]=75d6c971  D[7]=18579428

Step  6: (r=14, s=27)
A[0]=e2da4c64  B[0]=b831223e  C[0]=869c803f  D[0]=882838a8
A[1]=669fc262  B[1]=55960999  C[1]=95d17831  D[1]=f5222b0d
A[2]=58d89a36  B[2]=52e6e92b  C[2]=660ab156  D[2]=7a0c6a39
A[3]=96ad6542  B[3]=8287816d  C[3]=90da4874  D[3]=8a1c0de2
A[4]=a521e23c  B[4]=94ae468d  C[4]=33b658d8  D[4]=1dc4dd95
A[5]=c6c4402d  B[5]=2ba1c49c  C[5]=9f503fc3  D[5]=9eb8a1c5
A[6]=e1cd5e07  B[6]=819e7d53  C[6]=7477313b  D[6]=fd7ba757
A[7]=1e4c0dee  B[7]=e7dbea3b  C[7]=82a1da03  D[7]=75d6c971
```

```
Step  7: (r=27, s= 3)
A[0]=20d0a57c  B[0]=2716d263  C[0]=b831223e  D[0]=869c803f
A[1]=ba16e382  B[1]=1334fe13  C[1]=55960999  D[1]=95d17831
A[2]=a0023c2e  B[2]=b2c6c4d1  C[2]=52e6e92b  D[2]=660ab156
A[3]=50865df7  B[3]=14b56b2a  C[3]=8287816d  D[3]=90da4874
A[4]=6931689f  B[4]=e5290f11  C[4]=94ae468d  D[4]=33b658d8
A[5]=bfe57469  B[5]=6e362201  C[5]=2ba1c49c  D[5]=9f503fc3
A[6]=e5d64219  B[6]=3f0e6af0  C[6]=819e7d53  D[6]=7477313b
A[7]=985b17c4  B[7]=70f2606f  C[7]=e7dbea3b  D[7]=82a1da03

Step  8: (r=26, s= 4)
A[0]=828b8c52  B[0]=f0834295  C[0]=2716d263  D[0]=b831223e
A[1]=dc77d2b4  B[1]=0ae85b8e  C[1]=1334fe13  D[1]=55960999
A[2]=d469cfdc  B[2]=ba8008f0  C[2]=b2c6c4d1  D[2]=52e6e92b
A[3]=db108c81  B[3]=dd421977  C[3]=14b56b2a  D[3]=8287816d
A[4]=474a7184  B[4]=7da4c5a2  C[4]=e5290f11  D[4]=94ae468d
A[5]=63c3b26c  B[5]=a6ff95d1  C[5]=6e362201  D[5]=2ba1c49c
A[6]=d597f0f3  B[6]=67975908  C[6]=3f0e6af0  D[6]=819e7d53
A[7]=0d455b38  B[7]=12616c5f  C[7]=70f2606f  D[7]=e7dbea3b

Step  9: (r= 4, s=23)
A[0]=1df8b06c  B[0]=28b8c528  C[0]=f0834295  D[0]=2716d263
A[1]=59c304f5  B[1]=c77d2b4d  C[1]=0ae85b8e  D[1]=1334fe13
A[2]=24d40e13  B[2]=469cfdcd  C[2]=ba8008f0  D[2]=b2c6c4d1
A[3]=f5d5ba39  B[3]=b108c81d  C[3]=dd421977  D[3]=14b56b2a
A[4]=21b74488  B[4]=74a71844  C[4]=7da4c5a2  D[4]=e5290f11
A[5]=e710bb7f  B[5]=3c3b26c6  C[5]=a6ff95d1  D[5]=6e362201
A[6]=2e16af09  B[6]=597f0f3d  C[6]=67975908  D[6]=3f0e6af0
A[7]=080a3e93  B[7]=d455b380  C[7]=12616c5f  D[7]=70f2606f

