# Lattice Based Quantum Resistant Cryptography

Virginia Tech

Alex Klee

**Abstract**

With the rapid development of quantum computers all over the world, security threats are evolving, and post quantum cryptography has emerged as a popular new field of study with the important task of safeguarding digital communication against quantum threats. Lattice based cryptographic schemes, specifically ones using taking advantage of the hardness of problems including the Shortest Vector Problem (SVP), Learning With Errors (LWE), and Short Integer Solution (SIS) are currently leading candidates for post quantum security. This report investigates the roots and motiviations for quantum resistant cryptography and explores new cutting-edge quantum resistant cryptosystems, specificlally Kyber and Dilithium, two lattice based schemes selected by NIST. I will explain the mathematical foundations of these systems, evaluate their security properties and performance metrics, and discuss their deployment in real-world applications.

## 1 Introduction

The rise of quantum computing poses a major threat to many modern cryptosystems, even ones that are widely used across the internet today today. This means that once a large enough quantum computer is built, algorithms such as RSA, Diffie-Hellman, and elliptic curve cryptography will become obsolete. This is because these systems rely on the computational difficulty of factoring large integers or solving discrete logarithm problems, tasks that are infeasible for classical computers. However, Shor's algorithm, a quantum algorithm, has been proved to solve these problems efficiently [1], which leaves these cryptosystems vulnerable. This has led to concern in academic, government, and industry communities alike about the long term security of encrypted data, especially given the "harvest now, decrypt later" attack where adversaries collect encrypted information today in the hopes of breaking it with future quantum machines. To address this threat, the field of post quantum cryptography (PQC) has emerged, with the goal of developing cryptosystems that are safe today and remain secure even against quantum adversaries. One of the leading candidates for PQC is lattice based schemes, which have been proven to be secure against classical and quantum attacks. In this paper, I will analyze the importance of PQC, discuss the technical aspects of lattices, explain why some lattice problems are hard for quantum computers, and implement and evaluate existing PQC schemes Kyber and Dilithium and how they perform when compared against modern classical and post quantum systems.

# 2 Technical Background

## 2.1 Lattices and Their Role in Cryptography

A lattice is a set of points in $\mathbb{R}^n$ formed by all integer linear combinations of linearly independent basis vectors [2]. Formally, given a set of $n$ linearly independent vectors $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ in $\mathbb{R}^n$, the lattice generated by $B$ is defined as:

$$\mathcal{L}(B) = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i \,\middle|\, z_i \in \mathbb{Z} \right\}$$

Lattices are commonly viewed geometrically, and can be described as grids of regularly spaced points extending infinitely in all directions. In two dimensions, a lattice would look like infinitely expanding parallelograms, while in higher dimensions, there are similar tilings but in an $n$-dimensional space. The region spanned by all linear combinations of the basis vectors with coefficients in $[0, 1)$ is called the fundamental region, and the volume remains constant across different bases.

Lattices are quite useful in cryptography due to the hardness of certain computational problems defined over them, usually in high dimensions. Unlike traditional computationally hard problems like discrete logarithms, some lattice problems have been shown to remain hard even for quantum computers. Also, these problems greatly increase in complexity as dimension increases, which is great for a cryptographic setting.

Lattices can also be used to implement many different cryptographic primitives, including public key encryption, digital signatures, identity based encryption, and more advanced constructions like fully homomorphic encryption. The combination of this versatility with the property of post quantum security makes lattices very important to the development of future cryptographic standards.

## 2.2 Core Problems

As mentioned before, the security of these lattice based cryptographic schemes relies on the hardness of specific computationally hard problems. I will focus on three of these problems, the Shortest Vector Problem, Learning With Errors, and the Short Integer Solution problems. These problems are believed to be hard even for quantum computers are heavily involved in lattice based cryptography schemes like Kyber and Dilithium.

### Shortest Vector Problem (SVP)

Given a basis $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ for a lattice $\mathcal{L}(B) \subset \mathbb{R}^n$, find the shortest nonzero vector in the lattice with respect to the Euclidean norm:

$$\text{Find } \mathbf{v} \in \mathcal{L}(B) \setminus \{\mathbf{0}\} \text{ such that } \|\mathbf{v}\| \text{ is minimized}$$

Although this problem seems geometrically simple, it becomes exponentially more difficult as the lattice dimension increases. SVP is known to be NP-hard with certain conditions, and there are no known polynomial time algorithms for solving in high dimensions [3]. There are existing algorithms that attempt to approximate the SVP problem, and these attacks as well as different versions of SVP are also widely studied.

