Cryptology ePrint Archive: Report 2011/090

Generic Methods to Achieve Tighter Security Reductions for a Category of IBE Schemes

Yu Chen and Liqun Chen and Zhong Chen

Abstract: We show that Katz-Wang's duplicating key and ciphertext technique can be extended to a generic method that can be used in a certain category of Identity-Based Encryption (IBE) schemes for the purposes of improving their security reductions. We further develop two refined approaches by adapting the randomness reuse technique in the Katz-Wang technique: one is public key duplication, and the other is master key duplication. Compared to the Katz-Wang technique, our two refined approaches do not only improve the performances of the resulting IBE schemes but also enable a reduction algorithm to deal with decryption queries correctly and therefore can achieve chosen ciphertext security. As case studies, we apply these two approaches to modify the Boneh- Franklin IBE scheme and the Boneh-Boyen IBE scheme, respectively. Both of the modifications improve the tightness of security reductions, compared to the original schemes, with a reasonably low cost.

Category / Keywords: public-key cryptography / identity based encryption, provable security, tight reduction, generic method

Publication Info: This is the full version of a paper accepted for publication at ISPEC 2011

Date: received 22 Feb 2011, last revised 28 Feb 2011

Contact author: cycosmic at gmail com