Cryptology ePrint Archive: Report 2011/486

On the Joint Security of Encryption and Signature, Revisited

Kenneth G. Paterson and Jacob C.N. Schuldt and Martijn Stam and Susan Thomson

Abstract: We revisit the topic of joint security for combined public key schemes, wherein a single keypair is used for both encryption and signature primitives in a secure manner. While breaking the principle of key separation, such schemes have attractive properties and are sometimes used in practice. We give a general construction for a combined public key scheme having joint security that uses IBE as a component and that works in the standard model. We provide a more efficient direct construction, also in the standard model. We then consider the problem of how to build signcryption schemes from jointly secure combined public key schemes. We provide a construction that uses any such scheme to produce a triple of schemes -- signature, encryption, and signcryption -- that are jointly secure in an appropriate and strong security model.

Category / Keywords: public-key cryptography /

Publication Info: Full version of paper to appear at Asiacrypt 2011.

Date: received 8 Sep 2011, last revised 12 Sep 2011

Contact author: kenny paterson at rhul ac uk

Available formats: PDF | BibTeX Citation

Version: 20110912:091818 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]