### Learning With Errors (LWE)

The Learning With Errors problem can be described as a lattice based version of the classic "noisy linear system" problem: Given a random matrix $A \in \mathbb{Z}_q^{m \times n}$, a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a noise vector $\mathbf{e} \in \mathbb{Z}_q^m$, the LWE problem is to recover $\mathbf{s}$ from the set of approximate equations:

$$A \cdot \mathbf{s} + \mathbf{e} \equiv \mathbf{t} \mod q$$

where the vector $\mathbf{t} \in \mathbb{Z}_q^m$ is public. The noise vector $\mathbf{e}$ is what causes standard techniques for solving linear systems to fail, so recovering $\mathbf{s}$ becomes computationally intractable.

One important property of LWE for cryptographic settings is that it is provably as hard as worst case instances of certain lattice problems in high dimensions, subject to quantum reductions. This worst case to average case reduction essentially guarantees that any attack on LWE would require a breakthrough on solving the hardest lattice problems in general. [4]

### Short Integer Solution (SIS)

The Short Integer Solution problem is another fundamental hard problem in lattice based cryptography. It is similar to the problem of finding short vectors in the nullspace of a matrix modulo a prime. SIS serves as the security foundation for many digital signature schemes, including Dilithium. The SIS problem is formally defined as:

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

$$A \cdot \mathbf{x} \equiv \mathbf{0} \mod q \quad \text{and} \quad \|\mathbf{x}\| \leq \beta$$

for some norm bound $\beta$. The main challenge in this problem lies in finding such a short solution. Without the norm constraint, the problem would be pretty simple, since the nullspace of $A$ is typically non trivial.

The SIS problem is believed to be hard in average case scenarios and also has worst case hardness reductions from problems like SVP in ideal lattices [5]. SIS is usually used as the basis for hash-and-sign schemes, where the goal is to produce signatures that are both short and secure. Unlike LWE, SIS is a homogeneous problem, which makes it ideal for constructing signatures where collision resistance is needed.

## 2.3 Cryptographic Constructions

Now that we have defined lattices and the SVP, LWE, and SIS problems, I can define how lattices are used in cryptographic structures for tasks including public key encryption, digital signatures, and key encapsulation.

### Structured Lattice Problems: Module-LWE and Module-SIS

Lattice based cryptosystems often use structured lattices, which are just lattices with additional algebraic properties. Two important problems built on structured lattices are Module-LWE and Module-SIS, which generalize LWE and SIS to work over modules of polynomial rings.

- **Module-LWE:** This is a version of the LWE problem where secrets and error terms are vectors over a module of the ring $\mathbb{Z}_q[x]/(f(x))$, and the goal is still to recover the secret from noisy inner products. The lattice here is structured but still discrete. Kyber, the NIST selected encryption scheme, is built on this foundation. [6]

- **Module-SIS:** This problem involves finding short vectors that satisfy a linear relation over a structured lattice. In Dilithium, signatures are produced by sampling short lattice vectors and using hash based challenges to prove knowledge of the secret without revealing it. The security of this problem relies on the difficulty of finding sufficiently short vectors in module structured lattices. [7]

# 3 Implementation

In this section I will explore two different cryptosystems that take advantage of these hard problems. The two I will describe are Kyber and Dilithium, two NIST standardized postquantum algorithms.

## 3.1 Kyber

Kyber is a lattice based key encapsulation mechanism that has recently been selected by the NIST as a standard for post quantum public key encryption. It is built upon the Module-LWE problem, specifically over polynomial rings with modulus $q = 3329$ [6].

In Kyber, the private key consists of one or more short vectors in a the described lattice. The public key is derived by computing a noisy matrix vector multiplication using a public matrix $A$ and the secret vector $\mathbf{s}$, along with a small noise vector $\mathbf{e}$:

$$\mathbf{t} = A \cdot \mathbf{s} + \mathbf{e} \mod q.$$

This output $\mathbf{t}$ then becomes part of the public key. In the encapsulation process, a shared secret is encoded and embedded into a noisy lattice point. The ciphertext can then be computed, consisting of two components, the encrypted secret vector and the polynomial component. Both of these are constructed such that the receiver can use their secret key to cancel the noise and recover the shared secret [6].

## 3.2 Dilithium

Dilithium is a post quantum digital signature scheme that also leverages structured lattice problems. Dilithium was also selected as a NIST standard for post quantum digital signatures. It is based on the Module-SIS problem and Module-LWE [7].

Dilithium operates under a "commitment-challenge-response" style protocol. First, the signer samples a random short lattice vector and computes a commitment. This commitment, together with the message, is hashed to generate a challenge. The signer then combines the challenge with their secret key to produce a response. To make sure no secret information is leaked, the response is bounded by a specific norm. If it exceeds this bound, the process is rejected and retried, which guarantees it is statistically random [8].

Many lattice based signatures rely on trapdoors or Gaussian sampling, but it is important to note that Dilithium does not use either of those, which makes its implementation a lot simpler. Dilithium is designed to ensure that signatures are both small and efficient for both signing and verification.

