

# PhD Thesis proposal

## Probabilistic analysis of “cryptographic” lattices

*Supervisor:* Brigitte VALLÉE, Directrice de Recherche au CNRS

*Co-supervisors:*

Julien CLÉMENT, Chargé de Recherche au CNRS,

Fabien LAGUILLAUMIE, Maître de conférences à l’Université de Caen

emails: {brigitte.vallee,julien.clement,fabien.laguillaumie}@info.unicaen.fr

Laboratoire GREYC (Université de Caen, ENSICAEN et CNRS)  
Boulevard du Maréchal Juin, BP 5186, 14032 Caen Cedex, France.

**Context.** A central object in the geometry of numbers is the *lattice*, defined informally as a regular arrangement of points in an Euclidean space. One of the essential algorithmic problems in geometry of numbers consists in lattice reduction, that is finding a good basis, with good Euclidean qualities. A very good basis is most surely out of reach in polynomial time. However there exist algorithms that find a “quite good” basis in polynomial time, the most famous amongst these being the LLL algorithm [7].

The common history between cryptography and geometry of numbers is already long and fruitful. Indeed, in an unexpected manner, many cryptographic systems are linked to lattices, either because these systems are based on a difficult algorithmic problem on lattices (like in the cryptosystems of Ajtai-Dwork [1], or those of Peikert [8],...), either because the cryptosystems, or more specifically, their cryptanalyses can be reduced to a lattice problem. In particular, each time a system relies on a linear problem, or can be efficiently linearised, lattices are a very efficient tool for cryptanalysis: one maps a cryptographic instance to a lattice instance and the cryptanalysis consists in finding a small vector. Lattices involved in this cryptographic framework will be called in the following *cryptographic lattices*. These lattices are very peculiar, and, especially, can not be considered at all as “generic”.

In order to get a better view of the security of such cryptosystems, one has to evaluate the difficulty of lattice reduction on these particular lattices. Is it easier or more difficult to reduce a cryptographic lattice than a generic lattice? Is the shortest vector of such a lattice really short? And then, if the cryptographic security is to be considered in a realistic way, one has to ponder these questions in a probabilistic manner, the probabilistic model being tightly linked to geometric characteristics of cryptographic lattices.

**Objectives.** These cryptographic lattices are diverse in nature, depending on which problems they come from. For instance, the Coppersmith method [5], which allows to find “small” roots of univariate polynomials modulo an integer, or of multivariate polynomials, showed its extreme efficiency for the cryptanalysis of several variants of RSA [3, 6]. More generally, this technique is very efficient as soon as the attack can be formulated as a resolution of a system of polynomial equations. The underlying lattices, designated as Coppersmith lattices, are very particular, but also very different from other cryptographic lattices, like the ones encountered in the NTRU system, and systems based upon “knapsack” problems.

The specific study of cryptographic lattices (coming either from a cryptanalysis, or being the root of a cryptosystem) yields fundamental issues on the behaviour of reduction algorithms as well as on the geometric characteristics of these lattices. And these questions need to be considered probabilistically. In small dimension, these questions have been precisely answered [10, 11]. A similar study on cryptographic lattices could allow to explain the observations made in practice. This could also lead to algorithmic optimisation taking into account the specific geometric nature of these lattices.

**PhD Thesis Proposal.** The proposal (at the interface between cryptography, geometry of numbers, algorithmic of lattice reduction and probabilistic analysis of algorithms) focuses on the efficiency of lattice-based cryptanalyses and on the precise evaluation of the security of lattice-based cryptosystems. The geometric and algorithmic properties of these “cryptographic” lattices are still not well understood. The novelty of the proposed approach lies in its probabilistic point of view, in opposition to the usual “worst-case” setting.

This work is related to the LAREDA project of the “ANR blanche” (<http://lamfa.u-picardie.fr/paccaut/lareda/>)

**Qualifications.** Cryptology, algebra and arithmetic, computational number theory, probability, algorithmics, analysis of algorithms, C/C++.

## References

- [1] M. Ajtai and C. Dwork. *A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence*. Proc of STOC'97, pp. 284-293 (1997).
- [2] A. Bauer and A. Joux. *Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables*. Proc. of Eurocrypt'07, Springer LNCS Vol. 4515, pp. 361–378 (2007).
- [3] D. Boneh and G. Durfee. *Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$*  by IEEE Transactions on Information Theory, Vol 46, No. 4, pp. 1339–1349 (2000).
- [4] D. Boneh, G. Durfee, and N. Howgrave-Graham. *Factoring  $N = p^r q$  for large  $r$* . Proc. of Crypto '99, Springer LNCS Vol. 1666, pp. 326–337 (1999).
- [5] D. Coppersmith. *Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities*. J. Cryptology 10(4), pp. 233–260 (1997).
- [6] Matthias Ernst, Ellen Jochemsz, Alexander May and Benne de Weger *Partial Key Exposure Attacks on RSA up to Full Size Exponents*. Proc. of Eurocrypt'05, Springer LNCS Vol. 3494, pp. 371–386 (2005).
- [7] A.K. Lenstra, H. W. Lenstra, L. and Lovász. *Factoring Polynomials with Rational Coefficients*. Math. Ann. 261, pp. 515–534 (1982).
- [8] C. Peikert. *Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem*. To appear, STOC'09.
- [9] D. Stehlé. *On the Randomness of Bits Generated by Sufficiently Smooth Functions*. Proc. of ANTS VII, Springer LNCS Vol. 4078, pp. 257–274 (2006).
- [10] B. Vallée, A. Vera. *Lattice Reduction in two dimensions: analyses under realistic probabilistic models*, Proceedings of the conference AofA'07, *Discrete Mathematics and Theoretical Computer Science*, proc AH, 2007, 181-216.
- [11] B. Vallée, A. Vera. *Probabilistic analysis of Lattice Reduction Algorithms*, Proceedings of the conference LLL+25, to appear in *Information Security and Cryptography series, Springer*.