Initial Plan: Evaluating the Robustness of a Lattice-Based Cryptosystem

Author Andrea Pesigan [C1606020]
Final-Year Computer Science Undergraduate at Cardiff University

Project Supervisor Eirini Anthi
IoT and ICS Security Research Associate at Cardiff University

Project Moderator Dr. Frank Langbein
Senior Lecturer in the School of Computer Science and Informatics at Cardiff University

CM3203 One Semester Individual Project
40 credits

3 February 2020

Contents

Chapter 1

Project Description

The overall aim of this project is to evaluate the security of an existing lattice-based cryptosystem and suggest ways to improve upon that implementation. The programming portion of the project will involve writing code to attack the application and modifying it to improve on it. There will also be a written exploration of how the application can be scaled up to be safe against sufficiently-powerful quantum computers.

Preliminary research is needed to compare different implementations of lattice-based cryptography schemes. As code implementations have been publicly shared for the schemes NTRUEncrypt and GGH, it will be these two schemes whose implementations will be compared and selected, based on speed, security, and simplicity of the implementation given the short time frame given for the project. The selection will be justified based on these criteria. Upon analysing and understanding the inner workings of the implementation and why it provides security, the application will be tested against a set of attacks in an attempt to invalidate the security. Though attacks will be performed using a classical computer, an aim of this project is to investigate whether the implementation will be sufficient to provide security against quantum computers, directly based on the results of the attack attempts and through mathematical analysis. The produced work should provide a sufficient analysis of the security of this implemented lattice-based cryptosystem and the extent to which it is quantum-resistant.

Chapter 2

Project Background

Quantum computing is expected to become mainstream in the not-too-distant future [6]. If fault-tolerant, quantum computers can process information much quicker than classical (silicon-processor) computers. Companies such as IBM and Google have made headlines for exhibiting quantum computers of about 50 quantum bits (qubits) [8] [3]. Though these computers are not fault-tolerant, it is considerable progress from the first experimental demonstration of a quantum algorithm using a working 2-qubit quantum computer in 1998 [2] given the extreme conditions a qubit needs to maintain its state for an amount of time long enough to be useful.

A concern of the development of quantum computers is that current public-key cryptographic methods such as RSA can be broken by these devices with the use of algorithms such as Shor's algorithm (which can factor integers in polynomial time), meaning that data encrypted today using these methods is in danger of being decrypted later by these powerful machines [7]. The United States standards agency NIST decided in 2016 that it is time to look at standardising post-quantum cryptography, and called for proposals of quantum-resistant cryptosystems. Among the submitted proposed replacements for current public-key methods based on mathematical problems such as factorisation, public-key methods based on lattices have been the leading choice based on number of submissions [4]. According to IBM, lattice-based cryptography is said to be safe against both classical computers and fault-tolerant quantum computers boasting computing power even in the millions of qubits[5].

Lattices are, simply put, a set of points in infinite space of a given number of dimensions, where placement of the points is defined by a set of vectors known as the basis vector. Given any point in the lattice and the basis vector, one can find neighbouring points in the lattice. The security of public-key cryptosystems relies on the difficulty of certain mathematical problems; for example, the security of RSA depends on the difficulty of factoring large numbers made up of two large prime numbers. The difficult mathematical problems involving lattices include the shortest vector problem (SVP) and the closest vector problem (CVP). Lattice-based cryptosystems are public-key cryptography methods based around problems such as these. While solving these problems is not difficult to a great degree with few dimensions, the problems get increasingly difficult with more dimensions, as for classical computers "[t]he time complexity of known algorithms that find the exact solution are at least exponential in the dimension of the lattice"[1]. This project aims to assess the security of an implementation of one such cryptosystem.

Chapter 3

Ethics

After discussing the project with the project supervisor regarding ethical considerations, it has been established that the project will not involve the collection of data from humans and therefore will not require ethical approval from the Cardiff University School of Computer Science. The extent of data collected for the project will be independent research on lattice-based cryptography using information available to the public and/or to researchers of academia or industry.