Step 10: (r=23, s=11)
A[0]=edf8e3a6  B[0]=360efc58  C[0]=28b8c528  D[0]=f0834295
A[1]=f7e71668  B[1]=7aace182  C[1]=c77d2b4d  D[1]=0ae85b8e
A[2]=a7e78cc1  B[2]=09926a07  C[2]=469cfdcd  D[2]=ba8008f0
A[3]=46935bb0  B[3]=1cfaeadd  C[3]=b108c81d  D[3]=dd421977
A[4]=22aeec1d  B[4]=4410dba2  C[4]=74a71844  D[4]=7da4c5a2
A[5]=0cff7eb2  B[5]=bff3885d  C[5]=3c3b26c6  D[5]=a6ff95d1
A[6]=1020fb28  B[6]=84970b57  C[6]=597f0f3d  D[6]=67975908
A[7]=44806033  B[7]=4984051f  C[7]=d455b380  D[7]=12616c5f

Step 11: (r=11, s=26)
A[0]=93141e3d  B[0]=c71d376f  C[0]=360efc58  D[0]=28b8c528
A[1]=d2e1d7c2  B[1]=38b347bf  C[1]=7aace182  D[1]=c77d2b4d
A[2]=e3dde6a5  B[2]=3c660d3f  C[2]=09926a07  D[2]=469cfdcd
A[3]=7417c284  B[3]=9add8234  C[3]=1cfaeadd  D[3]=b108c81d
A[4]=5d201234  B[4]=7760e915  C[4]=4410dba2  D[4]=74a71844
A[5]=8496e902  B[5]=fbf59067  C[5]=bff3885d  D[5]=3c3b26c6
A[6]=9e3fc65d  B[6]=07d94081  C[6]=84970b57  D[6]=597f0f3d
```

```
A[7]=82e3c8d8  B[7]=03019a24  C[7]=4984051f  D[7]=d455b380

Step 12: (r=26, s= 4)
A[0]=35497f9c  B[0]=f64c5078  C[0]=c71d376f  D[0]=360efc58
A[1]=887a8aa7  B[1]=0b4b875f  C[1]=38b347bf  D[1]=7aace182
A[2]=1c86aab6  B[2]=978f779a  C[2]=3c660d3f  D[2]=09926a07
A[3]=798a13db  B[3]=11d05f0a  C[3]=9add8234  D[3]=1cfaeadd
A[4]=b56361ae  B[4]=d1748048  C[4]=7760e915  D[4]=4410dba2
A[5]=7f21e186  B[5]=0a125ba4  C[5]=fbf59067  D[5]=bff3885d
A[6]=eb7d50a3  B[6]=7678ff19  C[6]=07d94081  D[6]=84970b57
A[7]=ae8f9156  B[7]=620b8f23  C[7]=03019a24  D[7]=4984051f

Step 13: (r= 4, s=23)
A[0]=7d582902  B[0]=5497f9c3  C[0]=f64c5078  D[0]=c71d376f
A[1]=8fe21944  B[1]=87a8aa78  C[1]=0b4b875f  D[1]=38b347bf
A[2]=ce138997  B[2]=c86aab61  C[2]=978f779a  D[2]=3c660d3f
A[3]=bd5dbb7e  B[3]=98a13db7  C[3]=11d05f0a  D[3]=9add8234
A[4]=ca47d92a  B[4]=56361aeb  C[4]=d1748048  D[4]=7760e915
A[5]=429704a8  B[5]=f21e1867  C[5]=0a125ba4  D[5]=fbf59067
A[6]=7d0e25f5  B[6]=b7d50a3e  C[6]=7678ff19  D[6]=07d94081
A[7]=b1b754ba  B[7]=e8f9156a  C[7]=620b8f23  D[7]=03019a24

Step 14: (r=23, s=11)
A[0]=2d48fccc  B[0]=813eac14  C[0]=5497f9c3  D[0]=f64c5078
A[1]=d092d023  B[1]=a247f10c  C[1]=87a8aa78  D[1]=0b4b875f
A[2]=d4074d98  B[2]=cbe709c4  C[2]=c86aab61  D[2]=978f779a
A[3]=85790672  B[3]=bf5eaedd  C[3]=98a13db7  D[3]=11d05f0a
A[4]=647a6201  B[4]=956523ec  C[4]=56361aeb  D[4]=d1748048
A[5]=5f49c94f  B[5]=54214b82  C[5]=f21e1867  D[5]=0a125ba4
A[6]=8892c2d4  B[6]=fabe8712  C[6]=b7d50a3e  D[6]=7678ff19
A[7]=4d52b0ef  B[7]=5d58dbaa  C[7]=e8f9156a  D[7]=620b8f23

