Cryptology ePrint Archive: Report 2013/111

Message Authentication Codes Secure against Additively Related-Key Attacks

Keita Xagawa

Abstract: Message Authentication Code (MAC) is one of most basic primitives in cryptography. After Biham (EUROCRYPT 1993) and Knudsen (AUSCRYPT 1992) proposed related-key attacks (RKAs), RKAs have damaged MAC's security. To relieve MAC of RKA distress, Bellare and Cash proposed pseudo-random functions (PRFs) secure against multiplicative RKAs (CRYPTO 2010). They also proposed PRFs secure against additive RKAs, but their reduction requires sub-exponential time. Since PRF directly implies Fixed-Input Length (FIL) MAC, their PRFs result in MACs secure against multiplicative RKAs. In this paper, we proposed Variable-Input Length (VIL) MAC secure against additive RKAs, whose reductions are polynomial time in the security parameter. Our construction stems from MACs from number-theoretic assumptions proposed by Dodis, Kiltz, Pietrzak, Wichs (EUROCRYPT 2012) and public-key encryption schemes secure against additive RKAs proposed by Wee (PKC 2012).

Category / Keywords: secret-key cryptography / message authentication code, related-key attack

Date: received 25 Feb 2013, last revised 1 Apr 2013

Contact author: xagawa keita at lab ntt co jp

Available formats: PDF | BibTeX Citation

Note: Correct minor typos

Version: 20130401:073034 (All versions of this report)

Discussion forum: Show discussion | Start new discussion