Cryptology ePrint Archive: Report 2011/252

Cryptography Secure Against Related-Key Attacks and Tampering

Mihir Bellare and David Cash and Rachel Miller

Abstract: We show how to leverage the RKA (Related-Key Attack) security of blockciphers to provide RKA security for a suite of high-level primitives. This motivates a more general theoretical question, namely, when is it possible to transfer RKA security from a primitive P1 to a primitive P2? We provide both positive and negative answers. What emerges is a broad and high level picture of the way achievability of RKA security varies across primitives, showing, in particular, that some primitives resist ``more" RKAs than others. A technical challenge was to achieve RKA security even for the practical classes of related-key deriving (RKD) functions underlying fault injection attacks that fail to satisfy the ``claw-freeness" assumption made in previous works. We surmount this barrier for the first time based on the construction of PRGs that are not only RKA secure but satisfy a new notion of identity-collision-resistance.

Category / Keywords: Related-key attack, tamper-resistance, pseudorandom functions, signatures, identity-based encryption

Publication Info: Preliminary version in Asiacrypt 2011. This is the full version.

Date: received 20 May 2011, last revised 6 Sep 2011

Contact author: mihir at eng ucsd edu

Available formats: PDF | BibTeX Citation

Version: 20110906:203150 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]