Cryptology ePrint Archive: Report 2011/019

Collision Resistance of the JH Hash Function

Jooyoung Lee and Deukjo Hong

Abstract: In this paper, we analyze collision resistance of the JH hash function in the ideal primitive model. The JH hash function is one of the five SHA-3 candidates accepted for the final round of evaluation. The JH hash function uses a mode of operation based on a permutation, while its security has been elusive even in the random permutation model.

One can find a collision for the JH compression function only with two backward queries to the basing primitive. However, the security is significantly enhanced in iteration. For $c\leq n/2$, we prove that the JH hash function using an ideal n-bit permutation and producing c-bit outputs by truncation is collision resistant up to $O(2^{c/2})$ queries. This bound implies that the JH hash function provides the optimal collision resistance in the random permutation model.

Category / Keywords: secret-key cryptography / hash functions

Date: received 10 Jan 2011

Contact author: jlee05 at ensec re kr

Available formats: PDF | BibTeX Citation

Version: 20110114:041323 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]