Cryptology ePrint Archive: Report 2011/692

Fully Secure (Doubly-)Spatial Encryption under Simpler Assumptions

Cheng Chen and Zhenfeng Zhang and Dengguo Feng

Abstract: Spatial encryption was first proposed by Boneh and Hamburg in 2008. It is one implementation of the generalized identity-based encryption schemes and many systems with a variety of properties can be derived from it. Recently, Hamburg improved the notion by presenting a variant called doubly-spatial encryption. The doubly spatial encryption is more powerful and expressive. More useful cryptography systems can be builded from it, such as attribute-based encryption, etc. However, most presented spatial encryption schemes are proven to be selectively secure. Only a few spatial encryption schemes achieve adaptive security, but not under standard assumptions. And no fully secure doubly-spatial encryption scheme has been presented before. In this paper, we primarily focus on the adaptive security of (doubly-)spatial encryption. A spatial encryption scheme and a doubly-spatial encryption scheme have been proposed. Then we apply the dual system methodology proposed by Waters in the security proof. Both of the schemes can be proven adaptively secure under standard assumptions, the decisional linear (DLIN) assumption and the decisional bilinear Diffie-Hellman (DBDH) assumption, over prime order groups in the standard model. To the best of our knowledge, our second scheme is the first fully secure construction of doubly-spatial encryption.

Category / Keywords: public-key cryptography / spatial encryption, adaptive security, dual system encryption

Publication Info: submitted to conference

Date: received 20 Dec 2011

Contact author: chencheng at is iscas ac cn

Available formats: PDF | BibTeX Citation

Version: 20111223:122035 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]