Hanrot, Guillaume; **Pujol, Xavier**; **Stehlé, Damien**

Analyzing blockwise lattice algorithms using dynamical systems. (English) Zbl 1287.94072

Rogaway, Phillip (ed.), Advances in cryptology – CRYPTO 2011. 31st annual cryptology conference, Santa Barbara, CA, USA, August 14–18, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-22791-2/pbk). Lecture Notes in Computer Science 6841, 447-464 (2011).

Summary: Strong lattice reduction is the key element for most attacks against lattice-based cryptosystems. Between the strongest but impractical HKZ reduction and the weak but fast LLL reduction, there have been several attempts to find efficient trade-offs. Among them, the BKZ algorithm introduced by *C. P. Schnorr* and *M. Euchner* [Math. Program. 66, No. 2(A), 181–199 (1994; Zbl 0829.90099); FCT 1991, Lect. Notes Comput. Sci. 529, 68–85 (1991; Zbl 0925.11049)] seems to achieve the best time/quality compromise in practice. However, no reasonable complexity upper bound is known for BKZ, and *N. Gama* and *P. Q. Nguyen* [Eurocrypt 2008, Lect. Notes Comput. Sci. 4965, 31–51 (2008; Zbl 1149.94314)] observed experimentally that its practical runtime seems to grow exponentially with the lattice dimension. In this work, we show that BKZ can be terminated long before its completion, while still providing bases of excellent quality. More precisely, we show that if given as inputs a basis $(b_i)_{i\leq n} \in \mathbb{Q}^{n\times n}$ of a lattice L and a block-size β, and if terminated after

$$\Omega\left(\frac{n^3}{\beta^2}(\log n + \log\log \max_i \|b_i\|)\right)$$

calls to a β-dimensional HKZ-reduction (or SVP) subroutine, then BKZ returns a basis whose first vector has norm

$$\leq 2\nu_\beta^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det L)^{\frac{1}{n}},$$

where $\nu_\beta \leq \beta$ is the maximum of Hermite's constants in dimensions $\leq \beta$. To obtain this result, we develop a completely new elementary technique based on discrete-time affine dynamical systems, which could lead to the design of improved lattice reduction algorithms.

For the entire collection see [Zbl 1219.94002].

MSC:

94A60 Cryptography
68Q25 Analysis of algorithms and problem complexity
11H06 Lattices and convex bodies (number-theoretic aspects)

Cited in **17** Documents

Keywords:

Euclidean lattices; BKZ; lattice-based cryptanalysis

Software:

NTRU

Full Text: DOI

© 2021 FIZ Karlsruhe GmbH