Cryptology ePrint Archive: Report 2011/455

The Relation and Transformation between Hierarchical Inner Product Encryption and Spatial Encryption

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

Abstract: Hierarchical inner product encryption (HIPE) and spatial encryption (SE) are two important classes of functional encryption (FE) that have a large number of applications. Although HIPE and SE both involve some notion of linear algebra, the former works in vectors while the latter is based on (affine) spaces. Moreover, they currently possess different properties in terms of security, anonymity (payload/attribute-hiding) and ciphertext sizes, for example. In this paper, we formally study the relation between HIPE and SE. In our work, we discover some interesting and novel property-preserving transformation techniques that enable generic construction of an SE scheme from an HIPE scheme, and vice versa.

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

Date: received 19 Aug 2011, last revised 20 Aug 2011

Contact author: s080001 at e ntu edu sg

Available formats: PDF | BibTeX Citation

Version: 20110820:155351 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]