Step 15: (r=11, s=26)
A[0]=369e55be  B[0]=47e6616a  C[0]=813eac14  D[0]=5497f9c3
A[1]=2fcb9c0a  B[1]=96811e84  C[1]=a247f10c  D[1]=87a8aa78
A[2]=42a0cd1f  B[2]=3a6cc6a0  C[2]=cbe709c4  D[2]=c86aab61
A[3]=06d58535  B[3]=c833942b  C[3]=bf5eaedd  D[3]=98a13db7
A[4]=e5654ef2  B[4]=d3100b23  C[4]=956523ec  D[4]=56361aeb
A[5]=12af5951  B[5]=4e4a7afa  C[5]=54214b82  D[5]=f21e1867
A[6]=a080554c  B[6]=9616a444  C[6]=fabe8712  D[6]=b7d50a3e
A[7]=5f8774f4  B[7]=95877a6a  C[7]=5d58dbaa  D[7]=e8f9156a

Step 16: (r=19, s=28)
A[0]=cb5c9742  B[0]=adf1b4f2  C[0]=47e6616a  D[0]=813eac14
A[1]=5daff08d  B[1]=e0517e5c  C[1]=96811e84  D[1]=a247f10c
A[2]=be5a0436  B[2]=68fa1506  C[2]=3a6cc6a0  D[2]=cbe709c4
A[3]=406d3775  B[3]=29a836ac  C[3]=c833942b  D[3]=bf5eaedd
A[4]=ff297dab  B[4]=77972b2a  C[4]=d3100b23  D[4]=956523ec
A[5]=8e0a556a  B[5]=ca88957a  C[5]=4e4a7afa  D[5]=54214b82
```

```
A[6]=7cbce14a  B[6]=aa650402  C[6]=9616a444  D[6]=fabe8712
A[7]=fdc0a79e  B[7]=a7a2fc3b  C[7]=95877a6a  D[7]=5d58dbaa

Step 17: (r=28, s= 7)
A[0]=9f372df9  B[0]=2cb5c974  C[0]=adf1b4f2  D[0]=47e6616a
A[1]=aa0d281a  B[1]=d5daff08  C[1]=e0517e5c  D[1]=96811e84
A[2]=50a4e697  B[2]=6be5a043  C[2]=68fa1506  D[2]=3a6cc6a0
A[3]=d5963ad2  B[3]=5406d377  C[3]=29a836ac  D[3]=c833942b
A[4]=5b8ec9ae  B[4]=bff297da  C[4]=77972b2a  D[4]=d3100b23
A[5]=8f065863  B[5]=a8e0a556  C[5]=ca88957a  D[5]=4e4a7afa
A[6]=34b20ae2  B[6]=a7cbce14  C[6]=aa650402  D[6]=9616a444
A[7]=18a7b23c  B[7]=efdc0a79  C[7]=a7a2fc3b  D[7]=95877a6a

Step 18: (r= 7, s=22)
A[0]=6844ec54  B[0]=9b96fccf  C[0]=2cb5c974  D[0]=adf1b4f2
A[1]=29138868  B[1]=06940d55  C[1]=d5daff08  D[1]=e0517e5c
A[2]=da5692fb  B[2]=52734ba8  C[2]=6be5a043  D[2]=68fa1506
A[3]=3af31af2  B[3]=cb1d696a  C[3]=5406d377  D[3]=29a836ac
A[4]=137769d8  B[4]=c764d72d  C[4]=bff297da  D[4]=77972b2a
A[5]=00fd5b7b  B[5]=832c31c7  C[5]=a8e0a556  D[5]=ca88957a
A[6]=5b8f7df7  B[6]=5905711a  C[6]=a7cbce14  D[6]=aa650402
A[7]=cbb12d90  B[7]=53d91e0c  C[7]=efdc0a79  D[7]=a7a2fc3b

