Gama, Nicolas; **Nguyen, Phong Q.**; **Regev, Oded**

Lattice enumeration using extreme pruning. (English) Zbl 1280.94056

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, 257-278 (2010).

Summary: Lattice enumeration algorithms are the most basic algorithms for solving hard lattice problems such as the shortest vector problem and the closest vector problem, and are often used in public-key cryptanalysis either as standalone algorithms, or as subroutines in lattice reduction algorithms. Here we revisit these fundamental algorithms and show that surprising exponential speedups can be achieved both in theory and in practice by using a new technique, which we call extreme pruning. We also provide what is arguably the first sound analysis of pruning, which was introduced in the 1990s by Schnorr et al.

For the entire collection see [Zbl 1188.94008].

MSC:

94A60 Cryptography

Full Text: DOI