Cryptology ePrint Archive: Report 2011/650

Fully Secure Spatial Encryption under Simple Assumptions with Constant-Size Ciphertexts

Jie Chen and Hoon Wei Lim and San Ling and Huaxiong Wang

Abstract: In this paper, we propose two new spatial encryption (SE) schemes based on existing inner product encryption (IPE) schemes. Both of our SE schemes are fully secure under simple assumptions and in prime order bilinear groups. Moreover, one of our SE schemes has constant-size ciphertexts. Since SE implies hierarchical identity-based encryption (HIBE), we also obtain a fully secure HIBE scheme with constant-size ciphertexts under simple assumptions. Our second SE scheme is attribute-hiding (or anonymous). It has sizes of public parameters, secret keys and ciphertexts that are quadratically smaller than the currently known SE scheme with similar properties. As a side result, we show that negated SE is equivalent to non-zero IPE. This is somewhat interesting since the latter is known to be a special case of the former.

Category / Keywords: public-key cryptography / Functional Encryption, Spatial Encryption, Inner Product Encryption

Date: received 2 Dec 2011

Contact author: s080001 at e ntu edu sg