Chapter 4

Aims and Objectives

Overall aim: evaluate the security of and suggest a more robust version of an implementation of a lattice-based cryptosystem.

4.1 Phase 1: Choosing an implementation (2 weeks)

- Background research
  - Learn how lattices work and how it fits in the context of cryptography
  - Look at what experts say about lattice-based cryptography
  - Look at what has been created so far and what the results of that work are
- Compare code implementations of NTRUEncrypt and GGH publicly shared
  - Consider speed, security, and simplicity
- Choose one implementation and justify selection
  - Explain to supervisor and/or moderator how the cryptosystem works to confirm that (1) it is understood and (2) it is suitable for the project

4.2 Phase 2: Attacking the implementation (3 weeks)

- Decrypt ciphertext, when (1) given ciphertext and partial plaintext and (2) when given just ciphertext
- Find the private key from the public key
- Propose and evaluate more attacks after attaining a deeper understanding of the cryptosystem

4.3 Phase 3: Improving on the implementation (3 weeks)

- Modify the application to strengthen it against the above attacks
- Understand and explain the mathematics behind the attacks and why successful/unsuccessful
- If attacks from previous phase are unsuccessful (indicating robustness), explain what can be done to attack the cryptosystem more intensely and/or explain what parameters (e.g. key sizes) are needed to ensure security, ideally against a sufficiently-powerful quantum computer but at least against a classical computer
- Start a draft of the following sections of the final report: overview, introduction, background, approach, implementation, glossary, references

4.4 Phase 4: Formal exploration of quantum-resistance (3 weeks)

- Understand and explain mathematics behind lattices, in the context of quantum computers
- Understand and explain what needs to change about the coded cryptosystem in order for it to be resistant to fault-tolerant quantum computers of 2 qubits, 100 qubits and thousands of qubits

- Consult Dr. Frank Langbein to confirm understanding
- Start a draft of the following sections of the final report, based on findings made during the course of the project: results and evaluation, conclusions

4.5 Phase 5: Final report writing (6 weeks, with 3 weeks dedicated solely to final report)

- Tidy code for comprehensibility
- Put together report from notes and from the report draft gradually added to over the previous four phases
- Step away from the report for two to three days while acquiring feedback from others, and afterwards return to the report with a clear mind to proofread and submit

Meetings with the project supervisor will take place weekly to ensure that the student understands the technical contents of the project, recognises and plans around the objectives to complete, and is adhering to a feasible time plan. Review meetings will take place at weeks 5 and 9 to discuss overall progress and adjust the time plan.

Meetings with the project moderator will be scheduled as necessary with regards to the quantum computing aspect of the project.