Step 19: (r=22, s=19)
A[0]=c6027462  B[0]=151a113b  C[0]=9b96fccf  D[0]=2cb5c974
A[1]=29ee88f0  B[1]=1a0a44e2  C[1]=06940d55  D[1]=d5daff08
A[2]=89c77b5a  B[2]=bef695a4  C[2]=52734ba8  D[2]=6be5a043
A[3]=ee5a1f4a  B[3]=bc8ebcc6  C[3]=cb1d696a  D[3]=5406d377
A[4]=b3f4be74  B[4]=7604ddda  C[4]=c764d72d  D[4]=bff297da
A[5]=0b3f3df5  B[5]=dec03f56  C[5]=832c31c7  D[5]=a8e0a556
A[6]=8002ca30  B[6]=7dd6e3df  C[6]=5905711a  D[6]=a7cbce14
A[7]=41070801  B[7]=6432ec4b  C[7]=53d91e0c  D[7]=efdc0a79

Step 20: (r=19, s=28)
A[0]=1a7e228e  B[0]=a3163013  C[0]=151a113b  D[0]=9b96fccf
A[1]=ed3f3caf  B[1]=47814f74  C[1]=1a0a44e2  D[1]=06940d55
A[2]=7529c029  B[2]=dad44e3b  C[2]=bef695a4  D[2]=52734ba8
A[3]=41bd727d  B[3]=fa5772d0  C[3]=bc8ebcc6  D[3]=cb1d696a
A[4]=e6377e53  B[4]=f3a59fa5  C[4]=7604ddda  D[4]=c764d72d
A[5]=27fd32be  B[5]=efa859f9  C[5]=dec03f56  D[5]=832c31c7
A[6]=e33f961f  B[6]=51840016  C[6]=7dd6e3df  D[6]=5905711a
A[7]=15e1762c  B[7]=400a0838  C[7]=6432ec4b  D[7]=53d91e0c

Step 21: (r=28, s= 7)
A[0]=c3c6393c  B[0]=e1a7e228  C[0]=a3163013  D[0]=151a113b
A[1]=09b78923  B[1]=fed3f3ca  C[1]=47814f74  D[1]=1a0a44e2
A[2]=bb568e59  B[2]=97529c02  C[2]=dad44e3b  D[2]=bef695a4
A[3]=93694634  B[3]=d41bd727  C[3]=fa5772d0  D[3]=bc8ebcc6
A[4]=50aed5d0  B[4]=3e6377e5  C[4]=f3a59fa5  D[4]=7604ddda
```

```
A[5]=33affb30  B[5]=e27fd32b  C[5]=efa859f9  D[5]=dec03f56
A[6]=6e482c9f  B[6]=fe33f961  C[6]=51840016  D[6]=7dd6e3df
A[7]=3b707b7b  B[7]=c15e1762  C[7]=400a0838  D[7]=6432ec4b

Step 22: (r= 7, s=22)
A[0]=5dc6917a  B[0]=e31c9e61  C[0]=e1a7e228  D[0]=a3163013
A[1]=56498afa  B[1]=dbc49184  C[1]=fed3f3ca  D[1]=47814f74
A[2]=8ed658f7  B[2]=ab472cdd  C[2]=97529c02  D[2]=dad44e3b
A[3]=5c9e50b5  B[3]=b4a31a49  C[3]=d41bd727  D[3]=fa5772d0
A[4]=37a326c8  B[4]=576ae828  C[4]=3e6377e5  D[4]=f3a59fa5
A[5]=99207bda  B[5]=d7fd9819  C[5]=e27fd32b  D[5]=efa859f9
A[6]=a2f9bab0  B[6]=24164fb7  C[6]=fe33f961  D[6]=51840016
A[7]=f32bdfdd  B[7]=b83dbd9d  C[7]=c15e1762  D[7]=400a0838

Step 23: (r=22, s=19)
A[0]=c23810fd  B[0]=5e9771a4  C[0]=e31c9e61  D[0]=e1a7e228
A[1]=81f1076e  B[1]=be959262  C[1]=dbc49184  D[1]=fed3f3ca
A[2]=ff3314e6  B[2]=3de3b596  C[2]=ab472cdd  D[2]=97529c02
A[3]=e1e27f71  B[3]=2d572794  C[3]=b4a31a49  D[3]=d41bd727
A[4]=83a0d7df  B[4]=b20de8c9  C[4]=576ae828  D[4]=3e6377e5
A[5]=ab10675a  B[5]=f6a6481e  C[5]=d7fd9819  D[5]=e27fd32b
A[6]=f77097a4  B[6]=ac28be6e  C[6]=24164fb7  D[6]=fe33f961
A[7]=acbb71b9  B[7]=f77ccaf7  C[7]=b83dbd9d  D[7]=c15e1762

