Agrawal, Shweta; **Boneh, Dan**; **Boyen, Xavier**

Efficient lattice (H)IBE in the standard model. (English) Zbl 1227.94022

Gilbert, Henri (ed.), Advances in cryptology – EUROCRYPT 2010. 29th annual international conference on the theory and applications of cryptographic techniques, French Riviera, May 30 – June 3, 2010. Proceedings. Berlin: Springer (ISBN 978-3-642-13189-9/pbk). Lecture Notes in Computer Science 6110, 553-572 (2010).

Summary: We construct an efficient identity-based encryption system based on the standard learning with errors (LWE) problem. Our security proof holds in the standard model. The key step in the construction is a family of lattices for which there are two distinct trapdoors for finding short vectors. One trapdoor enables the real system to generate short vectors in all lattices in the family. The other trapdoor enables the simulator to generate short vectors for all lattices in the family except for one. We extend this basic technique to an adaptively-secure IBE and a Hierarchical IBE.

For the entire collection see [Zbl 1188.94008].

MSC:

94A60 Cryptography

Keywords:

identity-based encryption; learning with errors; Hierarchical IBE

Full Text: DOI