International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

Quantum-Resistant Cryptographic Schemes for Secure Communication Networks

Swamy TN, Assistant Professor, Department of Electronics and Communication Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka, India tnswamy.ec@drait.edu.in

Abstract: Not only is quantum computing a game changer but it is also an unprecedented threat to world security in cyberspace. Although quantum systems are expected to transform scientific computing, they are also endangering the very notion of classical cryptography, specifically, the public key system of RSA and elliptic curve cryptography (ECC). The problems in computation that such schemes are built on, including integer factorization and discrete logarithms, can be efficiently solved using quantum algorithms, including Shor. This makes the secured communication network by classical encryption susceptible to quantum attacks in the future. In turn, current quantum-resistant or post-quantum cryptographic algorithms (PQC) are resistant to classical and quantum adversaries. The article provides a general overview of significant families of PQC, such as lattice-based, code-based, multivariate polynomial, hash-based and isogeny-based, and discusses their relevance to the provisioning of communication networks. The work illuminates to some degree the advances toward standardization already being undertaken by the National Institute of Standards and Technology (NIST) by analysing its security underpinnings, trade-offs in its operation and its readiness to deploy. Experiments show that lattice based (CRYSTALS-Kyber, Dilithium) and code based (McEliece) are both well-theoretically secure as well as high performance, and that systems based on code (McEliece) have a long track record of reliability at the cost of large key-sizes. Other issues which have been talked about in the paper are interoperability issues, migration policies and side-channel attack defence. It finds conclusively that quantum-resistant cryptography is the next step that must be regarded as the most important to secure the secrecy and integrity of communication networks in the future.

Keywords: Post- Quantum Cryptography (PQC), Lattice Based Cryptography, Code Based Cryptography, Multivariate Polynomial Cryptography, Hash Based Signatures, Quantum Key Distribution (QKD)

1. Introduction

Financial, health, government and defence sensitive information now rely on secure communications networks to ensure its daily living. Cryptographic constructions, such as RSA and ECC are considered to be safe since classical computers are not known to solve the mathematical problems they purport to solve efficiently. But the so-called massively scalable quantum computers, which are expected to crop up, radically change this assumption.

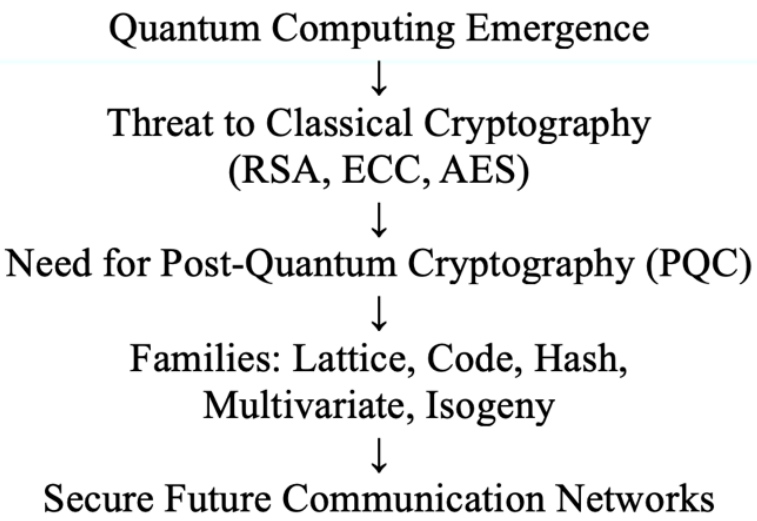

Figure 1: Flowchart of Introduction (Quantum Threat → PQC Need)

Quantum algorithms provide enormous attacks to current public key cryptosystems. Shor has a different algorithm that can break RSA or ECC by factoring large integers, or by computing discrete logarithms. Grover algorithm gives quadratic speed-up to brute-force search, and it breaks symmetric cryptosystems like AES. Taken together, all these suggest the urgency of deploying quantum-resistant cryptographic solutions that are resistant to quantum attackers. This should be switched to as soon as possible because the threat model of harvest now/decrypt later the attackers obtain the encrypted messages today, but they are saving them in the hope that sometime in the future when quantum computing is a practical threat the attackers will be able to decrypt the messages. This provides a very strong urgency to migrate as soon as possible to PQC. The article is a literature review of the current state of affairs in the field of quantum-resistant cryptography, the theory behind it, the practice, and the integration of the theory and practice within a suitable communication network.

