Cryptology ePrint Archive: Report 2011/644

McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes

Ewan Fleischmann and Christian Forler and Stefan Lucks and Jakob Wenzel

Abstract: On-Line Authenticated Encryption (OAE) combines privacy with data integrity and is on-line computable. Most block cipher-based schemes for Authenticated Encryption can be run on-line and are provably secure against nonce-respecting adversaries. But they fail badly for more general adversaries. This is not a theoretical observation only - in practice, the reuse of nonces is a frequent issue. In recent years, cryptographers developed misuse resistant schemes for Authenticated Encryption. These guarantee excellent security even against general adversaries which are allowed to reuse nonces. Their disadvantage is that encryption can be performed in an off-line way, only. This paper introduces a nw family of OAE schemes - called McOE - dealing both with nonce-respecting and with general adversaries. Furthermore, we present three family members, i.e., McOE-X, McOE-D, and McOE-G. All of these members are based on a 'simple' block cipher. In contrast to all other OAE schemes known so far, they provably guarantee reasonable security against general adversaries as well as standard security against nonce-respecting adversaries.

Category / Keywords: secret-key cryptography / authenticated encryption, online encryption, provable security, misuse resistant

Date: received 29 Nov 2011, last revised 2 Mar 2012

Contact author: ewan fleischmann at uni-weimar de

Available formats: PDF | BibTeX Citation

Version: 20120302:084741 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]