# 4 Security Analysis

## 4.1 Security Foundations of Lattice Based Systems

We know that lattice based cryptography derives its strength from hard mathematical problems on lattices, particularly the three problems discussed earlier. A critical advantage of these problems that helps prove their security is their connection to worst case hardness guarantees. Specifically, there exist reductions from worst case lattice problems such as the Shortest Vector Problem and the GapSVP to average case instances of LWE and SIS [9]. This means that an attack capable of breaking a lattice based scheme in the average case would also be capable of solving some of the hardest lattice problems in the worst case, which is clearly a strong theoretical foundation for security.

Perhaps the most important property of these problems is their resistance to quantum attacks. Unlike classic hard problems like prime factorization and discrete logaithms which are vulnerable to Shor's algorithm, there are no known quantum polynomial time algorithms for solving LWE or SIS. This fact is a big reason why lattice based schemes are a leading candidate for post quantum cryptography.

## 4.2 Attacks and Cryptanalysis

While lattice based cryptograhy clearly has strong security foundations, these schemes are of course not immune to cryptanalysis. Most attacks involve lattice reduction, where the goal is to find short vectors in a high dimensional lattice. Two examples of this are the Lenstra–Lenstra–Lovász (LLL) algorithm and Block Korkine-Zolotarev (BKZ) [10]. BKZ is somewhat of an improvement on LLL due to the operation under a set block size.

These attacks are great for lattice reduction in low dimensions, but the success of the attacks is very limited once the lattice dimension grows high. For this reason, lattice schemes like Kyber and Dilithium use lattices of dimension 512 or higher, which is way beyond the reach of current lattice reduction algorithms, including LLL and BKZ. The runtime of BKZ grows exponentially with the block size, so it becomes infeasible to apply at higher dimensions. There are some quantum algorithms that offer polynomial speedups parts of these algorithms, but currently there is still no full quantum algorithm capable of solving LWE or SIS efficiently. Extensive cryptanalysis has so far failed to find any major vulnerabilities in the NIST selected systems Kyber and Dilithium.

# 5 Performance Evaluation

## 5.1 Kyber vs RSA

Kyber comes with three different versions: Kyber512, Kyber768, and Kyber1024, which have AES128, AES192, and AES256 security levels, respectively. In this section, I will compare the security levels, key sizes, and ciphertext sizes for the three kyber versions and 2 versions of RSA. RSA is a very widely deployed cryptosystem due to its provable security on classical computers and efficiency, so it serves as a good benchmark to compare to Kyber. This table shows the scheme used, along with the security level, key sizes, and ciphertext sizes:

| Scheme | Security | Public Key (B) | Private Key (B) | Ciphertext (B) |
|---|---|---|---|---|
| Kyber512 | AES128 | 800 | 1632 | 768 |
| Kyber768 | AES192 | 1184 | 2400 | 1088 |
| Kyber1024 | AES256 | 1568 | 3168 | 1568 |
| RSA3072 | AES128 | 384 | 384 | 384 |
| RSA15360 | AES256 | 1920 | 1920 | 1920 |

As we can see, RSA has smaller sizes for AES128 level security, but as the security level increases, RSA's key sizes grow much more rapidly than Kyber. Kyber also has low runtime for key generation and encryption, so it is definitely a promising alternative to systems that are broken by quantum algorithms.

### 5.2 Dilithium vs Other Signature Schemes

In this section I will evaluate the performance of Dilithium against 3 other post quantum signature schemes as well as RSA-4096. Falcon is another lattice based scheme, and SPHINCS+ is a stateless hash based signature scheme. This study from Mandev and Kavun [11] shows that Dilithium provides fast signing and verification times across multiple platforms. It also outperforms RSA significantly at comparable security levels. The left graph compares the time taken to sign a message for 9 different message lengths, while the graph on the right shows the time taken to verify a message for 9 different lengths.

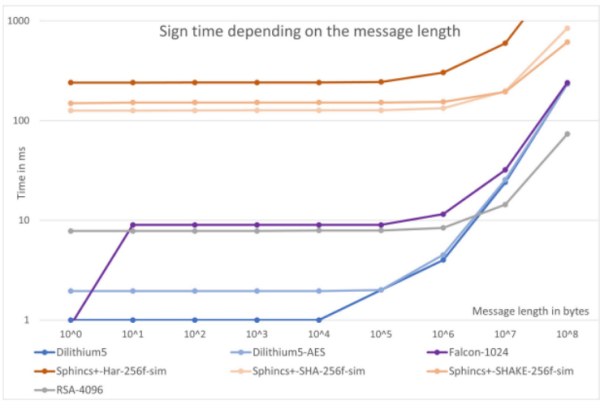


Figure 1: Sign Time / Message Length [11]

