Cryptology ePrint Archive: Report 2011/542

Certificate-Based Signcryption: Security Model and Efficient Construction

Yang Lu and Jiguo Li

Abstract: Signcryption is an important cryptographic primitive that simultaneously achieves confidentiality and authentication in an efficient manner. In 2008, Luo et al. introduced the notion of certificate-based signcryption and proposed the first construction of certificate-based signcryption. However, their scheme is insecure under the key replacement attack and also does not provide insider security. To overcome these disadvantages, we introduce a strengthened security model of certificate-based signcryption in this paper. The new security model accurately models insider security and the key replacement attacks that might be attempted by an adversary in a real certificate-based signcryption system. We also propose a new certificate-based signcryption scheme that reaches insider security and resists key replacement attacks. We show that this scheme is both chosen-ciphertext secure and existentially unforgeable in the random oracle model. Furthermore, performance analysis shows that the proposed scheme is efficient and practical.

Category / Keywords: public-key cryptography / Certificate-based signcryption, Key replacement attack, Insider security, Security model, Chosen-ciphertext security, Existential unforgeability

Publication Info: Unpublished

Date: received 2 Oct 2011

Contact author: luyangnsd at 163 com