Lattices Algorithms in Cryptography

Bachelor Thesis Proposal

Léo Ducas

Lattices have two facets in cryptography: for a while, they have been mainly used for cryptanalysis (1), and recently they have also become a versatile tool for the construction secure cryptosystems (2). The topic of the Bachelor Thesis may be chosen among this two facets.

Lattices are discrete subgroups of finite-dimensional euclidean vector spaces. In particular lattices have $\mathbb{Z}$-bases but unlike euclidean vector spaces, lattices do not necessary admit an *orthogonal* basis. A fundamental algorithmic task is, given a basis of a lattice, to *reduce* it, i.e. finding a basis that is close to being orthogonal, in some quantifiable sense.

The two metrics of interest for a reduction algorithm are its running time, and its quality, i.e. a measure of how close to orthogonal the output basis is. Even though some reduction algorithms run time polynomial in the rank d of the lattice, finding a very good basis requires exponential time. Once in possession of a good enough basis, other algorithmic tasks of interest – such as CVP, the *close vector problem* – become solvable.

1) Lattice Reduction for Cryptanalysis

The famous LLL algorithm [1] was the first to provide bases of useful quality in *polynomial time*. Even though LLL-reduced bases can remain quite far from orthogonal, they are good enough for many applications, including cryptanalysis of various kind of cryptosystems (knapsack, RSA, elliptic curves ...).

The LLL algorithm proceeds *locally*, namely by optimizing bases of 2-dimensional projected sub-lattices, and repeating this subroutine until not much more progress can be achieved. The running time of LLL can be analyzed using a so-called *sandpile argument*. More interestingly, the design of LLL can be seen as a (relaxed) algorithmic version of the proof of Hermite's inequality $\gamma_d \leq \gamma_2^{d-1}$, one of the earliest bounds on *dense sphere packing*.

The student is invited to get acquainted with the LLL algorithm and its properties [2]. From there, a possible development is to study a generalization of LLL [3], where the local optimization is done on sub-lattice of dimension $k > 2$. Again, a parallel is to be made with a bound on sphere packing, namely Mordell's inequality $\gamma_d \leq \gamma_k^{(d-1)/(k-1)}$.

The student may also explore applications of LLL in cryptanalysis, e.g. for *factorization* [4].

2) Sampling Discrete Gaussian over a Lattice

As mentioned earlier, knowing very good basis of a lattice allows to quickly solve CVP while it remains exponentially slower knowing only a bad basis or even an LLL-reduced basis. This suggest the construction of *asymmetric cryptography protocols*, where a very good basis can be chosen first and used as a secret key, and from which a bad basis can be derived to be used as a public key.

Unfortunately, the standard algorithm to solve CVP – Babai's *nearest plane algorithm* – is not suitable for all cryptographic application because it reveals a good *tiling* of the lattice. Therefore a *statistical learning attack* [5] can recover the secret key. To thwart learning attacks, a technique called *Gaussian Sampling* was developed. The idea is to replace the deterministic rounding step of Babai by a discrete Gaussian distribution that *smoothes out* the lattice tiles.

The project may start with the study of the learning attack, motivating the Gaussian Sampling technique. After studying the Gaussian Sampling algorithm over general lattices, the student can also explore optimizations [6] of this algorithm over the *structured lattices* which are used for cryptographic constructions. Typically, those structured lattices are modules over some cyclotomic ring $\mathbb{Z}[\zeta_n]$. This topic of research is relatively young, and there is certainly room for new ideas.

References

[1] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[2] Phong Q Nguyen. Hermites constant and lattice algorithms. In *The LLL Algorithm*, pages 19–69. Springer, 2010.

[3] Nicolas Gama and Phong Q Nguyen. Finding short lattice vectors within mordell's inequality. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 207–216. ACM, 2008.

[4] Alexander May. Using LLL-reduction for solving RSA and factorization problems. In *The LLL algorithm*, pages 315–348. Springer, 2010.

[5] Phong Q Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In *Advances in Cryptology-EUROCRYPT 2006*, pages 271–288. Springer, 2006.

[6] Léo Ducas. *Lattice Based Signatures: Attacks, Analysis and Optimization.* PhD thesis, École Normale Supérieure de Paris and Université Paris Diderot, 2013.