Lattices and Cryptography: an Overview

Jacques Stern
Jacques.Stern@ens.fr

Ecole Normale Suprieure
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 sequnece $(b_1, \cdots, b_p)$ 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 $2^{n/2}$. 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 $2^{(\log n)^{0.99}}$ 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 ([Adl83]) 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 ([FHK$^+$88]), against truncated linear congruential generators ([FHK$^+$88, Ste87]), against cryptosystems based on rational numbers ([ST90]) or modular knapsacks ([JS91, CJS91]), and, more recently, against RSA with exponent 3 ([Cop96]) 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 acheme 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 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

[ABSS97] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317–331, 1997.

[AD97] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th ACM Symposium on Theory of Computing*, pages 284–293, 1997.

[Adl83] L. M. Adleman. On breaking generalized knapsack public key cryptosystems. In *Proc. 15th ACM Symposium on Theory of Computing*, pages 402–412, 1983.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th ACM Symposium on Theory of Computing*, pages 99–108, 1996.

[Ajt97] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. Unpublished manuscript, May 1997.

[Bab86] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[Boa81] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, Mathematische Instituut, University of Amsterdam, 1981. Report 81-04.

[Bri84] E. F. Brickell. Solving low density knapsacks. In D. C. Chaum, editor, *Proceedings of CRYPTO 83*, pages 25–37. Plenum Press, New York, 1984.

[Bri85] E. F. Brickell. Breaking iterated knapsacks. In G. R. Blakley and D. C. Chaum, editors, *Proceedings CRYPTO 84*, pages 342–358. Springer, 1985. Lecture Notes in Computer Science No. 196.

[CJL+92] M. J. Coster, A. Joux, B. A. LaMacchia, A. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2:11–28, 1992.

[CJS91] Y. M. Chee, A. Joux, and J. Stern. The cryptanalysis of a new public-key cryptosystem based on modular knapsacks. In J. Feigenbaum, editor, *Advances in Cryptology: Proceedings of Crypto'91*, volume 576 of *LNCS*, pages 204–212. Springer-Verlag, 1991.

[CN97] J.-Y. Cai and A. P. Nerurkar. An improved worst-case to average-case connection for lattice problems. In *Proc. 38th IEEE Conference on Foundations of Computer Science*, pages 468–477, 1997.

[Cop96] D. Coppersmith. Finding a small root of a univariate modular equation. In U. Maurer, editor, *Proceedings of EUROCRYPT 96*, pages 155–165. Springer, 1996. Lecture Notes in Computer Science No. 1070.

[CS97] D. Coppersmith and A. Shamir. Lattice attacks on NTRU. In W. Fumy, editor, *Proceedings of EUROCRYPT 97*, pages 52–61. Springer, 1997. Lecture Notes in Computer Science No. 1233.

[FHK+88] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM J. Computing*, 17(2):262–280, April 1988.

[Gau01] C.F. Gauss. Disquisitiones arithmeticae. Leipzig, 1801.

[GG] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. Preprint. Revision of ECCC Report TR97-031, Oct 16, 1997. Can be found at `http://www.eccc.uni-trier.de/eccc/`.

[GGH97] O. Goldreich, S. Goldwasser, and S. Halevy. Public-key cryptography from lattice reduction problems. In *Proc. CRYPTO'97*, volume 1294 of *LNCS*, pages 112–131, 1997.

[Her50] C. Hermite. Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre. *J. Reine Angew. Math*, 40:279–290, 1850.

[JS91] A. Joux and J. Stern. Cryptanalysis of another knapsack cryptosystem. In *Advances in Cryptology: Proceedings of AsiaCrypt'91*, volume 739 of *Lecture Notes in Computer Science*, pages 470–476. Springer-Verlag, 1991.

[KZ73] A. Korkine and G. Zolotarev. Sur les formes quadratiques. *Math. Ann.*, 6:336–389, 1873.

[Lag73] L. Lagrange. *Recherches d'arithmétique*, pages 265–312. Nouv. Mém. Acad., Berlin, 1773.

[Len83] H. W. Lenstra. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8:538–548, 1983.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Methematische Ann.*, 261:513–534, 1982.

[LO85] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *J. ACM*, 32:229–246, 1985. Preliminary version in Proc. 24th IEEE Foundations Computer Science Symposium, 1–10, 1983.

[MH78] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inform. Theory*, IT-24:525–530, September 1978.

[Min10] H. Minkowski. *Geometrie der Zahlen*. Teubner, Leipzig, 1910.

[NS] P. Nguyen and J. Stern. A converse to the Ajtai-Dwork security result and its cryptographic implications. submitted to STOC 98.

[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[Sch88] C.-P. Schnorr. A more efficient algorithm for lattice basis reduction. *J. Algorithms*, 9:47–62, 1988.

[Sha82] A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, pages 145–152. IEEE, 1982.

[ST90] J. Stern and P. Toffin. Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers. In *Advances in Cryptology: Proceedings of Eurocrypt'90*, volume 473 of *Lecture Notes in Comp Sci*, pages 313–317. Springer-Verlag, 1990.

[Ste87] J. Stern. Secret linear congruential generators are not cryptographically secure. In *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pages 421–426. IEEE, 1987.