Cryptology ePrint Archive: Report 2011/156

Strong Forward Security in Identity-Based Signcryption

Madeline González Muñiz and Peeter Laud

Abstract: Due to the possibility of key exposure, forward security in encryption and signing has been well studied, especially in the identity-based setting where an entity's public key is that entity's name. From an efficiency point of view, one would like to use the signcryption primitive and have the best of both worlds. However, strong forward security, where the adversary cannot signcrypt in sender's name nor designcrypt in receiver's name for past time periods even if it has the secrets of both, requires periodic updating of the secret keys of the users. This is an improvement over signcryption schemes that only protect against designcrypting in the past. In this paper, we propose the fi rst ever strong forward secure identity-based signcryption scheme which has public ciphertext veri fiability and a third-party verification protocol.

Category / Keywords: public-key cryptography / forward security, signcryption, pairing-based cryptography, identity-based cryptography

Date: received 29 Mar 2011

Contact author: madeline at research cyber ee