Cryptology ePrint Archive: Report 2011/389

Spatial Encryption

Mike Hamburg

Abstract: In this thesis, we build on Boneh and Hamburg's work on generalized identity-based encryption and spatial encryption. GIBE is a model that covers many of the generalizations of identity-based cryptography that have appeared in the past decade. It is simple and flexible, and can be tuned to different attack models such as selective security.

Spatial encryption is an encryption system within the GIBE model. It is designed as a toolbox from which other encryption systems can be built, using linear algebra as an encoding method. It is based on the work of Boneh, Boyen and Goh, and generalizes hierarchical IBE as well as the hierarchical inner-product encryption of Okamoto and Takashima.

Here we show several new results related to spatial encryption. We show how to build adaptively secure spatial systems (under a compact but nonstandard assumption) using Lewko and Waters' dual-system encryption. In doing this, we also show how to adapt Lewko and Waters' result to a prime-order setting without sacrificing constant-size ciphertexts. We also show new embeddings of other cryptosystems into spatial encryption.

Beyond spatial encryption, we propose a variant called "doubly-spatial encryption", which generalizes both spatial encryption and Attrapadung and Libert's "negated spatial encryption". This generalization adds more flexibility, including more flexible revocation systems and potential improvements in policy language. Unfortunately, we were only able to prove selective security for doubly-spatial encryption, and its ciphertext is no longer constant-size.

Category / Keywords: public-key cryptography / identity-based encryption, spatial encryption

Publication Info: Stanford University thesis, 2011

Date: received 17 Jul 2011

Contact author: mike at shiftleft org