Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Diyala

College of Science

Computer Science Department

"NTRU Modification Against LLL Attack"

A Thesis Submitted to

the University of Diyala / College of Science / Department of Computer Science, In partial Fulfillment of the Requirements for the Degree of Master in Computer Science

By

Omar Sapti Guma'a

Supervised By

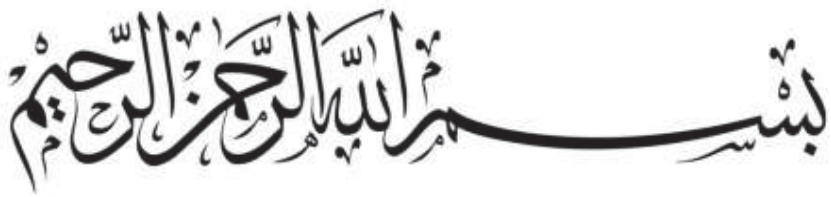
Prof. Dr.

Ziyad Tariq Mustafa Al-Ta'i

Prof. Dr.

Qasim Mohammed Hussein Al-Shamry

December / 2020 A.D. **Diyala** **Rabi Al-Akhar / 1441 A.H**



"وَقُل رَّبِّ أَدْخِلْنِي مُدْخَلَ صِدْقٍ وَأَخْرِجْنِي مُخْرَجَ صِدْقٍ وَاجْعَل لِّي مِن لَّدُنكَ سلُطْاَنانًصَيراً"

الإسراء (80)

DEDICATED TO

To the martyrs of Iraq ...

To my father …

To my mother …

To my wife …

To my brothers …

To my sisters …

Omar

ACKNOWLEDGMENTS

*Above all else, I want to express my great thanks to my God (Allah) for his uncountable gifts and for helping me to present this work. Furthermore, I would like to express my deepest gratitude to my supervisors (**Prof. Qasim Mohammed Hussein**) and (**Prof. Ziyad Tariq Mustafa Al-Ta'i**) for their powerful guidance, motivation, valuable suggestions, support and attention throughout this research.*

Special thanks to the Faculty of Science at the University of Diyala / Postgraduate to give me the opportunity to join the Master's in Computer Science.

I would like to say "thank you" to my faithful friends for supporting and giving me advice

Finally, I am most grateful to my parents who provided me with endless love and support morally and materistically during all my years of studying. As I would like to mention that without my wife insistence, I might not be pursuing my study. Words are simply not enough to express my gratitude to My father who always believed in me, and recovered me when I find myself in the gloom. Many thanks to him.

Thanks for All

Omar

ABSTRACT

The existence of quantum computers makes the execution of algorithms that requiring high computational very possible, which makes many current cryptosystems broken with the execute of these algorithms. Peter Shor developed a quantum algorithm called Shor's algorithm in 1994, and considered this an important discovery in this area. Therefore, breaking many existing cryptosystems such as RSA and ECC is possible with a quantum computer.

Consequently, there is needs to new cryptographic schemes that be resistant to quantum. These new cryptographic constructions should be efficient and secure enough to be used in practice and standardized for a large number of years, replacing the current ones if needed.

Lattice-based public-key cryptosystem (LB-PKC) consider as one presented solutions to overcome this challenge. NTRU is one of a LB-PKCs that based on truncated polynomial ring $Z[x]/(x^N - 1)$. But, NTRU system has been attacked by using the LLL algorithm under certain conditions, which can find the secret key when the length of the public key is less than 127.

The aim of the thesis is to make modifications on the original NTRU cryptosystem to ensure the failing the LLL attack on it. This thesis can be divided in two parts: first, presents a method to add new parameter to the parameters of the original NTRU, the values of this parameter depends on the linear feedback shift registers (LFSR). Secondly, presents a modification on the original NTRU by doing swapping operation between the values of public key. in addition to generate a long keys sequences dynamically to use in encryption. Experimental results on the proposed methods have demonstrated the ability of these methods to resist against the LLL algorithm attacking, even if the public key length does not exceed 11, also these proposals could generate approximately (Np-1) versions of key sequence with length N.

