Lattice-Based Cryptography: Post-Quantum Cryptography

Luciano Scarpaci

May 18, 2025

Abstract

This report provides an overview of lattice-based cryptography as a leading candidate for post-quantum cryptography. It covers the historical context, fundamental lattice problems, and their cryptographic applications, with a focus on the mathematical hardness assumptions that underpin their security.

1 Introduction

Cryptography is the practice and study of designing protocols to prevent third parties or the public from reading private messages. The earliest evidence of cryptography dates back to Ancient Rome, where Julius Caesar used the Caesar cipher, a simple substitution cipher. Over time, cryptographic methods have evolved, from the ciphers of Mary Queen of Scots to the Enigma machine used during World War II.

In 1976, Diffie and Hellman introduced secure key agreement based on the discrete logarithm problem. A year later, Rivest, Shamir, and Adleman developed RSA, a public-key encryption scheme based on the integer factorization problem. These problems are computationally hard for classical computers.

However, in 1994, Peter Shor developed a polynomial-time quantum algorithm for integer factorization, threatening the security of RSA and similar schemes. As quantum computers advance, there is a pressing need for cryptographic algorithms that remain secure against quantum attacks. Among the candidates submitted to the National Institute of Standards and Technology (NIST), lattice-based cryptography stands out as a promising solution.

2 Lattice-Based Cryptography

Lattice-based cryptography can be used to construct post-quantum secure hash functions, signature schemes, public-key systems, and to secure existing internet protocols.

2.1 What is a Lattice?

A **lattice** is a periodic arrangement of points in space generated by integer linear combinations of basis vectors. Formally, for basis vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, the lattice is

$$L = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

A basis of a lattice is a set of linearly independent vectors that generate all points in the lattice.

2.2 Hard Problems in Lattices

Lattice-based cryptography relies on the presumed hardness of certain lattice problems, even for quantum computers.

- **Shortest Vector Problem (SVP):** Given a basis for a lattice L, find the shortest nonzero vector in L.
- **Closest Vector Problem (CVP):** Given a basis for L and a target vector $\mathbf{t}$, find the lattice vector closest to $\mathbf{t}$.
- **Unique Shortest Vector Problem (uSVP):** Find the shortest vector in a lattice where it is unique up to sign.
- **Bounded Distance Decoding (BDD):** Given a lattice basis B and a vector $\mathbf{t}$ close to the lattice, find the closest lattice vector.
- **Shortest Independent Vectors Problem (SIVP):** Find n linearly independent lattice vectors, all as short as possible.

Many of these problems are NP-hard or believed to be hard even for quantum computers.

2.3 Average-Case and Worst-Case Hardness

A key feature of lattice-based cryptography is that the average-case hardness of certain problems (e.g., SIS, LWE) can be reduced to the worst-case hardness of lattice problems like SVP and SIVP.

2.4 Short Integer Solution (SIS) Problem

Given a random matrix $A \in \mathbb{Z}_q^{n \times m}$, find a short nonzero integer vector $\mathbf{r} \in \mathbb{Z}^m$ such that

$$A\mathbf{r} = \mathbf{0} \pmod{q}, \quad \|\mathbf{r}\| \leq \beta.$$

SIS is used to construct collision-resistant hash functions and digital signatures.

2.5 Learning With Errors (LWE) Problem

Given a random matrix $A \in \mathbb{Z}_q^{n\times m}$, a secret vector $\mathbf{s} \in \mathbb{Z}_q^m$, and a noise vector $\mathbf{e}$ with small entries, the LWE problem is: Given $(A, A\mathbf{s} + \mathbf{e})$, recover $\mathbf{s}$. The addition of noise makes the problem hard.

2.6 Ring-LWE (R-LWE)

R-LWE is a variant of LWE defined over polynomial rings, which allows for more efficient key sizes and operations. It is used in practical post-quantum cryptographic schemes such as NewHope.

2.7 Key Exchange: RLWE-KEX

Ring-LWE-based key exchange protocols allow two parties to securely agree on a shared secret, even in the presence of quantum adversaries. The NewHope protocol is a notable example, using parameters $n = 1024$, $q = 12289$, and the polynomial ring $\mathbb{Z}_q[x]/(x^{1024} + 1)$.

3 Cryptographic Constructions

3.1 Digital Signatures from SIS

A typical lattice-based signature scheme uses a public key matrix A and a secret key matrix S with small coefficients such that $AS = 0 \pmod q$. To sign a message, the signer computes a short vector z such that $Az = H(m) \pmod q$, where H is a hash function.

3.2 Collision-Resistant Hash Functions

Ajtai's construction uses a random matrix $M \in \mathbb{Z}_q^{n\times m}$ and defines the hash function

$$h_M(\mathbf{s}) = M\mathbf{s} \pmod q$$

for $\mathbf{s} \in \{0, 1\}^m$. This function is collision-resistant under the hardness of SIS.

3.3 Public-Key Encryption from LWE

Regev's public-key encryption scheme is based on LWE. The public key is $(A, \mathbf{b}^T = \mathbf{s}^T A + \mathbf{e}^T)$, and encryption and decryption use LWE samples to hide the message.

4 Security and Efficiency

Lattice-based schemes are believed to be secure against quantum attacks and are often more efficient than classical schemes like RSA and ECC, especially in terms of speed and parallelizability. The hardness of the underlying problems is well-studied, and reductions from worst-case to average-case instances provide strong security guarantees.

5 Conclusion

Lattice-based cryptography provides a secure foundation for constructing hash functions, signature schemes, public-key encryption, and securing protocols against quantum adversaries. Its efficiency and strong security assumptions make it a leading candidate for post-quantum cryptography.

References

[1] Ding et al., “A Simple Provably Secure Key Exchange Based on the Learning with Errors Problem.”

[2] Erdem Alkim, Leo Ducas, Thomas Pöppelmann, Peter Schwabe. “Post-quantum key exchange - a new hope,” 2015.

[3] Joppe W. Bos, Craig Costello, Michael Naehrig, Douglas Stebila. “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem,” 2014.

[4] Miklos Ajtai. “Generating Hard Instances of Lattice Problems.” IBM Almaden Research Center, 1996.

[5] Oded Goldreich, Shafi Goldwasser, Shai Halevi. “Collision-Free Hashing from Lattice Problems,” 1996.

[6] Peter W. Shor. “Algorithms for quantum computation: Discrete logarithms and factoring.” In 35th Annual Symposium on Foundations of Computer Science, 1994.

[7] Dipayan Das, Jeffrey Hoffstein, Jill Pipher, William Whyte, Zhenfei Zhang. “Modular Lattice Signatures, revisited.”

[8] Vadim Lyubashevski. “Lattice Signatures without Trapdoors,” INRIA / Ecole Normale Supérieure, 2012.

[9] Vadim Lyubashevski. “On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem.” School of Computer Science, Tel Aviv University, 2009.

[10] `https://en.wikipedia.org/wiki/Ring_learning_with_errors`

[11] `https://en.wikipedia.org/wiki/Ring_learning_with_errors_key_exchange`

[12] `https://github.com/vscrypto/ringlwe`