Step 24: (r=15, s= 5)
A[0]=837af0bc  B[0]=087ee11c  C[0]=5e9771a4  D[0]=e31c9e61
A[1]=59a69130  B[1]=83b740f8  C[1]=be959262  D[1]=dbc49184
A[2]=95ad44e2  B[2]=8a737f99  C[2]=3de3b596  D[2]=ab472cdd
A[3]=e2511a0c  B[3]=3fb8f0f1  C[3]=2d572794  D[3]=b4a31a49
A[4]=7f7cb393  B[4]=6befc1d0  C[4]=b20de8c9  D[4]=576ae828
A[5]=dc61e65e  B[5]=33ad5588  C[5]=f6a6481e  D[5]=d7fd9819
A[6]=a5d7221d  B[6]=4bd27bb8  C[6]=ac28be6e  D[6]=24164fb7
A[7]=a8b54f6c  B[7]=b8dcd65d  C[7]=f77ccaf7  D[7]=b83dbd9d

Step 25: (r= 5, s=29)
A[0]=d7af223d  B[0]=6f5e1790  C[0]=087ee11c  D[0]=5e9771a4
A[1]=03d416d3  B[1]=34d2260b  C[1]=83b740f8  D[1]=be959262
A[2]=ba96a715  B[2]=b5a89c52  C[2]=8a737f99  D[2]=3de3b596
A[3]=65a2cbab  B[3]=4a23419c  C[3]=3fb8f0f1  D[3]=2d572794
A[4]=370d7624  B[4]=ef96726f  C[4]=6befc1d0  D[4]=b20de8c9
A[5]=1b26f2eb  B[5]=8c3ccbdb  C[5]=33ad5588  D[5]=f6a6481e
A[6]=6c86cd05  B[6]=bae443b4  C[6]=4bd27bb8  D[6]=ac28be6e
A[7]=a7d2e3d2  B[7]=16a9ed95  C[7]=b8dcd65d  D[7]=f77ccaf7

Step 26: (r=29, s= 9)
A[0]=8df61e03  B[0]=baf5e447  C[0]=6f5e1790  D[0]=087ee11c
A[1]=caf1d16f  B[1]=607a82da  C[1]=34d2260b  D[1]=83b740f8
A[2]=52877cfb  B[2]=b752d4e2  C[2]=b5a89c52  D[2]=8a737f99
A[3]=0e12ca94  B[3]=6cb45975  C[3]=4a23419c  D[3]=3fb8f0f1
```

```
A[4]=6db8a56e  B[4]=86e1aec4  C[4]=ef96726f  D[4]=6befc1d0
A[5]=909c5cf6  B[5]=6364de5d  C[5]=8c3ccbdb  D[5]=33ad5588
A[6]=eb3ceaeb  B[6]=ad90d9a0  C[6]=bae443b4  D[6]=4bd27bb8
A[7]=5b412468  B[7]=54fa5c7a  C[7]=16a9ed95  D[7]=b8dcd65d

Step 27: (r= 9, s=15)
A[0]=0f51dbd2  B[0]=ec3c071b  C[0]=baf5e447  D[0]=6f5e1790
A[1]=51cff3aa  B[1]=e3a2df95  C[1]=607a82da  D[1]=34d2260b
A[2]=5010fc90  B[2]=0ef9f6a5  C[2]=b752d4e2  D[2]=b5a89c52
A[3]=e9bd0c37  B[3]=2595281c  C[3]=6cb45975  D[3]=4a23419c
A[4]=ee2b0a6b  B[4]=714adcdb  C[4]=86e1aec4  D[4]=ef96726f
A[5]=d0c96cc3  B[5]=38b9ed21  C[5]=6364de5d  D[5]=8c3ccbdb
A[6]=a0444adc  B[6]=79d5d7d6  C[6]=ad90d9a0  D[6]=bae443b4
A[7]=1e163893  B[7]=8248d0b6  C[7]=54fa5c7a  D[7]=16a9ed95

