Cryptology ePrint Archive: Report 2011/107

Threshold Encryption into Multiple Ciphertexts

Martin Stanek

Abstract: We propose (T,N) multi-ciphertext scheme for symmetric encryption. The scheme encrypts a message into N distinct ciphertexts. The knowledge of the symmetric key allows decryption of the original message from any ciphertext. Moreover, knowing T+1 ciphertexts allows efficient recovery of the original message without the key (and without revealing the key as well). We define the security property of the scheme, and prove the security of the proposed scheme. We discuss several variants of the basic scheme that provides additional authenticity and efficiency.

Category / Keywords: secret-key cryptography /

Date: received 4 Mar 2011, last revised 17 May 2011

Contact author: stanek at dcs fmph uniba sk