Cryptology ePrint Archive: Report 2011/252

A Comparitive Study of Achievability of Security against Related-Key Attack

Mihir Bellare and David Cash and Rachel Miller

Abstract: This paper begins with a practical contribution, namely a way to leverage the RKA security of blockciphers to provide RKA security for a suite of highlevel primitives. This motivates a more general theoretical question, namely, when is it possible to transfer RKA security from a primitive P_1 to a primitive P_2? 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

Date: received 20 May 2011, last revised 25 May 2011

Contact author: mihir at cs ucsd edu