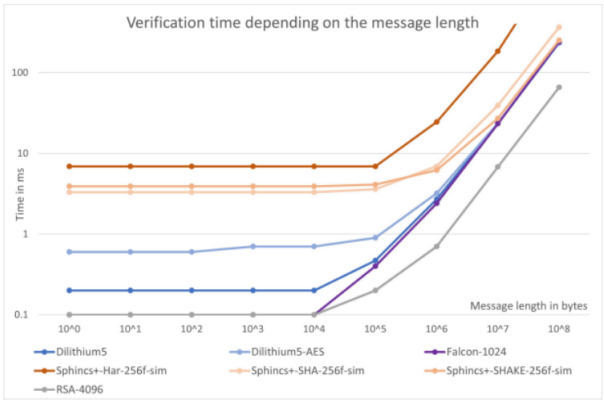


Figure 2: Verification Time / Message Length [11]

The study clearly demonstrates that Dilithium offers quite efficient performance alongside its proven security. Its signing times are consistently faster than SPHINCS+ and RSA-4096, and slightly slower than Falcon in some cases although it comes at the cost of added complexity. For verification, Dilithium outperforms both Falcon and SPHINCS+ across almost all message lengths. This performance combined with its strong security shows why Dilithium was selected as the NIST's preferred lattice based signature scheme.

## 6 Real-World Applications

Although the main goal of post quantum cryptography is securing digital communications in the presence of quantum computers, some lattice based cryptographic schemes like Kyber and Dilithium

have already began integrating into real world systems. Both were selected by NIST as part of the first standardized post quantum cryptographic algorithms, and were deemed ready for deployment. These schemes have also been picked up by large companies such as Google and Clouldflare, who experimented with Kyber in TLS 1.3. Some existing TLS connections online are actually already using Cloudflare [12]. Also, these schemes are included in widely used cryptographic libraries such as OpenSSL, BoringSSL, and liboqs, so developers can begin using them today. Kyber, Dilithium, and other lattice based schemes have the potential to span a range of security domains: secure email communication, signing for embedded devices, VPNs, and key storage. These systems are also being incorporated into hybrid schemes that use both classical and quantum resistant algorithms together.

# 7 Open Problems and Future Directions

Despite significant recent progress, several open challenges remain in lattice based cryptography, along with post quantum cryptography in general. One key area that has been heavily researched is the optimization of implementations such as Kyber and Dilithium for low resource environments such as IoT and mobile devices, since they are relatively compact. There are also some long term concerns in these schemes, since quantum computing is still a very new and raw field of study and it is hard to predict what type of attacks may develop in the future. With that being said, I believe that the replacement of classic cryptography algorithms with quantum resistant ones like Kyber and Dilithium will continue and spread widely across the internet.

# 8 Conclusion

Lattice based cryptography offers a promising path forward in the face of uncertain quantum threats, with provable security grounded in hard mathematical problems even for quantum adversaries. Kyber and Dilithium are great examples of this promise with their practicalilty and efficiency as shown in this report. Their selection by NIST and adoption in the real world highlight the importance of transitioning to post quantum cryptography. The transition to post quantum cryptography marks a pivotal shift in the landscape digital security, and lattice based schemes stand at the forefront, potentially securing data online for decades to come.

## References


[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 1994, pp. 124–134.

[2] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[3] ——, "Lattices in cryptography: Lecture 2 – svp, gram-schmidt, lll," https://web.eecs.umich.edu/ cpeikert/lic13/lec02.pdf, 2013, lecture notes, Georgia Tech, Fall 2013. [Online]. Available: https://web.eecs.umich.edu/ cpeikert/lic13/lec02.pdf

[4] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[5] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: a cryptographic perspective*. Springer Science & Business Media, 2002, vol. 671.

[6] J. W. Bos, L. Ducas, E. Kiltz, T. Lange, C. van Vredendaal, and J. Renes, "Crystals - kyber: A cca-secure module-lattice-based kem," in *IACR Cryptology ePrint Archive*, no. 634, 2017.

[7] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals - dilithium: Digital signatures from module lattices," in *IACR Cryptology ePrint Archive*, no. 633, 2017.

[8] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology – EUROCRYPT 2012*. Springer, 2012, pp. 738–755.

[9] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM, 1996, pp. 99–108.

[10] K. Abe and M. Ikeda, "Estimating the effectiveness of lattice attacks," Cryptology ePrint Archive, Paper 2021/1489, 2021. [Online]. Available: https://eprint.iacr.org/2021/1489

[11] R. Mandev and E. B. Kavun, "Performance comparison of post-quantum signature algorithms through an android email application plug-in," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, 2023, pp. 1–6.

[12] B. Westerbaan. (2024) The state of the post-quantum internet. Accessed: 2025-05-08. [Online]. Available: https://blog.cloudflare.com/pq-2024/