Cryptology ePrint Archive: Report 2011/630

Indifferentiability Security of the Fast Widepipe Hash: Breaking the Birthday Barrier

Dustin Moody and Souradyuti Paul and Daniel Smith-Tone

Abstract: The main result of the paper is the solution to a longstanding open problem in the hash function literature: to show that an n-bit iterative hash function can achieve both the rate 1 efficiency, and the indifferentiability security bound that is more than n/2 bits. No hash functions, not even the SHA3 finalists, achieve this property. The Fast Widepipe (FWP) hash mode has been proposed by Nandi and Paul in 2010, as a faster variant of the popular Widepipe (WP) construction proposed by Lucks in 2005. Both FWP and WP can be constructed from an identical primitive; however, FWP enjoys a speed-up factor of at least 2 compared to WP for a reasonable selection of parameter-values. Despite many heuristic arguments provided in favor of the optimal security of FWP, the proven indifferentiability bound for the mode was only up to the birthday barrier of n/2 bits. In this paper, we break the barrier. We improve the bound to 2n/3 bits. We compare the FWP mode with other popular modes with respect to security and efficiency. To the best of our knowledge, this is the first time the indifferentiability security bound of a hash mode with rate 1 has been shown to be beyond the birthday barrier. The novel technique used to break the barrier which is based on the detection of a special set of events -- namely, 3-multi-collision on n bits, n-bit and 2n-bit query collisions -- may be of independent interest; the technique is likely to be applied to other similar rate 1 hash functions such as the JH and the Parazoa family. Our rigorous experiments give evidence that the bound could be further improved, possibly towards very close to n bits.

Category / Keywords: secret-key cryptography / Hash Function, Birthday Barrier, Indifferentiability Framework

Publication Info: A shorter version is in submission to a conference.

Date: received 21 Nov 2011, last revised 16 Jan 2012

Contact author: souradyuti paul at gmail com