Cryptology ePrint Archive: Report 2011/630

Indifferentiability Security of the Fast Wide Pipe Hash: Breaking the Birthday Barrier

Dustin Moody and Souradyuti Paul and Daniel Smith-Tone

Abstract: A hash function secure in the indifferentiability framework (TCC 2004) is able to resist all meaningful generic attacks. Such hash funct also play a crucial role in establishing the security of protocols that use them as random functions.

To eliminate multi-collision type attacks on the MD mode (Crypto 1989), Lucks proposed widening the size of the internal state of hash functio More specifically, he suggested that hash functions h:{0,1}*->{0,1}^n use underlying primitives of the form C:{0,1}^a -> {0,1}^{2n} (Asiacry 2005). The Fast Wide Pipe (FWP) hash mode was introduced by Nandi and Paul at Indocrypt 2010, as a faster variant of Lucks' Wide Pipe m Despite the higher speed, the proven indifferentiability bound of the FWP mode has so far been only up to the birthday barrier of n/2 bits. The m result of this paper is the improvement of the FWP bound to 2n/3 bits (up to an additive constant).

The 2n/3-bit bound for FWP comes with two important implications. Many popular hash modes use primitives with a=2n, that is C:{0,1}^{2n} {0,1}^{2n}. For this important case, the FWP becomes the _only_ mode to achieve indifferentiability security of more than n/2 bits; thus we so longstanding open problem. Secondly, among n-bit hash modes with a>2n, the FWP mode has the highest rate among all modes which have beyond-birthday-barrier security.

To obtain the bound of 2n/3 bits, we follow the usual technique of constructing games with simulators, with certain BAD events to distinguish between the games. However, we introduce some novel ideas. In designing the BAD events, we used multi-collisions in addition to collisions. W also allowed the query-response graphs, maintained by the simulators, to grow for two phases every iteration, rather than just one phase. Finally carefully chosen set of sixteen BAD events establish an isomorphism of simulator graphs, from which the 2n/3-bit bound follows.

We also provide evidence that extending the bound beyond 2n/3 bits may be possible if we allow the simulator-graph to grow for three (or mor phases every iteration. Another noteworthy feature of our proof -- that may be of independent interest -- is that we work with only three games rather than a long sequence games.

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 15 Nov 2012

Contact author: souradyuti paul at esat kuleuven be

Available formats: PDF | BibTeX Citation

Note: The results of the paper are now compared with more modes (e.g. HAMSI) than before, and a few more references on related work we added after taking into account third-party comments and remarks.

Version: 20121115:075841 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]