Cryptology ePrint Archive: Report 2013/018

Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption

Jae Hong Seo and Keita Emura

Abstract: In the public key cryptosystems, revocation functionality is required when a secret key is corrupted by hacking or the period of a contract expires. In the public key infrastructure setting, numerous solutions have been proposed, and in the Identity Based Encryption (IBE) setting, a recent series of papers proposed revocable IBE schemes. Delegation of key generation is also an important functionality in cryptography from a practical standpoint since it allows reduction of excessive workload for a single key generation authority. Although fficient solutions for either revocation or delegation of key generation in IBE systems have been proposed, an important open problem is efficiently delegating both the key generation and revocation functionalities in IBE systems. Libert and Vergnaud, for instance, left this as an open problem in their CT-RSA 2009 paper. In this paper, we propose the first solution for this problem. We prove the selective-ID security of our proposal under the Decisional Bilinear Diffie-Hellman assumption in the standard model.

Category / Keywords: public-key cryptography / identity-based encryption, revocation,delegation

Publication Info: An extended abstract will appear at CT-RSA 2013. This is the full version.

Date: received 10 Jan 2013, last revised 20 Jan 2013

Contact author: jhsbhs at gmail com