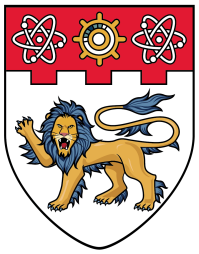

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

# URECA: Security Evaluation of NTRU Public Key Cryptosystem

**Assoc. Prof Wu Hongjun and Charissa Irene Utomo**
Matriculation number: U2040071K
Email: cutomo001@e.ntu.edu.sg

**Nanyang Technological University**
**School of Physical and Mathematical Sciences**

**2021**

# Abstract

**Keywords:**

# Acknowledgement

# Table of Contents

**Abstract** i

**Acknowledgement** ii

**Nomenclature** iv

**1 Introduction** 1

**2 Conclusion** 2

**References** 3

**Lists of Figures** 3

# Nomenclature

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

# Introduction

NTRU is a public key cryptosystem which allows two remote parties to communicate in a secure way without sharing a secret key. NTRU is expected to be secure against the future quantum computer. In this project, we will analyze the security of NTRU. We will try to improve the existing attacks on NTRU, or to develop new attacks against NTRU. Math (more specifically, lattice), programming and algorithms are needed in this project. The program is available at https://github.com/charutomo/Security-Evaluation-of-NTRU-Public-Key-Cryptosystem.
**Keywords:** optimally, isolate, isolation wards

# Conclusion

---

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