Quantum Secure Encryption Hardware Implementation of Ring Learning With Errors

Anthony Fortner, Lahiru Perera, Vasanth Sadhasivan

June 14, 2019

Contents

1 Introduction 2

1.1 Project Background 2

1.2 Potential Beneficiaries 2

2 Research & Planning 2

2.1 LWE Basics 2

2.1.1 Private Key Generation 2

2.1.2 Public Key Generation 2

2.2 Why Ring LWE 3

3 Prototype design 3

3.1 Functions & Features 3

3.2 Challenges & Revisions 3

3.3 System Diagram 3

3.4 Software Flow Chart 3

4 Conclusions 3

4.1 Current State 3

4.2 Next Steps 3

5 LaTeXref 3

1 Introduction

1.1 Project Background

As the world become more dependent of technology the need to secure our data become a growing concern. Though there are numerous security algorithm that we use today, none are expected to be computationally robust against the processing power of quantum computers. Learning with errors (LWE) is different in the since that it is based on lattice cryptography, a method though to be more resistant to an attack due to its higher complexity.

1.2 Potential Beneficiaries

With the growing need to secure data the possible applications for LWE are countless. The future of computing is widely thought to become dominated my quantum computers and LWE has the potential to become our primary means to secure data. This would allow alleviate one of the major concerns of quantum computers and assist in their adoption.

2 Research & Planning

2.1 LWE Basics

2.1.1 Private Key Generation

To generate the private key Alice simply needs to come up with a vector that is in the vector space of n integers modulo q or Z_q^n

$$s \in Z_q^n$$

The vector elements are chosen uniformly at random $q \geq 2$, is a prime number between n^2 and $2n^2$

2.1.2 Public Key Generation

Initially Alice choose m vectors from Z_q^n uniformly and independently, let this set of vectors be set A

$$A = a_1, a_2 \ldots a_m \in Z_q^n$$

Then she choose a random set of m errors

$$E = e_1, e_2 \ldots e_m \in Z_q^n$$

Error values are selected according to the distribution χ

$$m = (1 + y)(n + 1)log(q)$$

for an arbitrary y

2.2 Why Ring LWE

3 Prototype design

3.1 Functions & Features

3.2 Challenges & Revisions

3.3 System Diagram

3.4 Software Flow Chart

4 Conclusions

4.1 Current State

4.2 Next Steps

5 LaTeXref

$$1+2=3$$

$$1=3-2$$

$$\begin{multline*}1+2=3\\1=3-2\end{multline*}$$

$$\begin{aligned}f(x)&=x^2\\g(x)&=\frac{1}{x}\\F(x)&=\int_b^a\frac{1}{3}x^3\end{aligned}$$

$\begin{matrix}1&0\\0&1\end{matrix}$
$\begin{bmatrix}1&0\\0&1\end{bmatrix}$

$$\left(\frac{1}{\sqrt{x}}\right)$$

Random citation [1] embedded in text.

References

[1] J. Doe, *The Book without Title.* Dummy Publisher, 2100.