CCA-Secure IB-KEM from Identity-Based Extractable Hash Proof Systems

Yu Chen and Zongyang Zhang and Dongdai Lin and Zhenfu Cao

Abstract: In this paper, we introduce a general paradigm called identity-based extractable hash proof system (IB-EHPS), which is an extension of extractable hash proof system (EHPS) proposed by Wee (CRYPTO '10). We show how to construct identity-based key encapsulation mechanism (IB-KEM) from IB-EHPS in a simple and modular fashion. Our construction provides a generic method of building and interpreting CCA-secure IB-KEMs based on computational assumptions. As instantiations, we realize IB-EHPS from the bilinear Diffie-Hellman assumption and the modified bilinear Diffie-Hellman assumption, respectively.

Category / Keywords: public-key cryptography / identity-based extractable hash proof, identity-based key encapsulation mechanism, CCA security, BDH assumption

Publication Info: An extended abstract of this paper has been accepted by ACNS 2012 entitled "Identity-Based Extractable Hash Proofs and Their Applications". This is the full version with newly added materials.

Date: received 24 Jan 2013, last revised 22 Feb 2013

Contact author: cycosmic at gmail com