Table of Contents

Title ***Page No.***

Acknowledgement..... i

Abstract.....ii

Table of Contents iii

List of Figures……..……...….vi

List of Tables ……..……..…….....vi

List of Algorithms ……..……...vii

List of Abbreviations viii

Chapter One: Introduction

1.1 Overview….……...…….……..……..1

1.2 Related Work ……...…….……...…..……2

1.3 Problem Statement ……..……..……4

1.4 Aim of Thesis…….……..……...…5

1.5 Thesis Outline ……..……..……...…….....5

Chapter Two: Theoretical Background

2.1 Introduction …….……..……..……7

2.2 Lattice-based Cryptography (LBC) ……...7

2.3 Mathematical and Computational background ……..…..……...8

2.3.1 Linear Feedback Shift Register (LFSR)…….……..…....8

2.3.2 Truncated polynomial ring……...10

2.3.3 Finding the greatest common divisor ……...…...13

2.3.4 Extended Euclidean algorithm……...……...…...13

2.3.5 Finding the polynomial multiplicative inverse……....15
2.3.6 Convolution multiplication of two polynomials……..……....16
2.3.7 Inverse of truncated polynomial rings……..18
2.3.8 Lattices…….……....21
2.4 NTRU Public Key Cryptosystem……..20
2.4.1 NTRU public parameters…….22
2.4.2 Key generation…….23
2.4.3 Encryption Algorithm……..……...24
2.4.4 Decryption Algorithm …….……....25
2.5 NTRU Parameter Selection…….……..26
2.5.1 Small polynomial…….……27
2.5.2 Choice NTRU parameter……..27
2.6 Low hamming weight polynomial……28
2.7 The advantages of NTRU……..30
2.8 Encryption and Decryption Speeds……..…….31
2.9 Attack on NTRU cryptosystem…….32
2.10 Lattice-based attack……....32
2.10.1 The LLL algorithm……...……...32
2.10.2 Lattice-based attack on the public key…….34
2.10.3 Lattice-based attack on the cipher text……...……..35

Chapter Three: Design of The Proposed System

3.1 Introduction…….……..37
3.2 Objectives……...…….……..38
3.3 The Proposal One…….……39
3.3.1 Key Generation…….……...39
3.3.2 Encryption…….……...41
3.4 The Proposal Two…….…….……...42
3.4.1 Key Generation…….……...44

