University of Bergen
Department of Informatics

Title of your master thesis

Author: Eirik Djupvik Skjerve

Supervisors: Igor Aleksandrovich Semaev & Martin Feussner

UNIVERSITETET I BERGEN

Det matematisk-naturvitenskapelige fakultet

November, 2024

Abstract

Quantum computers threaten todays encryption schemes. NIST asked for new standards, among them is HAWK. This thesis will investigate if HAWK is secure against a variation of an attack that broke NTRU-Sign.

Acknowledgements

Thank you to some people

Eirik D. Skjerve

Saturday 2nd November, 2024

Contents

Chapter 1

Introduction

1.1 Context and motivation

Digital signatures are an important part of secure communication today. The most used cryptographic scheme used for digital signatures today is DSA (Digital Signature Algorithm) or RSA (Rivest, Shamir, and Adleman) signatures (source). However, in 1994, Peter Shor developed Shor's algorithm, which, given a large enough quantum computer, is able to solve the hard problems DSA and RSA is based upon, namely the Discrete Logarithm Problem and Prime Factorization(source). Whether big enough quantum computers will emerge any time soon is debatable. However, measures against this potential looming threat has already begun. In 2016, NIST (National Institute of Standards and Technology) announced a standardization process for new standard schemes for KEMs (Key Encapsulation Methods) and digital signatures that have strong security against quantum computers (source). Many of the submissions to this process, including KRYSTALS-Dilithium which is to be standardized, are based on lattice problems that are believed to be hard to solve for both classical and quantum computers (source).

Cryptographic schemes based on lattice problems are not an enirely new phenomenon, however. NTRU-Sign, published in 2003(source), is a digital signature scheme based on the hardness of the Closest Vector Problem (source). The original scheme was broken due to Phong. Q. Nguyen & Oded Regev in 2006 [3], who showed that by observing enough signatures generated with one secret key, one can retrieve the secret key. A newer digital signature scheme, Hawk (source), submitted to NIST's standardization process, is a scheme similar that of NTRU and GGH. The goal of this thesis is to try and adapt the Hidden Parallelepiped Problem attack to Hawk [2]. Hawk spec here [1]

1.2 Objectives

The objective for this thesis is comprised of two main parts:

- **Implementation of Hawk in Rust**. As the first part of the thesis I implement the Hawk digital signature scheme in the Rust programming language. Implementing a scheme on ones own is a good way to actually learn how it works. I chose to implement it in Rust for the sake of learning the programming language. Moreover, having ones own version makes it easier to experiment, adjust and modify to ones need. It would also be just a big a challenge to understand and work with complicated source code someone else has written.

  Cryptanalysis and experimentation. As part two of the thesis I want to do cryptanalysis of Hawk. By using the "Learning a parallelepiped" attack [3] and adjusting it to try and break Hawk. This requires both mathematical, theorethical work, as well as practical experimentation and implementation, which will also be done in Rust.

1.3 Thesis outline

Chapter 2

Background

2.1 Asymmetric cryptography

2.2 Linear algebra & lattices

2.3 Lattice problems

Chapter 3

Adapting HPP to Hawk

In this chapter we investigate the steps needed to possibly apply the Hidden Parallelepiped Problem to the Hawk digital signature scheme.

3.1 Covariance matrix of secret matrix

Nothing yet I'm afraid

Bibliography

[1] Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. Hawk. Technical report, NXP Semiconductors, Centrum Wiskunde & Informatica, Mathematical Institute at Leiden University, NCC Group, PQShield, Institut de Mathématiques de Bordeaux, September 2024.
URL: `https://hawk-sign.info/`.

[2] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. Cryptology ePrint Archive, Paper 2022/1155, 2022.
URL: `https://eprint.iacr.org/2022/1155`.

[3] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures, 2009.

Appendix A

Generated code

Listing A.1: Source code of something

```
println!("Goodbye World");
```