Cryptology ePrint Archive: Report 2011/543

Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption

Tatsuaki Okamoto and Katsuyuki Takashima

Abstract: This paper proposes the first inner product encryption (IPE) scheme that is adaptively secure and fully attribute-hiding (attribute-hiding in the sense of the definition by Katz, Sahai and Waters), while the existing IPE schemes are either fully attribute-hiding but selectively secure or adaptively secure but weakly attribute-hiding. The proposed IPE scheme is proven to be adaptively secure and fully attribute-hiding under the decisional linear assumption in the standard model. The IPE scheme is comparably as efficient as the existing attribute-hiding IPE schemes. We also present a variant of the proposed IPE scheme with the same security that achieves shorter public and secret keys. A hierarchical IPE scheme can be constructed that is also adaptively secure and fully attribute-hiding under the same assumption. In this paper, we extend the dual system encryption technique by Waters into a more general manner, in which new forms of ciphertext and secret keys are employed and new types of information theoretical tricks are introduced along with several forms of computational reduction.

Category / Keywords: public-key cryptography / Functional Encryption, Predicate Encryption, Attribute-Hiding

Publication Info: This is the full version of a paper appearing in EUROCRYPT 2012, the 31st International Conference on the Theory and Applications of Cryptographic Techniques, April 15-19, 2012, Cambridge, United Kingdom.

Date: received 2 Oct 2011, last revised 26 Jan 2012

Contact author: Takashima Katsuyuki at aj MitsubishiElectric co jp