Cryptology ePrint Archive: Report 2011/592

Generic Constructions for Verifiable Signcryption

Laila El Aimani

Abstract: Signcryption is a primitive which simultaneously performs the functions of both signature and encryption in a way that is more efficient than signing and encrypting separately. We study in this paper constructions of signcryption schemes from basic cryptographic mechanisms; our study concludes that the known constructions require expensive encryption in order to attain confidentiality, however some adjustments make them rest on cheap encryption without compromising their security. Our constructions further enjoy verifiability which entitles the sender or the receiver to prove the validity of a signcryption with/out revealing the \emph{signcrypted} message. They also allow the receiver to release some information which allows anyone to publicly verify a signcryption on a given message. Finally, our constructions accept efficient instantiations if the building blocks belong to a wide class of signature/encryption schemes.

Category / Keywords: cryptographic protocols / signcryption, sign-then-encrypt paradigm, commit-then-encrypt-and sign paradigm, encrypt-then-sign paradigm, (public) verifiability, homomorphic encryption.

Publication Info: ICISC'11

Date: received 2 Nov 2011

Contact author: laila elaimani at yahoo fr