Cryptology ePrint Archive: Report 2011/269

Authenticated and Misuse-Resistant Encryption of Key-Dependent Data

Mihir Bellare and Sriram Keelveedhi

Abstract: This paper provides a comprehensive treatment of the security of authenticated encryption (AE) in the presence of key-dependent data, considering the four variants of the goal arising from the choice of universal nonce or random nonce security and presence or absence of a header. We present attacks showing that universal-nonce security for key-dependent messages is impossible, as is security for key-dependent headers, not only ruling out security for three of the four variants but showing that currently standarized and used schemes (all these target universal nonce security in the presence of headers) fail to provide security for key-dependent data. To complete the picture we show that the final variant (random-nonce security in the presence of key-dependent messages but key-independent headers) is efficiently achievable. Rather than a single dedicated scheme, we present a RO-based transform RHtE that endows ANY AE scheme with this security, so that existing implementations may be easily upgraded to have the best possible seurity in the presence of key-dependent data. RHtE is cheap, software-friendly, and continues to provide security when the key is a password, a setting in which key-dependent data is particularly likely. We go on to give a key-dependent data treatment of the goal of misuse resistant AE. Implementations are provided and show that RHtE has small overhead.

Category / Keywords: Authenticated encryption, symmetric encryption, random oracles

Publication Info: Preliminary version appears in proceedings of CRYPTO 2011. This is the full version.

Date: received 26 May 2011, last revised 29 May 2011

Contact author: sriramkr at cs ucsd edu