DOI: 10.20396/revpibic2720191576



# Choosing Parameters for Lattice-based Cryptosystems

**Caio Teixeira*, Ricardo Dahab**

**Abstract**
This study focuses on estimating good parameters for lattice-based cryptosystems. Through complexity analyses of known attacks to such systems, our objective was to understand current estimates in the literature and develop a calculator that determines the security of cryptosystems using the parameters given as input.

***Key words:***
*Post-quantum Cryptography, Lattices, Learning with Errors.*

## Introduction

This work aims to develop a better understanding of parameter selection in lattice-based cryptosystems. Lattice-based cryptography is a prominent field in post-quantum cryptography - cryptographic schemes that are resistant to attacks using quantum computers, as opposed to today's most widespread algorithms, which are easily broken using quantum computing. Through hard problems in these algebraic structures called lattices we are able to build computationally efficient cryptographic schemes, although careful parameter selection is necessary to make these schemes resistant to currently known attacks that exploit their structure.

## Results and Discussion

This investigation was carried out through the study of a particular subset of lattice-based cryptosystems, namely those using as underlying hard problem the Learning with Errors (LWE) problem. In this problem, we are given a point in $\mathbb{R}^n$ and a lattice basis **B**, and then asked to determine if this point was randomly generated using a uniform distribution in $\mathbb{R}^n$, or if it was generated using a lattice point with some perturbation on its coordinates. This problem's difficulty relies heavily on the choice of the basis - since a lattice has infinitely many bases, we may choose one that has long vectors and is far from orthogonal, as to make this decoding more difficult - and also on the choice of the perturbation distribution - if we take only points close to our lattice points, they form clusters in the space that are easily distinguishable from a uniform sample. These choices characterize the parameters we choose to instantiate our cryptosystems, and are fundamental to their security.

In this project, we studied the LWE problem and some of its variants (Poly-LWE and Ring-LWE), along with cryptosystems based on these problems and, most importantly, the currently known attacks to such cryptosystems. These attacks can be described within three categories: primal attacks, dual attacks, and combinatorial attacks. Our primary goal was to develop a parameter calculator, in which we would estimate the security of a cryptosystem using the parameters given as input to our algorithm and estimating the attack cost; however, during our research, we discovered that such calculator had already been recently constructed[1], and ours would either be comparatively simplistic and irrelevant, or take an unfeasible amount of time to develop.

We then shifted our focus to studying these attacks, with special emphasis on primal attacks, which try to solve the underlying decoding problem, and how the current implementation of the calculator estimated security against them. As a highlight, we demonstrate below the estimates of the analyzed calculator for 3 different cryptosystems with similar parameterization that were submitted to the NIST Post-Quantum Cryptography Standardization Process.

**Table 1.** Bit-security estimates for NIST candidates using the LWE Estimator[2].

| Scheme | Claimed Sec. | Est. Security |
|---|---|---|
| NewHope | 233 | 235 |
| Rlizard | 195 | 225 |
| LIMA-2p | 208 | 198 |

## Conclusions

While our initial goal had to be changed to a more abstract one, this study has helped lay a solid ground for further studies of the candidate, going from zero knowledge on lattice-based cryptography to being able to understand complex analyses and implement relevant algorithms. This work links now to a master's research on the same topic, with a much deeper scope thanks to the knowledge obtained through this project.

## Acknowledgement

This project was financed by CNPq, through the PIBIC grant 100023/2019-3.

---

[1] Albrecht M, Player R, Scott S. On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. 2015 10;9.

[2] Albrecht MR, Curtis BR, Deo A, Davidson A, Player R, Postlethwaite EW, et al. Estimate All the {LWE, NTRU} Schemes! In: Catalano D, De Prisco R, editors. Security and Cryptography for Networks. Cham: Springer International Publishing; 2018. p. 351–367.