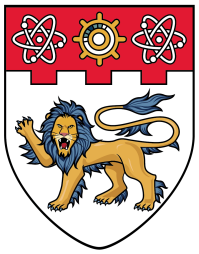

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

URECA: Security Evaluation of NTRU Public Key Cryptosystem

Charissa Irene Utomo
Matriculation number: U2040071K
Email: cutomo001@e.ntu.edu.sg

Supervisor: Assoc. Prof. Wu HongJun

Nanyang Technological University
School of Physical and Mathematical Sciences

2021/2022

Abstract

Keywords:

Nomenclature

$MITM$	Meet-in-the-middle attack
$NTRU$	N-th degree Truncated polynomial Ring Units
$s.t.$	Such That
$SPMS$	School of Physical and Mathematical Sciences
$URECA$	Undergraduate Research Experience on CAmpus

Table of Contents

Introduction

1.1 About

We would be investigating the security of N-th degree Truncated polynomial Ring Units which is also known as NTRU for short. NTRU is an open-sourced public-key cryptosystem which allows two remote parties to communicate in a secure way without sharing a secret key. NTRU is required to be secure against the future quantum computer to minimise information intersections and attacks where . In this project, we will analyze the security of NTRU and delve on the characteristics of lattice-based cryptosystem. Furthermore, we will study and improve the current existing attacks on NTRU and attempt to develop new attacks against NTRU. The program is available at https://github.com/charutomo/Security-Evaluation-of-NTRU-Public-Key-Cryptosystem.
Keywords: NTRU, open-sourced, public-key cryptosystem, quantum computer

1.2 Background Information

NTRU was introduced by Hoffstein J., Pipher J. and Silverman J.H. in the year 1996 and was patented the following year by their company, NTRU Cryptosystems Inc, alongside with Lieman D..

1.3 Deliverables

The expected deliverables for the project is an overall analysis report of the existing attacks calibrating its advantages and suggestive improvement and an attempt on python implementation of a new attack against NTRU.

Definitions

2.1 Key Definitions

2.2 Principles and Theorems

2.2.1 Kerckhoffs's principle

In modern cryptography, reduced focus on security on obscurity unlike the past is due to Kerckhoff's principle. Kerckhoff's principle states that security should not be breached even if majority of the detail about a general cryptosystem such as encryption and decryption except secret key is publicly known.

NTRU

3.1 Behind the math

In this section, we evaluate the Mathematical aspect of NTRU particularly lattice-based cryptography and its characteristics. This is crucial in understanding the crux of how NTRU works and what can be the potential improvements be made.

3.1.1 Lattice-based Cryptography

3.1.2 Characteristics of NTRU

3.2 Existing Attacks

Now, we would study the current existing attacks such as brute force attack and meet in the middle attack. By understanding each attack, it can inspire other forms of attack which can be more targeted to the system.

3.2.1 Brute-force attack

Brute-force is one of the most common attacks for cryptosystems. However, it usually can take a longer period to be able to fully attack the system. Due to large runtime complexity, it may take many permutation to be carried out before determining the actual plaintext.

3.2.2 Meet-in-the- middle attack

Meet-in-the-middle attack, also known as MITM, is a form of cryptanalysis to observe the patterns from both ends until the middle part of the ciphertext. This attack can break the system in faster and more elegant manner as compared to brute-force as it reduces the number of permutations to discover the secret keys of NTRU.

3.2.3 Multiple transmission attacks

3.2.4 Lattice-based attacks

3.3 Proposed new attack

3.3.1 Targeted Attack

Keywords:

Conclusion

4.1 Ending Statement

In a nutshell, we have gain knowledge on the characteristics of lattice-based cryptography specifically NTRU. Moreover, we examined its attacks and flaws to understand the security of NTRU. Conversely, I strongly believe that overall NTRU remains as secure and can be used universally. This concludes our project (readily available at https://github.com/charutomo/Security-Evaluation-of-NTRU-Public-Key-Cryptosystem) and feel free to contact us via email for further enquires. Thank you for your upmost support.

Lists of Figures