Lattices and Cryptography: an Overview

Jacques Stern
Jacques.Stern@ens.fr

Ecole Normale Supérieure
Laboratoire d'informatique
45, rue d'Ulm
75230 Paris Cedex 05

Abstract. We briefly discuss the history of lattices and cryptography during the last fifteen years.

A lattice is a discrete subgroup of $\mathbf{R}^n$ or equivalently the set $L$

$$\lambda_1 b_1 + \cdots + \lambda_p b_p$$

of all integral linear combination of a given set of independant $n$-dimensional vectors $b_1, \cdots, b_p$. The sequence $(b_1, \cdots, b_p)$ is said to be a basis of $L$ and $p$ is its dimension.

From the mathematical point of view, the history of lattice reduction goes back to the theory of quadratic forms developed by Lagrange, Gauss, Hermite, Korkine-Zolotareff and others (see [Lag73, Gau01, Her50, KZ73]) and to Minkowski's geometry of numbers ([Min10]).

With the advent of algorithmic number theory, the subject had a revival around 1980. Two basic problems have emerged: the shortest vector problem (SVP) and the closest vector problem (CVP). SVP refers to the question of computing the lattice vector with minimum non-zero euclidean length while CVP addresses the non-homogeneous analog of finding a lattice element minimizing the distance to a given vector. It has been known for some time that CVP is NP-complete [Boa81] and Ajtai has recently proved that SVP is NP-hard for polynomial random reductions [Ajt97].

The celebrated LLL algorithm computes a so-called reduced basis of a lattice and provides a partial answer to SVP since it runs in polynomial time and approximates the shortest vector within a factor of $2^{\sqrt{n}/2}$. Actually, a reduction algorithm of the same flavor had already been included in Lenstra's work on integer programming (cf. [Len83], circulated around 1979) and the lattice reduction algorithm reached a final form in the paper [LLL82] of Lenstra, Lenstra and Lovász, from which the name LLL algorithm comes. Further refinements of the LLL algorithm were proposed by Schnorr ([Sch87, Sch88]), who has improved the above factor into $(1 + \epsilon)^n$. Babai [Bab86] gave an algorithm that approximates the closest vector by a factor of $(3/\sqrt{2})^n$. The existence of polynomial bounds is completely open: CVP is hard to approximate within a factor $2^{(\log n)^{0.89}}$ as shown in [ABSS97] but a result of Goldreich and Goldwasser [GG] suggests that it is hopeless to try to extend this inapproximability result to $\sqrt{n}$. 
The relevance of lattice reduction algorithms to cryptography was immediately understood: in April 1982, Shamir ([Sha82]) found a polynomial time algorithm breaking the Merkle-Hellman public key cryptosystem ([MH78]) based on the knapsack problem, that had been basically the unique alternative to RSA. Shamir used Lenstra's integer programming algorithm but, the same year, Adleman ([Ad83]) extended Shamir's work by treating the cryptographic problem as a lattice problem rather than a linear programming problem. Further improvements of these methods were obtained by Brickell ([Bri84, Bri85]), by Lagarias and Odlyzko ([LO85]), and, more recently by Coster, La Macchia, Odlyzko, Schnorr and the authors ([CJL+92]).

Lattice reduction has also been applied successfully in various other cryptographic contexts: against a version of Blum's protocol for exchanging secrets ([FKH+88]), against truncated linear congruential generators ([FKH+88, Ste87]), against cryptosystems based on rational numbers ([ST90]) or modular knapsacks ([JS91, CJ91]), and, more recently, against RSA with exponent 3 ([Cor96]) and in order to attack a new cryptosystem proposed by Hoffstein, Pipher and Silverman under the name NTRU (see [CS97]).

Recently, in a beautiful paper, Ajtai [Ajt96] discovered a fascinating connection between the worst-case complexity and the average-case complexity of some well-known lattice problems. More precisely, he established a reduction from the problem of finding the shortest non-zero element \( u \) of a lattice provided that it is “unique” (i.e. that it is polynomially shorter than any other element of the lattice which is not linearly related) to the problem of approximating SVP for randomly chosen instances of a specific class of lattices. This reduction was improved in [CN97]. Later, Ajtai and Dwork [AD97] proposed a cryptosystem based on Ajtai’s theorem. Actually, they introduced three such systems which we will describe as AD1, AD2 and AD3 and showed that the third was provably secure under the assumption that the “unique” shortest vector problem considered above is difficult. The same year, Goldreich, Goldwasser and Halevy [GGH97] proposed another cryptosystem based on lattices.

Again, from a theoretical point of view, the achievement in the Ajtai-Dwork paper is a masterpiece. However, its practical significance is unclear. At the “rump” session of CRYPTO'97, Phong Nguyen, Victor Shoup and the author reported on initial experiments on the cryptosystem AD1: their conclusion was that, in order to be secure, practical implementations of AD1 would require lattices of very high dimension. This would lead to a totally impractical system requiring a message of more than one megabyte to simply exchange a DES key. At the same rump session, Claus Schnorr and his students announced that they had broken many instances of the scheme proposed by Goldreich, Goldwasser and Halevy. Later, my student Phong Nguyen could break even larger instances.

Does this mean that lattice cryptosystems cannot be practically viable. Extensive experiments have to be carried out but there is some theoretical indication that it might well be the case. Together with Phong Nguyen [NS], we have established a converse to the Ajtai-Dwork security result by reducing the question of distinguishing encryptions of one from encryptions of zero to approximating
CVP or SVP (recall that AD encrypts bits). In a way, it becomes possible to reverse the basic paradigm of the AD cryptosystem “If lattice problems are difficult, then AD is difficult” into the following “If lattice problems are easy, then AD is insecure”. It remains to understand which of the two paradigms is the right one.

References


This article was processed using the \LaTeX{} macro package with LLNCS style.