Step 28: (r=15, s= 5)
A[0]=34ef7f18  B[0]=ede907a8  C[0]=ec3c071b  D[0]=baf5e447
A[1]=b63145fd  B[1]=f9d528e7  C[1]=e3a2df95  D[1]=607a82da
A[2]=6cd2a5de  B[2]=7e482808  C[2]=0ef9f6a5  D[2]=b752d4e2
A[3]=ab712a6b  B[3]=861bf4de  C[3]=2595281c  D[3]=6cb45975
A[4]=0c4f745d  B[4]=8535f715  C[4]=714adcdb  D[4]=86e1aec4
A[5]=4d54d198  B[5]=b661e864  C[5]=38b9ed21  D[5]=6364de5d
A[6]=faa03754  B[6]=256e5022  C[6]=79d5d7d6  D[6]=ad90d9a0
A[7]=39f89f52  B[7]=1c498f0b  C[7]=8248d0b6  D[7]=54fa5c7a

Step 29: (r= 5, s=29)
A[0]=a2e775a1  B[0]=9defe306  C[0]=ede907a8  D[0]=ec3c071b
A[1]=587313c0  B[1]=c628bfb6  C[1]=f9d528e7  D[1]=e3a2df95
A[2]=bba18946  B[2]=9a54bbcd  C[2]=7e482808  D[2]=0ef9f6a5
A[3]=505c942f  B[3]=6e254d75  C[3]=861bf4de  D[3]=2595281c
A[4]=58ebbba3  B[4]=89ee8ba1  C[4]=8535f715  D[4]=714adcdb
A[5]=532aaf15  B[5]=aa9a3309  C[5]=b661e864  D[5]=38b9ed21
A[6]=65d3aac7  B[6]=5406ea9f  C[6]=256e5022  D[6]=79d5d7d6
A[7]=afa88b13  B[7]=3f13ea47  C[7]=1c498f0b  D[7]=8248d0b6

Step 30: (r=29, s= 9)
A[0]=3c69fffe  B[0]=345ceeb4  C[0]=9defe306  D[0]=ede907a8
A[1]=f59530ec  B[1]=0b0e6278  C[1]=c628bfb6  D[1]=f9d528e7
A[2]=fbd60003  B[2]=d7743128  C[2]=9a54bbcd  D[2]=7e482808
A[3]=4158e2c8  B[3]=ea0b9285  C[3]=6e254d75  D[3]=861bf4de
A[4]=00c7d1f0  B[4]=6b1d7774  C[4]=89ee8ba1  D[4]=8535f715
A[5]=db5ee903  B[5]=aa6555e2  C[5]=aa9a3309  D[5]=b661e864
A[6]=2e5d1b6c  B[6]=ecba7558  C[6]=5406ea9f  D[6]=256e5022
A[7]=afe73023  B[7]=75f51162  C[7]=3f13ea47  D[7]=1c498f0b

Step 31: (r= 9, s=15)
A[0]=593c673c  B[0]=d3fffc78  C[0]=345ceeb4  D[0]=9defe306
A[1]=e5aa9e29  B[1]=2a61d9eb  C[1]=0b0e6278  D[1]=c628bfb6
A[2]=f4afa723  B[2]=ac0007f7  C[2]=d7743128  D[2]=9a54bbcd
```

```
A[3]=491e506e  B[3]=b1c59082  C[3]=ea0b9285  D[3]=6e254d75
A[4]=594e5418  B[4]=8fa3e001  C[4]=6b1d7774  D[4]=89ee8ba1
A[5]=c539dc20  B[5]=bdd207b6  C[5]=aa6555e2  D[5]=aa9a3309
A[6]=fbf8267e  B[6]=ba36d85c  C[6]=ecba7558  D[6]=5406ea9f
A[7]=7d041314  B[7]=ce60475f  C[7]=75f51162  D[7]=3f13ea47

