Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van

Stellingen

behorende bij het proefschrift
"Lattice Cryptography, from Cryptanalysis to New Foundations"

(i) When implemented on GPUs with tensor cores, sieving algorithms can solve a shortest vector challenge in a lattice of dimension 180 within 2 months. This improves about two orders of magnitude upon previous records in terms of wall-clock time and energy efficiency.

(ii) There exists an efficient estimator that, contrary to known loose asymptotic bounds, predicts precisely when and how the BKZ algorithm discovers the dense sublattice of an NTRU lattice.

(iii) Lattices and codes are often treated as separate research areas, but they are closely related. In particular, there exists a translation of the LLL algorithm to binary codes with the Hamming metric.

(iv) Most geometric properties of a lattice can be hidden simply by rotating the lattice and randomizing the basis, and this can be used for cryptography. Based on this, every efficiently decodable lattice can be turned into an encryption scheme, while every efficiently Gaussian sampleable lattice can be turned into a signature scheme.

(v) Cryptology should have a careful balance between creating and breaking assumptions. Today, however, creators of new assumptions rarely behave as breakers. This can lead to a bias towards applicability, and not security.

(vi) Lattice-based cryptography and cryptanalysis should go back to its geometric roots. From this perspective, limiting research to only LWE, SIS and NTRU lattices introduces artificial constraints.

(vii) Lattice sieving is faster than enumeration, both in theory and in practice.

(viii) In practice and contrary to theory, the hardness of unique-SVP has seemingly nothing to do with the uniqueness of the shortest vector, but only with its (unusual) length.

(ix) Scientists should not only show the results of computational experiments, but also strive to make their code available, open-source and runnable.

(x) Not actively thinking about a problem, for example by taking a walk or a nap, can be more productive than overstraining one's mind.

Wessel van Woerden
Leiden, February 23, 2023