Cryptology ePrint Archive: Report 2011/238

Attacks On a Double Length Blockcipher-based Hash Proposal

Yiyuan Luo, Xuejia Lai

Abstract: In this paper we attack a $2n$-bit double length hash function proposed by Lee et al. This proposal is a blockcipher-based hash function with hash rate $2/3$. The designers claimed that it could achieve ideal collision resistance and gave a security proof. However, we find a collision attack with complexity of $\Omega(2^{3n/4})$ and a preimage attack with complexity of $\Omega(2^{n})$. Our result shows this construction is much worse than an ideal $2n$-bit hash function.

Category / Keywords: secret-key cryptography / Blockcipher-based, hash functions

Date: received 12 May 2011

Contact author: luoyiyuan at gmail com