THE MATHEMATICS OF LATTICE-BASED CRYPTOGRAPHY

1. Introduction

Alfred Menezes
cryptography101.ca

December 2024

NIST's PQC standards

- In August 2024, the US government's National Institute of Standards and Technology (NIST) published a suite of standards for key encapsulation and digital signatures schemes that are resistant to attacks by quantum computers.
- These quantum-safe schemes are intended to replace their RSA and ECC counterparts, which we know can be completely broken by attacks that run on quantum computers.
- Even though the timeline for building cryptographically-relevant quantum computers remains uncertain, the effort to replace ECC and RSA with quantum-safe algorithms is accelerating.

Kyber and Dilithium

- The quantum-safe schemes that are expected to see the most deployment in the coming years are **Kyber** and **Dilithium**.
- The security of Kyber is based on the hardness of the **Decisional-Module-Learning With Errors** (D-MLWE) problem, which in turn is related to the hardness of the **Module Learning With Errors** (MLWE) problem.
- The security of Dilithium is based on the hardness of D-MLWE and also the **Module Short Integer Solutions** (MSIS) problem.

Lattice-based cryptosystems

- In my short course "Kyber and Dilithium", I gave detailed descriptions of Kyber (ML-KEM) and Dilithium (ML-DSA) as standardized in the NIST standards FIPS 203 and FIPS 204.
- I didn't explain the connection between Kyber/Dilithium and lattices.
- The purpose of this course is to fill this gap, and explain why the MSIS and MLWE problems can be viewed as computational problems with lattices.
- This will justify calling Kyber and Dilithium **lattice-based cryptosystems**.

Course outline

1. Introduction
2. Short Integer Solutions (SIS) problem
3. Learning With Errors (LWE) problem
4. Lattices
5. SIS/LWE and lattices
6. Ring-SIS and Ring-LWE
7. Module-SIS and Module-LWE

Course material

- The course webpage is cryptography101.ca, where you can find links to the Youtube **videos** and the lecture **slides**.
- If you are just getting started in post-quantum cryptography, you should first watch the following videos from my "Kyber and Dilithium" course:
  - **V1a**: Post-quantum cryptography
  - **V1b**: Mathematical prerequisites
- My other online courses are:
  - Kyber and Dilithium
  - Cryptography 101: Building Blocks
  - Cryptography 101: Deployments (coming in 2025)
  - Error-Correcting Codes

Please subscribe to my YouTube channel and recommend my courses to your colleagues and fellow students.