Cryptology ePrint Archive: Report 2011/648

Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption

Tatsuaki Okamoto and Katsuyuki Takashima

Abstract: In this paper, we present two non-zero inner-product encryption (NIPE) schemes that are adaptively secure under a standard assumption, the decisional linear (DLIN) assumption, in the standard model. One of the proposed NIPE schemes features constant-size ciphert and the other features constant-size secret-keys. Our NIPE schemes imply an identity-based revocation (IBR) system with constant-size ciphert or constant-size secret-keys that is adaptively secure under the DLIN assumption. Any previous IBR scheme with constant-size ciphertexts or constant-size secret-keys was not adaptively secure in the standard model. This paper also presents two zero inner-product encryption (ZIPE) schemes each of which has constant-size ciphertexts or constant-size secret-keys and is adaptively secure under the DLIN assumption in the standard model. They imply an identity-based broadcast encryption (IBBE) system with constant-size ciphertexts or constant-size secret-keys t adaptively secure under the DLIN assumption. We also extend the proposed ZIPE schemes into two directions, one is a fully-attribute-hiding Z scheme with constant-size secret-keys, and the other a hierarchical ZIPE scheme with constant-size ciphertexts.

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

Publication Info: This is the full version of a paper appearing in CANS 2011, the 10th International Conference on Cryptology and Network Security, December 10-12, 2011, Sanya, China.

Date: received 1 Dec 2011, last revised 26 Jul 2012

Contact author: Takashima Katsuyuki at aj MitsubishiElectric co jp