Cryptology ePrint Archive: Report 2012/722

Hardness Preserving Reductions via Cuckoo Hashing

Itay Berman and Iftach Haitner and Ilan Komargodski and Moni Naor

Abstract: A common method for increasing the usability and uplifting the security of pseudorandom function families (PRFs) is to ``hash" the inputs into a smaller domain before applying the PRF. This approach, known as ``Levin's trick", is used to achieve ``PRF domain extension" (using a short, e.g., fixed, input length PRF to get a variable-length PRF), and more recently to transform non-adaptive PRFs to adaptive ones. Such reductions, however, are vulnerable to a ``birthday attack": after $\sqrt{|\mathcal U|}$ queries to the resulting PRF, where $\mathcal U$ being the hash function range, a collision (i.e., two distinct inputs have the same hash value) happens with high probability. As a consequence, the resulting PRF is insecure against an attacker making this number of queries.

In this work we show how to go beyond the birthday attack barrier, by replacing the above simple hashing approach with a variant of cuckoo hashing --- a hashing paradigm typically used for resolving hash collisions in a table, by using two hash functions and two tables, and cleverly assigning each element into one of the two tables. We use this approach to obtain: (i) A domain extension method that requires just two calls to the original PRF, can withstand as many queries as the original domain size and has a distinguishing probability that is exponentially small in the non cryptographic work. (ii) A security-preserving reduction from non-adaptive to adaptive PRFs.

Category / Keywords: foundations / cuckoo hashing; pseudorandom functions ; hardness preserving reductions; domain extension; non-adaptive to adaptive

Publication Info: TCC 2013 proceedings

Date: received 24 Dec 2012, last revised 24 Dec 2012

Contact author: ilan komargodski at weizmann ac il

Available formats: PDF | BibTeX Citation

Note: Full version.

Version: 20121227:173806 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]