The Skein Hash Function Family

NIST Round 2 Tweak Description

15 Sep 2009

Description of Changes

The only change to the Skein hash function is in the Threefish rotation constants, found in Table 4 (Section 3.3.1) of the newly submitted ("tweak") version 1.2 of the Skein specification document, reproduced here as Table 1.

N_w		4		8				16							
j		0	1	0	1	2	3	0	1	2	3	4	5	6	7
	0	14	16	46	36	19	37	24	13	8	47	8	17	22	37
	1	52	57	33	27	14	42	38	19	10	55	49	18	23	52
	2	23	40	17	49	36	39	33	4	51	13	34	41	59	17
$d =$	3	5	37	44	9	54	56	5	20	48	41	47	28	16	25
	4	25	33	39	30	34	24	41	9	37	31	12	47	44	30
	5	46	12	13	50	10	17	16	34	56	51	4	53	42	41
	6	58	22	25	29	39	43	31	44	47	46	19	42	44	25
	7	32	32	8	35	56	22	9	48	35	52	23	31	37	20

Table 1: Rotation constants $R_{d,j}$ for each N_w.

Further details and discussion of the tweak and its implications are found in version 1.2 of the Skein specification document, as follows:

- Section 8.3 ("Threefish Design Decisions," "Rotation constants")
- Section 9.3.1 ("Empirical Observations for Threefish-256")
- Section 9.3.2 ("Empirical Observations for Threefish-512 and Threefish-1024")
- Section 9.5 ("Third-Party Cryptanalysis")
- Section 9.6 ("Empirical Observations for Threefish with Random Rotation Constants")
- Section 9.7 ("Cryptanalysis Summary")
- Appendix B ("Initial Chaining Values")
- Appendix C ("Test Vectors")
- Appendix D ("NIST SHA-3 Round 2 Tweak: Rotation Constants")

In addition, the following items have been updated in the Skein tweak submission package:

- Reference C source code

- Optimized C source code (32-bit and 64-bit)
- Assembly source code (32-bit and 64-bit)
- Test vectors (KAT_MCT directory)