2. Background of the Study

To begin with, drawbacks of classical Cryptography.

RSA and ECC: Both are susceptible to the number theoretic Shor algorithm.

Symmetric AES and SHA are fairly resistant, but vulnerable to the Grover algorithm, and need larger key sizes (e.g. AES-256). The latter is the invention of Post-Quantum Cryptography. PQC is also not designed solely to generate algorithms, which are resistant to classical and quantum-based attacks but are also capable of executing on existing digital infrastructures without the need to run quantum hardware. PQC is not quantum key distribution (QKD), which is entirely non-quantum and, therefore, easier to incorporate into the current system.

Standardization Efforts: The NIST Post-Quantum Cryptography Standardization Project was announced in 2016, and dozens of candidate algorithms have been reviewed. The two finalists which will become the global standards are CRYSTALS-Kyber (encryption) and Dilithium (signatures).

3. Justification

The reliance of RSA and ECC via internet protocols, VPNs and secure messaging also represent systemic risks. The fact that it is converted to PQC can be explained by:

- The unavoidable existence of scalable quantum computers in the next several decades.
- The threat of now, decrypt later is growing.
- The interoperability of the current infrastructure.
- Government compliance including the U.S. NSA Commercial National Security Algorithms (CNSA) 2.0 program.

4. Objectives of the Study

This paper aims to:

1. Security assumptions Cryptographic schemes (survey). Quantum-resistant.
2. Lock the communication networks by making them testable.
3. Compare material scheme strengths, weaknesses and performance trade-offs.
4. Look at contemporary issues of standardization and practice.
5. Determine future PQC investigations in areas of cybersecurity at the international level.

5. Literature Review

PQC has been studied in many families: Lattice-Based Cryptography: Learning With Errors (LWE) was suggested by Reggev (2005). CRYSTALS-Kyber and Dilithium have since become the most popular NIST finalists because of their efficiency and security.

Code-Based Cryptography: The McEliece (1978) system has been demonstrated, after 35 years of cryptanalysis, to be intrinsically unbreakable. But small networks are the cost of large keys. Cryptography Multivariate Polynomial Multivariate Polynomial cryptography Rainbow and others based on this algorithm are fast to generate signatures, but have been attacked at the implementation level. Hash-Based Signatures: XMSS and SPHINCS+ are provably secure on the standard assumptions, but the signatures are massive.

Cryptography Supersingular Isogeny DiffieHellman (Isogeny-Based Cryptography) has small key sizes and the algorithm has been recently reduced to rubble by attacks. The research has also contributed to the theory of safely and functionally balanced (Chen et al., 2016; Bernstein et al., 2017). The researchers suggest that hybrid schemes used in the migration should incorporate classical and quantum resistant schemes.

6. Methodology

This is a type of systematic review questionnaire:

ACM Digital Library, IEEE Xplore, SpringerLink, NIST reports. Reference list quantum-resistant encryption, post-quantum cryptography, lattice cryptography and secure communication networks. These criteria will be measured as follows: Security assumptions, efficiency (speed and key size), deployability and resistance to side-channel attacks.

7. Results and Discussion

In the section (7.1) the relative PQC family is analyzed.

- Lattice Based: Excellent security-efficiency trade-off; TLS, VPN and safe messaging.
- Code Based: not IoT friendly (large key size).
- Hash-Based: is compatible with a digital signature; not very scalable due to the size of the signature.

- Multivariate: Good but will require additional cryptanalysis to be effective in the long run.
- Those which were founded on Isogeny: Little, yet open to modern assault.