Feed-Forward Step 0: (r=15, s= 5)
A[0]=cf042cdc  B[0]=339e2c9e  C[0]=d3fffc78  D[0]=345ceeb4
A[1]=cb2261cf  B[1]=4f14f2d5  C[1]=2a61d9eb  D[1]=0b0e6278
A[2]=2ac7a016  B[2]=d391fa57  C[2]=ac0007f7  D[2]=d7743128
A[3]=38768fd5  B[3]=2837248f  C[3]=b1c59082  D[3]=ea0b9285
A[4]=42972f24  B[4]=2a0c2ca7  C[4]=8fa3e001  D[4]=6b1d7774
A[5]=2395a8fe  B[5]=ee10629c  C[5]=bdd207b6  D[5]=aa6555e2
A[6]=4559b04d  B[6]=133f7dfc  C[6]=ba36d85c  D[6]=ecba7558
A[7]=0ee349f0  B[7]=098a3e82  C[7]=ce60475f  D[7]=75f51162

Feed-Forward Step 1: (r= 5, s=29)
A[0]=50335ebb  B[0]=e0859b99  C[0]=339e2c9e  D[0]=d3fffc78
A[1]=5a611ded  B[1]=644c39f9  C[1]=4f14f2d5  D[1]=2a61d9eb
A[2]=ab87b9bc  B[2]=58f402c5  C[2]=d391fa57  D[2]=ac0007f7
A[3]=b0844fea  B[3]=0ed1faa7  C[3]=2837248f  D[3]=b1c59082
A[4]=50f8affa  B[4]=52e5e488  C[4]=2a0c2ca7  D[4]=8fa3e001
A[5]=1ad3b52a  B[5]=72b51fc4  C[5]=ee10629c  D[5]=bdd207b6
A[6]=947a308a  B[6]=ab3609a8  C[6]=133f7dfc  D[6]=ba36d85c
A[7]=4f919427  B[7]=dc693e01  C[7]=098a3e82  D[7]=ce60475f

Feed-Forward Step 2: (r=29, s= 9)
A[0]=8b4d9c29  B[0]=6a066bd7  C[0]=e0859b99  D[0]=339e2c9e
A[1]=f502dd44  B[1]=ab4c23bd  C[1]=644c39f9  D[1]=4f14f2d5
A[2]=722c45ee  B[2]=9570f737  C[2]=58f402c5  D[2]=d391fa57
A[3]=af88d913  B[3]=561089fd  C[3]=0ed1faa7  D[3]=2837248f
A[4]=368c467a  B[4]=4a1f15ff  C[4]=52e5e488  D[4]=2a0c2ca7
A[5]=35c7a640  B[5]=435a76a5  C[5]=72b51fc4  D[5]=ee10629c
A[6]=e51bef2e  B[6]=528f4611  C[6]=ab3609a8  D[6]=133f7dfc
A[7]=09e2fe38  B[7]=e9f23284  C[7]=dc693e01  D[7]=098a3e82

Feed-Forward Step 3: (r= 9, s=15)
A[0]=df29704e  B[0]=9b385316  C[0]=6a066bd7  D[0]=e0859b99
A[1]=46cacf5f  B[1]=05ba89ea  C[1]=ab4c23bd  D[1]=644c39f9
A[2]=dbd4ef49  B[2]=588bdce4  C[2]=9570f737  D[2]=58f402c5
A[3]=966e6906  B[3]=11b2275f  C[3]=561089fd  D[3]=0ed1faa7
A[4]=56af090e  B[4]=188cf46d  C[4]=4a1f15ff  D[4]=52e5e488
A[5]=1ae7ba52  B[5]=8f4c806b  C[5]=435a76a5  D[5]=72b51fc4
A[6]=e92dd850  B[6]=37de5dca  C[6]=528f4611  D[6]=ab3609a8
A[7]=6425983e  B[7]=c5fc7013  C[7]=e9f23284  D[7]=dc693e01
```

Compression Function Output

```
A[0]=df29704e  B[0]=9b385316  C[0]=6a066bd7  D[0]=e0859b99
```

```
A[1]=46cacf5f  B[1]=05ba89ea  C[1]=ab4c23bd  D[1]=644c39f9
A[2]=dbd4ef49  B[2]=588bdce4  C[2]=9570f737  D[2]=58f402c5
A[3]=966e6906  B[3]=11b2275f  C[3]=561089fd  D[3]=0ed1faa7
A[4]=56af090e  B[4]=188cf46d  C[4]=4a1f15ff  D[4]=52e5e488
A[5]=1ae7ba52  B[5]=8f4c806b  C[5]=435a76a5  D[5]=72b51fc4
A[6]=e92dd850  B[6]=37de5dca  C[6]=528f4611  D[6]=ab3609a8
A[7]=6425983e  B[7]=c5fc7013  C[7]=e9f23284  D[7]=dc693e01
```

Hash Function Output

