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 n 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 again general adversaries which are allowed to reuse nonces. Their disadvantage is that encryption can be performed in an off-line way, only. This pap introduces a new family of OAE schemes --called McOE -- dealing both with nonce-respecting and with general adversaries. Furthermore, we present two family members, i.e., McOE-X and McOE-G. They are based on a 'simple' block cipher. In contrast to every other OAE scheme known in literature, 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

Publication Info: An abridged version of this paper appears in the Proceedings of FSE'12. This is the full version.

Date: received 29 Nov 2011, last revised 31 Oct 2012

Contact author: christian forler at uni-weimar de