3.4.2 Encryption……..……...45

Chapter Four: Results and Evaluation

4.1 Introduction…….…….....47

4.2 Initialization…….…….....47

4.3 LLL Algorithm Attack…….……..…...48

4.3.1 LLL Algorithm Attack on the public Key…….……...48

4.3.1.1 The attack on the original NTRU……..…..……....49

4.3.1.2 The attack on the proposal one……...52

4.3.1.2 The attack on the proposal two……...55

4.3.2 LLL Algorithm Attack on the Ciphertext……....57

4.3.2.1 The attack on the original NTRU……58

4.3.2.2 The attack on the proposal one……...60

4.3.2.3 The attack on the proposal two……...62

4.4 Dynamically Generation of Keys Sequences……....63

4.5 Performance Analysis……....65

4.5.1 Encryption Time and Decryption Time Analysis……....66

Chapter Five: Conclusions and Suggestions for Future Works

5.1 Introduction…….…….....68

5.2 Conclusions ……..……...……...…68

5.2 Suggestions for Future Works ……..……...….69

Publications…….…..…..70

References……..…….……...…70

List of Figures

Figure ***Page No.***

2.1 Block diagram of LFSR ……..….....8

2.2 Block diagram of LFSR example with 5-stage …….....9

2.3 Encryption and Decryption Speeds of NTRU ……..….....31

3.1 Flowchart of dynamic key generation ……...…….43

4.1 Performance timings of NTRU and the proposed algorithms ……..… .67

List of Tables

Table ***Page No.***

1.1 A review of some proposed modifications for NTRU …...……...…2

2.1 The contents of LFSR after shifting process ……...……...…….20

2.2 NTRU Parameters and Keys……...…….22

2.3 The parameters sets …….28

2.4 Encryption and Decryption of NTRU ……...……..... 31

4.1 The lattice basis L of h (NTRU cryptosystem)……..…… 49

4.2 The LLL algorithm results (NTRU cryptosystem) ……..…….……. 50

4.3 The lattice basis L for h (proposal one)…….……..... 53

4.4 The LLL algorithm results (proposal one)…….…….…….. 54

4.5 The lattice basis of L for h (proposal two)……..…... 55

4.6 The LLL algorithm results (proposal two)……..…….... 56

4.7 The lattice basis of L for the original NTRU ……...……..…….... 58

4.8 The LLL algorithm outputs for the original NTRU ……...…….... 59

4.9 The lattice basis of L (proposal one)……...……..... 60

4.10 The LLL algorithm outputs ……...……...…….... 61

4.11 The lattice basis of L (proposal two)……..……..... 62
4.12 The LLL algorithm outputs……...……... 63
4.13 Performance analysis for basic NTRU and the proposals…….... 65
4.14 Encryption Time and Decryption Time Analysis for original NTRU and the proposed algorithms per second ……..…….…... 66

List of Algorithms

Table ***Page No.***

2.1 GCG Algorithm……..……...……..13
2.2 The multiplicative inverse of a mod b ($a^{-1}{}_b$) ……..……...……..14
2.3 The extended Euclidean algorithm to find polynomial inverse…..…….16
2.4 Convolution multiplication of two polynomials with degree(N-1)……..17
2.5 Compute the inverse of polynomial in (Z/2Z)(X)/(X^N-1)……..... 18
2.6 Compute the inverse of polynomial in (z/3z) (x)/ (x^N-1)..……. 19
2.7 Compute the inverse of polynomial in (Z/pZ) (X) / (X^N-1)…….……20
2.8 Gram-Schmidt process …….…….....……34
2.9 LLL Algorithm…… …….…….....……34
3.1 Public key Generation (proposal one)……..……...…..40
3.2 Encryption process (proposal one)……..……..... 41
3.3 Public key Generation (proposal two)……..……..... 44
3.4 Encryption process (proposal two)……..……..... 45

List of Abbreviations

Abbreviation	***Meaning***
AES	Advanced Encryption Standard
CP	Cipher text Policy
CVP	Closest Vector Problem
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptosystem
FFT	Fast Fourier Transform
gcd	Greater Common Devisor
KP-ABE	Key Policy - Attribute-Based Encryption
LB-PKC	Lattice-Based Public Key Cryptography
LFSR	Linear Feedback Shift Register
LLL	Lenstra - Lenstra –Lovasz
LWE	Learning with errors
NTRU	Nth Degree Truncated Polynomial Ring Unit
RFID	Radio-frequency identification
RSA	Rivest, Shamir, and Adelman
SVP	Shortest Vector Problem

Chapter One

Introduction

Chapter One

Introduction

1.1 Overview

The great development in the field of the Internet and technology, in the modern world today and the increase in the number of devices that send and receive data, in addition to the fact that there are many of these devices that perform several functions without human intervention, it led to a large data transfer process. Certainly, these data contains sensitive data and personal information, so there is an urgent need to protect this data from attacks. There are many ways to protect information. This can be overcome by exploiting public-key cryptography (PKC) which has features such as confidentiality, data integrity, authentication, and non-repudiation. With these features, PKC can provide security for communication networks, especially for ensuring the privacy and confidentiality of important information. There are many PKC used at the present time. RSA and elliptic curve cryptosystem (ECC) are two currently popular public key systems in modern cryptography. These cryptosystems are based on mathematical problems named hard problems. These cryptosystems are considered to be somewhat safe nowadays due to the lack of effective algorithms able to resolve this type of cryptosystems. This situation does not last long with the progress in the development that we are witnessing and the emergence of quantum computing technology, because the computers that depend on this concept differ greatly from computers that depend on electronics. Quantum computers are greatly able to solve many hard mathematical problems[1][2]. Hence, more effective methods are needed to meet this

challenge. Lattice-based constructions are currently important candidates for post-quantum cryptography. Lattice-based public-key cryptosystem (LB-PKC) has many advantages compared with 'traditional' cryptography. NTRU is one of a LB-PKC that based on truncated polynomial ring $Z[x]/(x^N - 1)$, it has good features, which it makes to be an effective alternative to cryptosystems such as RSA and ECC [3].

This system has weak points, including the ability to attack it under certain condition using Lenstra–Lenstra–Lovász lattice basis reduction algorithm [4] discover the private keys or other private key called an alternative key that can be used to decrypt the cipher text, as well as it can be used to discover the plaintext by cipher text and public parameters[5]. To avoid the LLL algorithm attack, this thesis presents two proposals that suggest modifications on NTRU cryptosystem.

