Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

A New Design for Lattice-Based Cryptosystems

Charles F. de Barros[1]
Graduate Program in Informatics (PPGI), UFRJ, Rio de Janeiro, RJ
Luis Menasché Schechter[2]
Department of Computer Science (DCC), UFRJ, Rio de Janeiro, RJ

Abstract. We present a new mathematical problem related to the theory of lattices, which may be used as an underlying problem to new public-key cryptosystems.

Keywords. Cryptography, Lattices, Complexity

1 Lattices and Perturbations

Lattices are additive subgroups of $\mathbb{R}^n$. After the theoretical work of Ajtai and Dwork [1], the first practical proposal of a lattice-based cryptographic construction was made by Goldreich, Goldwasser and Halevi, the so-called GGH [2]. Two years after its creation, GGH was broken by Nguyen [4], and since then it has been regarded as a dead system.

Recently, Yoshino and Kunihiro proposed some improvements on GGH [6]. However, practical interest on this scheme has been overshadowed by the appearance of more efficient cryptosystems, such as NTRU [3], and elegant constructions based on the Learning With Errors (LWE) problem, originally presented by Regev [5].

The security of public-key cryptosystems relies on the hardness of solving some mathematical problem. There are two main problems underlying lattice-based cryptographic constructions: the closest vector problem (CVP) and the shortest vector problem (SVP). There are also variants such as SIVP (Shortest Independent Vectors Problem) and Gap-SVP, and the already mentioned LWE and its variant ring-LWE.

We are currently working on a new lattice problem, which consists of recovering a lattice basis from a given *perturbed* basis. A *perturbation* on a lattice basis B consists of adding a real matrix E to B. A precise definition of the problem is given below:

Definition 1.1 (Lattice Perturbation Problem)**.** *Consider that a lattice basis B was perturbed by a matrix E. We are given only the basis $B + E$, and we are asked to find a lattice basis R such that* $|\det(R)| = |\det(B)|$.

In a strong version of this problem, we are given no information about the matrices B and E. In this case, we have to deal with infinitely many candidate solutions, and there

[1] charles.barros@ppgi.ufrj.br
[2] luisms@dcc.ufrj.br

DOI: 10.5540/03.2015.003.02.0022

is no way of knowing when the correct one is found, since every pair of real matrices B' and E' such that $B' + E' = B + E$ is equally likely to be the correct answer. We propose a weaker version, in which some information about B and E may be available. We are not aware of any known algorithm to solve neither version of this problem, so that in both cases there seems to be no other approach than exhaustive search to find a solution.

Assuming the hardness of this problem, we are developing a public-key cryptosystem in which the secret key is a matrix S, and the public key is given by $P = US + E$, where $|\det(U)| = 1$. It is publicly known that all the matrices have integer coefficients, the matrix S has a particular structure, and the entries of E are limited to some interval.

The advantage of such a cryptosystem lies on its simplicity, since it deals basically with integer matrix operations, which allows very simple and fast implementations, employing reasonably smaller keys. We highly encourage further research on the complexity of the problem presented in this work, which is part of an ongoing research, and we hope to bring further significant results in the near future.

Acknowledgements

We thank Professors Severino Collier Coutinho and Luziane Ferreira de Mendonça for helpful discussions and comments. We also thank CAPES and CNPq for the financial support.

References

[1] M. Ajtai and C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, Proceedings of the Annual ACM Symposium on the Theory of Computing, 29, 284–293, (1997).

[2] O. Goldreich, S. Goldwasser and S. Halevi, Public-key cryptosystems from lattice reduction problems. Crypto'97, Lecture Notes in Computer Science, vol. 1294, 112–131 (1997).

[3] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: a ring based public key cryptosystem. Proceedings of ANTS-III, vol. 1423 of LNCS, 267–288 (1998).

[4] P. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. Advances in cryptology - Crypto '99. Proceedings of the 19th Annual International Cryptology Conference, Lecture Notes in Computer Science, vol. 1666, 288–304 (1999).

[5] O. Regev, On lattices, learning with errors, random linear codes, and cryptography. Proc. 37th ACM Symp. on Theory of Computing (STOC), 84–93 (2005).

[6] M. Yoshino and N. Kunihiro, Improving GGH cryptosystem for large error vector. International Symposium on Information Theory and its Applications, IEEE, 416–420 (2012).

DOI: 10.5540/03.2015.003.02.0022