Cryptology ePrint Archive: Report 2011/233

Correlated-Input Secure Hash Functions

Vipul Goyal and Adam O'Neill and Vanishree Rao

Abstract: We undertake a general study of hash functions secure under {\em correlated inputs}, meaning that security should be maintained when the adversary sees hash values of many related high-entropy inputs. Such a property is satisfied by a random oracle, and its importance is illustrated by study of the ``avalanche effect,'' a well-known heuristic in cryptographic hash function design. One can interpret ``security'' in different ways: e.g., asking for one-wayness or that the hash values look uniformly and independently random; the latter case can be seen as a generalization of correlation-robustness introduced by Ishai et al.~ (CRYPTO 2003). We give specific applications of these notions to password-based login and efficient search on encrypted data. Our main construction achieves them (without random oracles) for inputs related by {\em polynomials} over the input space (namely $\zz_p$ for a prime number p), based on corresponding variants of the q-Diffie Hellman Inversion assumption. Additionally, we show relations between correlated-input secure hash functions and cryptographic primitives secure under related-key attacks. Using our techniques, we are also able to obtain a host of new results for such related-key attack secure cryptographic primitives.

Category / Keywords: foundations /

Publication Info: TCC 2011

Date: received 11 May 2011

Contact author: vipul at microsoft com

Available formats: PDF | BibTeX Citation

Note: Full version

Version: 20110517:062434 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]