Cryptology ePrint Archive: Report 2011/472

Forward Secure Ring Signature without Random Oracles

Joseph K. Liu and Tsz Hon Yuen and Jianying Zhou

Abstract: In this paper, we propose a forward secure ring signature scheme without random oracles. With forward security, if a secret key of a corresponding ring member is exposed, all previously signed signatures containing this member remain valid. Yet the one who has stolen the secret key cannot produce any valid signature belonged to the past time period. This is especially useful in the case of ring signature, as the exposure of a single secret key may result in the invalidity of thousands or even millions ring signatures which contain that particular user. The only one with this feature relies on random oracles to prove the security. We are the first to construct a forward secure ring signature scheme that can be proven secure without random oracles. Our scheme can be deployed in many applications, such as wireless sensor networks and smart grid system.

Category / Keywords: public-key cryptography / Ring Signature

Publication Info: This is the full version of the one in ICICS 2011.

Date: received 31 Aug 2011, last revised 5 Sep 2011

Contact author: ksliu at i2r a-star edu sg