Cryptology ePrint Archive: Report 2011/601

A Multi-Receiver ID-Based Generalized Signcryption Scheme

Caixue Zhou

Abstract: Generalized signcryption(GSC) can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm. In this paper, the formal definition and security notions of multi-receiver identity-based generalized signcryption (MID-GSC) are defined. A concrete scheme is also proposed and proved to be confidential under the Bilinear Diffie-Hellman (BDH) assumption and existential unforgeable under the Computational Diffie-Hellman(CDH) assumption in the random oracle model, which only needs one pairing computation to generalized signcrypt a single message for n receivers using the randomness re-use technique. Compared with other multi-receiver ID-based signcryption schemes, the new scheme is also of high efficiency.

Category / Keywords: public-key cryptography / Multi-receiver identity-based generalized signcryption; Bilinear pairing; Provable security; Randomness re-use; Selective identity security; Random oracle model

Publication Info: no publication

Date: received 6 Nov 2011

Contact author: charlesjjjx at 126 com

Available formats: PDF | BibTeX Citation

Version: 20111110:005926 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]