Cryptology ePrint Archive: Report 2013/023

A New Practical Identity-Based Encryption System

Jong Hwan Park and Dong Hoon Lee

Abstract: We present a new practical Identity-Based Encryption (IBE) system that can be another candidate for standard IBE techniques. Our construction is based on a new framework for realizing an IBE trapdoor from pairing-based groups, which is motivated from the `two equation' revocation technique suggested by Lewko, Sahai, and Waters. The new framework enables our IBE system to achieve a tight security reduction to the standard Decision Bilinear Diffie-Hellman assumption. Due to its the tightness, our system can take as input the shorter size of security parameters than the previous practical BF, SK, and BB$_{1}$ systems, which provides better efficiency to our system in terms of computational cost. With appropriate parametrization at the current 80-bit security level, our IBE system can obtain 11 times faster decryption than the previous ones and 77 times faster encryption than the BF system. We prove that our system is fully secure against chosen ciphertext attacks in the random oracle model. From computational variant of Naor's observation, we can also suggest a new signature scheme that features a tight security reduction to the Computational Diffie-Hellman assumption and provides strong unforgeability simultaneously.

Category / Keywords: Public-key cryptography / Identity-based encryption, bilinear maps

Publication Info: not yet submitted

Date: received 15 Jan 2013, last revised 15 Jan 2013

Contact author: decartian at korea ac kr