1.2 Related Work

There are many proposed cryptosystems that suggest modifications on NTRU to improve it. Table (1.2) illustrates that:

Table (1.1): A review of some proposed modifications for NTRU

Publishing, Year	**Description**
[6,2010]	• Presents cryptosystem that depends on NTRU structure called OTRU. • OTRU has been designed based on the NTRU core and exhibits high levels of parallelism with full operand length.

	• OTRU is the first step in the design of the public key cryptosystems with a non-associative algebra.
[7,2013]	• Proposed a new cryptosystem that based on NTRU structure called ETRU, and the ring of this cryptosystem is Z[w] and the coefficients are integer numbers. • The LLL algorithm can be used to find short vector in this work because there is a relatively short vector.
[8,2015]	• It is based on ideal lattice which is special structured lattices. This scheme was motivated by ETRU[7], which is used to make this scheme provably secure.
[9,2015]	• Introduced CQTRU cryptosystem based on commutative quaternions algebra. • The resistance of CQTRU to lattice attack is at least four times better than that of NTRU at the same dimension and also in CQTRU even with the use of LLL reduce algorithm an attacker cannot always guarantee to find the private key.
[10,2016]	• The role played by Z in NTRU replaced by the ring Q[α] of polynomial in one variable α over the Rational Field. The same value of N, CTRU is faster than NTRU, but not always. • This proposed scheme may be secure against the LLL algorithm attack but not proved.
[11,2018]	• A general framework for NTRU is considered, and a new PKC called D-NTRU is proposed. • It is shown that the D-NTRU cryptosystem reduces the

	ciphertext expansion of the NTRU algorithm, and the encryption and decryption algorithms of D-NTRU perform even asymptotically faster than the NTRU algorithm only at the cost of slightly enlarged secret and public keys. • The IND-CPA security of D-NTRU was proven under the NTRU one-wayness hardness assumption.
[12,2019]	• Proposed GTRU cryptosystem that based on group based of NTRU algorithm. • The parameters (f and g) must be choosing as n x n matrices instead of small polynomials. • NTRU key size is much smaller than GTRU key size that constructed by Gn. • This work is slower than NTRU, but it is more secure against lattice-based attacks.
[13,2020]	• In this work, RCPKC is proposed, a secure and effective congruential, modulo q, public-key cryptosystem using big numbers. • It uses the same encryption/decryption mechanism as NTRU does but works with numbers.

1.3 Problem Statement

Many public key cryptosystems, such as RSA, ECC and Diffie-Hellman protocol, are based on hardness problem (factorization or the discrete logarithm problem). But, these cryptosystems can breaking by use efficient algorithm for quantum computers [14][15]. Therefore, we

need other ways to overcome this challenge. Lattice-based cryptography is NP-hard problem, post-quantum and it is considered one of the solutions presented because there is still no algorithm that can break these problems. NTRU is a lattice-based public key cryptosystem, but this system can be attacked by LLL algorithm under certain conditions. Therefore, the basic research problem is to find suitable solutions to prevent the LLL algorithm from breaking this system.

1.4 Aim of Thesis

The aim of the thesis is to make modifications on encryption algorithm of the NTRU public key cryptosystem, to ensure that the LLL algorithm cannot able to break this system.

Another aim is to find a method to generate long sequences of keys dynamically, without need addition private keys to ensure that the key is not repeated when encrypted data size is large, also and in order to increase encryption security strength.

1.5 Thesis Outline

This thesis is structured around Five chapters, including chapter one, it contains the following chapters:

- **Chapter Two**: **(Theoretical Background)**

This chapter explains in detail background of IoT, NTRU public key cryptosystem, as well as LLL algorithm.

- **Chapter Three** :**(Design of The Proposed System)**

In this chapter, the proposed algorithm design and the implementation steps are given.

- **Chapter Four: (Results and Evaluation)**

This chapter is dedicated to showing the outputs and tests of the proposed system.

- **Chapter Five: (Conclusions and Recommendations for Future Works)** some concluding remarks which are derived from the outputs of the conducted tests are given in this chapter; also some suggestions for future work are presented.