Characterizing Lattices for Cryptography

Tomás S. R. Silva*, Prof. Ricardo Dahab

Abstract

In this document, we aim to introduce a proposal of poster presentation at the XXVII Unicamp's Scientific Initiation Congress that will deal with the work that has been done on the characterization of lattices for cryptographic purposes. A lattice is a discrete additive subgroup of the n -dimensional real space that has a periodic structure. In other words, a lattice is a set constructed by all the integer combinations of linearly independent vectors defined on the n -dimensional real space. The usage of lattices for construct cryptographic models begins with the breakthrough work of Ajtai in 1996¹. Since then, cryptography based on lattices is being developed more and more, aiming to face the growing advance of computing power. In addition, some cryptographic models built on problems of non-polynomial difficulty on lattices are being considered as security solutions for building cryptoschemes that could face attacks from a sufficiently powerful quantum computer that may appear on the coming years. With this in perspective in view, it is interesting to characterize lattice structures and its parameters to create secure and efficient cryptoschemes.

Key words:

Cryptography, Lattices, Parameter Selection.

Introduction

Secure communication is a persistent subject in the history of humanity. In fact, it is notorious the constant development of measures and countermeasures related to the establishment of secure communication methods over the years.

With the advent of computers, there was a leap related to the capacity of transmission and processing information, that led to the creation of new techniques for private, secure and authentic communications.

The next great leap on the capacity of transmission and processing information may be the advent of a quantum computer sufficiently big, i.e., with enough quantum bits to run programs like Shor's Algorithm². Anticipating the advent of this quantum computer, the research community started the development of cryptographic techniques that can withstand an attack performed by such a machine; this effort is known as Post-quantum Cryptography. One of the most promising techniques of Post-quantum Cryptography is Lattice-based Cryptography, that is the main subject of this research project.

With this in view, this research project deals with the usage of a mathematical structure, called Lattices, applied to the construction of secure and efficient cryptographic schemes. Thus, it is interesting to start our discussion defining this structure and how we can use it to build cryptoschemes.

A lattice Λ is a discrete additive subgroup of the n -dimensional Euclidean space $\mathbb{R}^n$. A basis B for lattice Λ is a maximal set of linearly independent vectors of Λ having $k \leq n$ elements. The rank of the resulting lattice $\Lambda(B)$ is n . When $k=n$, then $\Lambda(B)$ is a full ranked lattice. The matrix representation for a lattice $\Lambda(B)$ is given by the set $\Lambda(B) = \{Bx : x \in \mathbb{Z}^n\}$.

Results and Discussion

In this project, we thought about lattices in Cryptography aiming to define what are good lattices to build secure and efficient cryptographic systems. With this objective in view, the efforts for characterizing good lattices for

Cryptography followed from the attempt to describe the mapping from a binary space of messages to a lattice, so that this mapping resembles closely a one-way-function.

The evaluation of the results consisted in comparing the prediction of good lattice constructions and selection of parameters like density and dimension, with well accepted heuristics that try to characterize those factors and with results that are being used on the constructions of lattice based cryptographic systems.

Conclusions

Our approach to try to characterize good lattices constructions and parameters for cryptographic purposes consisted of seeking good ways to define trapdoor functions that take points from a binary message space to points of a lattice in a direct way, i.e. the encryption function is applied directly over points from the message space. Commonly, the approach used to describe lattice parameters in terms of trapdoor construction uses the composition of two functions, the encoding function and the encryption function, where the encoding function takes points from a message space and maps them into lattice points; and then the encryption function takes points encoded on lattices and then maps them into other lattice points. The existence of eventual gaps between those two approaches is still being investigated.

Acknowledgement

This work was supported by São Paulo Research Foundation, Fapesp, under the grant number 18/08130-4.

I also want to recognize the support received from Prof. Ricardo Dahab, Jheyne N. Ortiz, Ramon Galate and Caio Teixeira.

¹ Ajtai, M. (1996). Generating Hard Instances of Lattice Problems (Extended Abstract). In Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96, pages 99–108, New York, NY, USA. ACM.

² Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput., 26(5):1484–1509, October 1997.