The Skein Hash Function Family

NIST Round 3 Tweak Description

25 Oct 2010

Description of Changes

The only change to the Skein hash function is in the key schedule parity constant, found in Section 3.3.2 of the newly submitted ("tweak") version 1.3 of the Skein specification document. The old constant was the value

$$C_5 \quad = \texttt{0x5555555555555555}.$$

The new constant is

$$C_{240} = \texttt{0x1BD11BDAA9FC1A22}.$$

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 ("Key Schedule Constant,")
- Section 9.3 ("Related-Key Attacks for the Threefish Block Cipher")
- Section 9.5.2 ("Rotational 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 E ("Empirical data for tweaking the key schedule constant")

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)