Cryptology ePrint Archive: Report 2011/210

The preimage security of double-block-length compression functions

Jooyoung Lee and Martijn Stam and John Steinberger

Abstract: We give improved bounds on the preimage security of the three ``classical'' double-block-length, double-call, blockcipher-based compression functions, these being Abreast-DM, Tandem-DM and Hirose's scheme. For Hirose's scheme, we show that an adversary must make at least 2^{2n-5} blockcipher queries to achieve chance 0.5 of inverting a randomly chosen point in the range. For Abreast-DM and Tandem-DM we show that at least 2^{2n-10} queries are necessary. These bounds improve upon the previous best bounds of $\Omega(2^n)$ queries, and are optimal up to a constant factor since the compression functions in question have range of size 2^{2n}.

Category / Keywords: secret-key cryptography / Hash functions, preimage resistance, ideal cipher model

Date: received 1 May 2011, last revised 1 May 2011

Contact author: stam at cs bris ac uk