Tweak of JH for Round 3

January 16, 2011

Hongjun Wu

wuhongjun@gmail.com

1 Tweak of JH

JH is tweaked as follows:
The round number of JH is changed from 35.5 rounds to 42 rounds.

Reasons for the tweak:

1. To improve the hardware efficiency of JH.
   The last half round in the original JH requires additional circuits in hardware implementation. We thus remove the last half round. (The cost of the last half round of AES has been mentioned by Frank K. Gurkaynak in the NIST hash forum.)
2. To increase the security margin.

2 Changes to the report

The following changes are made to the report:

1. Section 7 (bit-slice implementation) is re-organized.
   Section 7 now gives the bit-slice implementation of JH. The details of developing the bit-slice implementation are moved to Appendix B.
2. Section 9.1 and 9.2 are newly added. We explain how to develop the differential and truncated collision attacks against JH.
3. We explain at the beginning of Section 11 why MDS code is used in JH, and explain in Section 11.6 why the (4,2,3) MDS code is used.
4. The examples of differential paths are provided in Appendix D.
5. Following the tweak, the IVs are changed since they are computed from the compression function and the message digest size.

6. Following the tweak, the term “5(d-1)” in the original report is now changed to “6(d-1)”.