

SHA-3, Round 2 Tweaks

Candidate	Round 2 tweaks (status as of Sept. 22, 22:30 CEST)
BLAKE	None
BMW	Changed inputs to f_0 and f_1 ; Additional invocation of compression function at end
CubeHash	2x rounds ($r = 16$); 32x size of message block ($b = 32$)
ECHO	None
Fugue	None
Grøstl	None
Hamsi	None (but additional variants specified)
JH	None
Keccak	Increased message block size (rate); increased number of rounds (18 -> 24)
Luffa	Modification of S-box; Changed order of SubCrumb inputs; Always one round in output transformation
Shabal	None
SHAvite-3	Inversion of some counter values
SIMD	Changed rotation constants and permutations for diffusion between parallel Feistels
Skein	Changed rotation constants