Cryptology ePrint Archive: Report 2011/593

CCA Secure IB-KEM from the Computational Bilinear Diffie-Hellman Assumption in the Standard Model

Yu Chen and Liqun Chen and Zongyang Zhang

Abstract: In this paper, we propose several selective-identity chosen-ciphertext attack secure iden- tity based key encapsulation (IB-KEM) schemes that are provably secure under the computational bilinear Diffie-Hellman (CBDH) assumption in the standard model. Our schemes con favor- ably to previous results in efficiency. With delicate modification, our schemes can be strengthened to be full-identity CCA secure easily.

Category / Keywords: identity based encryption, standard model, CCA security, CBDH assumption

Publication Info: An extended abstract of this paper appears in the Proceedings of the 14th International Conference on Information Security a Cryptology (ICISC 2011).

Date: received 3 Nov 2011, last revised 24 Nov 2011

Contact author: cycosmic at gmail com