Cryptology ePrint Archive: Report 2011/583

Revocable Identity-Based Encryption from Lattices

Jie Chen and Hoon Wei Lim and San Ling and Huaxiong Wang and Ta Toan Khoa Nguyen

Abstract: In this paper, we present an identity-based encryption (IBE) scheme from lattices with efficient key revocation. We adopt multiple trapdoors from the Agrawal-Boneh-Boyen and Gentry-Peikerty-Vaikuntanathan lattice IBE schemes to realize key revocation, which in turn, makes use of binary-tree data structure. Using our scheme, key update requires logarithmic complexity in the maximal number of users and linear in the number of revoked users for the relevant key authority. We prove that our scheme is selective secure under the LWE assumption, which is as hard as the worst-case approximating short vectors on arbitrary lattices. Moreover, our key revocation techniques from lattices can be applied to obtain revocable functional encryption schemes in the similar setting.

Category / Keywords: public-key cryptography / Lattice-based Cryptography, Key Revocation, Identity-based Encryption, Functional Encryption

Date: received 27 Oct 2011, last revised 3 Dec 2011

Contact author: s080001 at e ntu edu sg

Note: This work is concurrent but independent from the very recent proposal of lattice-based FIBE. http://eprint.iacr.org/2011/414.

Version: 20111204:041045 (All versions of this report)