The Two Faces of Lattices in Cryptology

Phong Q. Nguyen

École Normale Supérieure, Département d'Informatique,
45 rue d'Ulm, 75005 Paris, France
pnguyen@ens.fr and http://www.di.ens.fr/~pnguyen/

Abstract. Lattices are regular arrangements of points in n-dimensional space, whose study appeared in the 19th century in both number theory and crystallography. Since the appearance of the celebrated Lenstra-Lenstra-Lovász lattice basis reduction algorithm twenty years ago, lattices have had surprising applications in cryptology. Until recently, the applications of lattices to cryptology were only negative, as lattices were used to break various cryptographic schemes. Paradoxically, several positive cryptographic applications of lattices have emerged in the past five years: there now exist public-key cryptosystems based on the hardness of lattice problems, and lattices play a crucial rôle in a few security proofs. In this talk, we will try to survey the main examples of the two faces of lattices in cryptology. The full material of this talk appeared in [2]. A preliminary version can be found in [1].

References

1. P. Q. Nguyen and J. Stern. Lattice reduction in cryptology: An update. In *Algorithmic Number Theory, Proc. of ANTS-IV*, volume 1838 of *LNCS*. Springer-Verlag, 2000.
2. P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Cryptography and Lattices, Proc. of CALC '01*, volume 2146 of *LNCS*. Springer-Verlag, 2001.

S. Vaudenay and A. Youssef (Eds.): SAC 2001, LNCS 2259, p. 313, 2001.