qFALL
Quantum-Resistant Fast Lattice Library

Laurens Porzenheim
Codes and Cryptography
July 18 2022
A Post-Quantum World
- Used by everyone daily for secure communication
- Relies on hardness of factoring, discrete logarithm
- Example: TLS, the ‘s’ in https
Bigger and better quantum computers are being developed

They break current public key cryptography

Shor’s Algorithm is used to break factoring, discrete logarithm
Lattices and Lattice Problems

- Lattice problems are conjectured to be quantum-resistant
  - E.g. finding a shortest vector in high-dimensional lattices
  - Learning With Errors
- Build new cryptography based on these problems
- The first constructions are being standardized by NIST
Learning With Errors

LWE:

- Choose a random matrix $A \in \mathbb{Z}_q^{m \times n}$ and random secret $s \in \mathbb{Z}_q^n$
- Choose an error term $e$ from distribution $\chi$
- Compute $b = As + e$
- Then $b$ looks indistinguishable from uniform, if an adversary only knows $A$
- We can build encryption schemes from this
Learning With Errors

LWE:

- Choose a random matrix $A \in \mathbb{Z}_q^{m \times n}$ and random secret $s \in \mathbb{Z}_q^n$
- Choose a an error term $e$ from distribution $\chi$
- Compute $b = As + e$
- Then $b$ looks indistinguishable from uniform, if an adversary only knows $A$
- We can build encryption schemes from this

Things to implement:

- How to sample $A, s$?
- How to do matrix-vector multiplication?
- How to choose and implement $\chi$?
  - E.g. discrete Gaussian
- Use more efficient base problems, such as Ring-LWE
  - In this case, $A \in \mathcal{R}_q^m$ with $\mathcal{R} = \mathbb{Z}_q[X] \setminus (X^n + 1)$
Learning With Errors

LWE:
- Choose a random matrix $A \in \mathbb{Z}_q^{m \times n}$ and random secret $s \in \mathbb{Z}_q^n$
- Choose an error term $e$ from distribution $\chi$
- Compute $b = As + e$
- Then $b$ looks indistinguishable from uniform, if an adversary only knows $A$
- We can build encryption schemes from this

Things to implement:
- How to sample $A, s$?
- How to do matrix-vector multiplication?
- How to choose and implement $\chi$?
  - E.g. discrete Gaussian
- Use more efficient base problems, such as Ring-LWE
  - In this case, $A \in \mathcal{R}_q^m$ with $\mathcal{R} = \mathbb{Z}_q[X]/(X^n + 1)$

I simply want to test my construction
$\Rightarrow$ much work for simple test
The Project Group
Our Goals

What we want:

- **Main Goal:** Open-source library for **prototyping** lattice cryptography
- Build it from the ground up (excluding number theory)
- Implementation of Basics and Schemes
  - E.g. Gaussian Sampling, Signatures, Encryption
- Implement one NIST candidate
- Somewhat optimized implementation
- Optional: write program to compute secure parameters

What is not the goal:

- Perfectly secure (we ignore side-channel attacks)
- Use every known optimization
What We Offer

- Meaningful project: will be used in the future for research (prototyping, sample implementations, teaching, ...)
- We set the first milestones, you decide how the PG will develop further depending on what interests you
- Experience in security related coding
- Short introduction, quick start, no long seminar phase
- You can use our lab (at main campus) next to our offices :)
  - short question/answer times
Prerequisites / Nice to Have

- You like writing clean or efficient code (or would like to learn/improve it).
- Understand formal specifications
- Some background in security / cryptography preferred, for instance IT Sicherheit, Introduction to Cryptography (Bachelor) or Foundations of Cryptography, Real World Crypto Engineering (Master)
- Advanced Math knowledge, if you want to do more theoretical tasks