```
4e 70 29 df 5f cf ca 46 49 ef d4 db 06 69 6e 96
0e 09 af 56 52 ba e7 1a 50 d8 2d e9 3e 98 25 64
16 53 38 9b ea 89 ba 05 e4 dc 8b 58 5f 27 b2 11
6d f4 8c 18 6b 80 4c 8f ca 5d de 37 13 70 fc c5
```

Bibliography

[1] Bellare, M.: New Proofs for NMAC and HMAC: Security without Collision-Resistance. In Dwork, C., ed.: CRYPTO. Volume 4117 of Lecture Notes in Computer Science., Springer (2006) 602–619

[2] Bellare, M., Canetti, R., Krawczyk, H.: Pseudorandom Functions Revisited: The Cascade Construction and Its Concrete Security. In: FOCS. (1996) 514–523

[3] Black, J., Rogaway, P., Shrimpton, T.: Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Yung, M., ed.: CRYPTO. Volume 2442 of Lecture Notes in Computer Science., Springer (2002) 320–335

[4] Chang, D., Nandi, M.: Improved Indifferentiability Security Analysis of chopMD Hash Function. [18] 429–443

[5] Coron, J.S., Dodis, Y., Malinaud, C., Puniya, P.: Merkle-Damgård Revisited: How to Construct a Hash Function. In: CRYPTO'05. (2005) 430–448

[6] Cramer, R., ed.: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. In Cramer, R., ed.: EUROCRYPT'05. Volume 3494 of Lecture Notes in Computer Science., Springer (2005)

[7] Dean, R.D.: Formal Aspects of Mobile Code Security. PhD thesis, Princeton University (January 1999)

[8] den Boer, B., Bosselaers, A.: Collisions for the Compression Function of MD5. In: EUROCRYPT. (1993) 293–304

[9] Dodis, Y., Gennaro, R., Håstad, J., Krawczyk, H., Rabin, T.: Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. [11] 494–510

[10] Fouque, P.A., Pointcheval, D., Zimmer, S.: HMAC is a randomness extractor and applications to TLS. In Abe, M., Gligor, V.D., eds.: ASIACCS, ACM (2008) 21–32

[11] Franklin, M.K., ed.: Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. In Franklin, M.K., ed.: CRYPTO'04. Volume 3152 of Lecture Notes in Computer Science., Springer (2004)

[12] Joux, A.: Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. [11] 306–316

[13] Jutla, C.S., Patthak, A.C.: Provably Good Codes for Hash Function Design. In Biham, E., Youssef, A.M., eds.: Selected Areas in Cryptography. Volume 4356 of Lecture Notes in Computer Science., Springer (2006) 376–393

[14] Kelsey, J., Schneier, B.: Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. [6] 474–490

[15] Lucks, S.: A Failure-Friendly Design Principle for Hash Functions. In Roy, B.K., ed.: ASIACRYPT'05. Volume 3788 of Lecture Notes in Computer Science., Springer (2005) 474–494

[16] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: A Modest Proposal for FFT Hashing. [18] 54–72

[17] Maurer, U.M., Tessaro, S.: Domain Extension of Public Random Functions: Beyond the Birthday Barrier. In Menezes, A., ed.: CRYPTO. Volume 4622 of Lecture Notes in Computer Science., Springer (2007) 187–204

[18] Nyberg, K., ed.: Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers. In Nyberg, K., ed.: FSE. Volume 5086 of Lecture Notes in Computer Science., Springer (2008)

[19] Preneel, B., Govaerts, R., Vandewalle, J.: Differential Cryptanalysis of Hash Functions Based on Block Ciphers. In: ACM Conference on Computer and Communications Security. (1993) 183–188

[20] Projet RNRT SAPHIR: sphlib 1.0. `http://www.crypto-hash.fr/modules/wfdownloads/singlefile.php?cid=9&lid=5`

[21] Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In Shoup, V., ed.: CRYPTO. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 17–36

[22] Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. [6] 19–35