Chapter 5

Time Plan

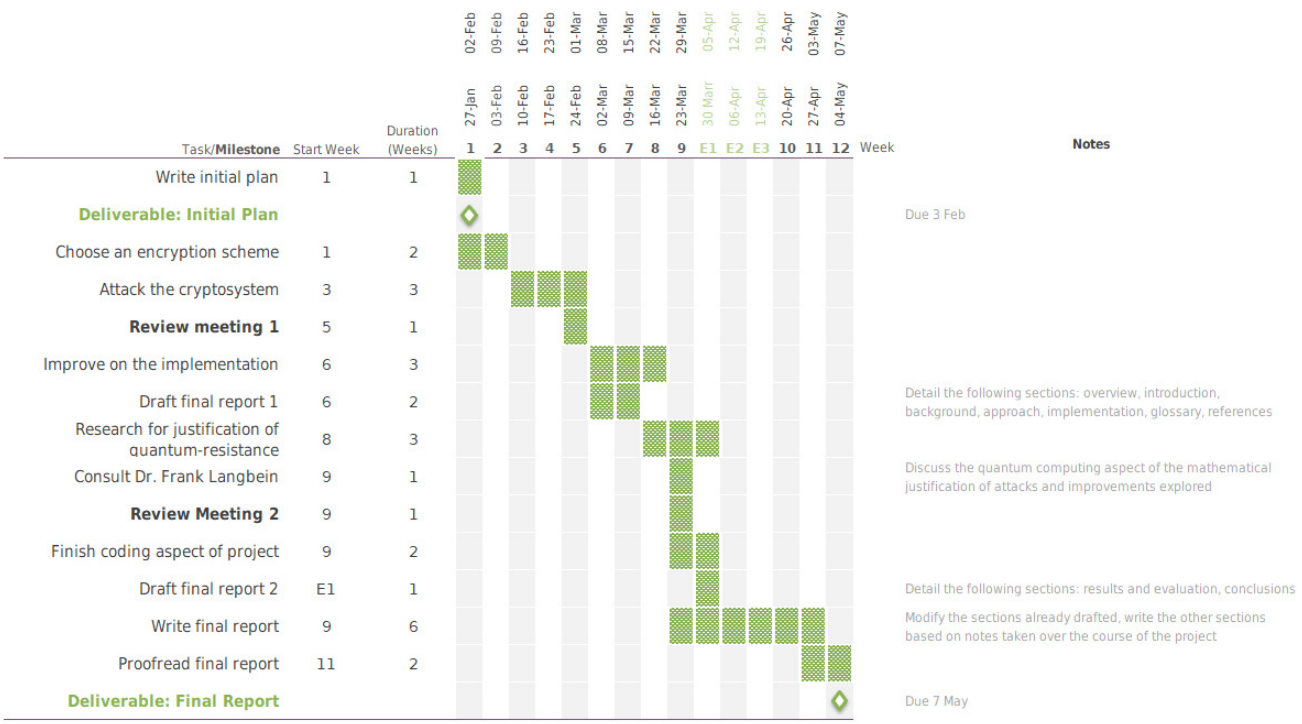

Figure 5.1: Gantt Chart of Time Plan

Chapter 6

Planning for Multiple Reports

An interim report will not be produced for this project. The final report will describe all achievements and reflections of the project, with the student keeping detailed notes of research performed, methods used, and results obtained, and gradually adding to the final report throughout the process.

References

[1] Anja Becker, Antoine Joux, Nicolas Gama. "Solving shortest and closest vector problems: The decomposition approach." Cryptology ePrint Archive, Report 2013/685, 2013. https://eprint.iacr.org/2013/685.

[2] Chuang, Isaac L., Gershenfeld, Neil, and Kubinec, Mark. "Experimental Implementation of Fast Quantum Searching." 1998.

[3] Edwin Pednault, Jay Gambetta, John Gunnels Dmitri Maslov. "On "Quantum Supremacy"." 2019.
https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[4] Gorjan Alagic, Daniel Apon David Cooper Quynh Dang Yi-Kai Liu Carl Miller Dustin Moody Rene Peralta Ray Perlner Angela Robinson Daniel Smith-Tone, Jacob Alperin-Sheriff. "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process." *National Institute of Standards and Technology Interagency or Internal Reports* .
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf

[5] IBM. "5 in 5: Lattice Cryptography." 2019.
https://www.research.ibm.com/5-in-5/lattice-cryptography/

[6] ———. "5 in 5: Quantum Computing." 2019.
https://www.research.ibm.com/5-in-5/quantum-computing/

[7] Lily Chen, Yi-Kai Liu Dustin Moody Rene Peralta Ray Perlner Daniel Smith-Tone, Stephen Jordan. "Report on Post-Quantum Cryptography." *National Institute of Standards and Technology Interagency or Internal*

Reports .
https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[8] Sample, Ian. "Google claims it has achieved 'quantum supremacy' – but IBM disagrees." *The Guardian* .
https://www.theguardian.com/technology/2019/oct/23/google-claims-it-has-achieved-quantum-supremacy-but-ibm-disagrees