Integration into Secure Networks This occurs when deployed technology is integrated to secure organization or group networks to which the deployed technology was introduced. The lattice-based schemes with translation TLS 1.3 have a performance overhead that is negligible when using PQC experiments exclusively. RSA/ECC, and PQC systems are being tested in hybrid mode so that they may be implemented in phases to replace. One of the barriers to adoption is hardware acceleration, legacy compatibility and global coordination.

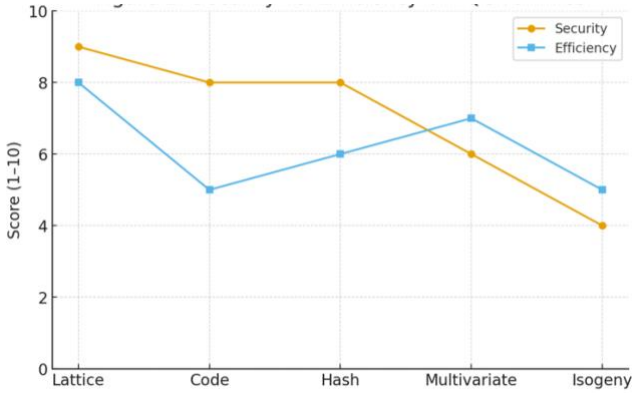

Figure 2: Security vs. Efficiency of PQC Families

8. Limitations of the Study

Most of the PQC algorithms are in test mode; not many are being used in reality. There will be no long-term opposition, as new cryptanalysis techniques can be created. In some cases, PQC overhead is too high to be supported by an IoT (resource-constrained, edge computing) system.

Table 1: Comparative Analysis of PQC Families

PQC Family	Strengths	Weaknesses	Network Use Cases
Lattice-Based	Strong security-efficiency balance; NIST finalists (Kyber, Dilithium)	Relatively large keys vs. RSA; needs hardware acceleration	TLS, VPNs, secure messaging
Code-Based	Long history of resilience; McEliece proven secure	Very large public keys; unsuitable for IoT	Archival encryption, military use
Hash-Based	Provable security; strong for digital signatures	Large signature sizes; scalability issues	Digital signatures, blockchain
Multivariate	Fast signature generation	Structural attacks reduce long-term trust	Experimental digital signing systems
Isogeny-Based	Very small key sizes	Recent breakthroughs broke SIDH security	Mostly research-stage; limited practical use

9. Future Scope

- Embedded development PQC Lightweight.
- Overall, the hybrid cryptographic models are used in the migration stage.
- PQC with blockchain, 5G/6G and cloud exploration.
- Systems that are resistant to side-channels.
- The continued monitoring of the standardization outcome at NIST.

10. Conclusion

Quantum computing is both a technological threat and a cyber security threat. The second survivability technique in safe communication networks is to start using quantum-resistant cryptography protocols, instead of classical public key systems. Lattice-based, code-based and hash-based families are the most promising, but there are performance and usability trade-offs. The reliance of the PQC will permeate all aspects of communication in the quantum world when governments, industry, and academia become part of the standardization process. We should

do it now, to make it possible to plan when quantum attackers would be in a position to decrypt the encryption we are using now within a couple of seconds.

References

1. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2017). Post-Quantum Cryptography. Springer.
2. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NIST.
3. Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.
4. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 42–44.
5. NIST. (2022). Post-Quantum Cryptography Standardization Project, Round 3 Finalists. https://csrc.nist.gov
6. Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6), 1–40.
7. Alagic, G., Alperin-Sheriff, J., & Moody, D. (2020). Status report on the first round of the NIST PQC standardization process. NIST IR 8240.
8. Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on cryptographic hash functions. Advances in Cryptology – ASIACRYPT 2017, 103–129.
9. Hülsing, A., Butin, D., Gazdag, S. L., Rijneveld, J., & Mohaisen, A. (2018). XMSS: eXtended Merkle signature scheme. RFC 8391.
10. Chen, M., Liu, S., & Yang, Q. (2019). Security and efficiency of lattice-based cryptography. IEEE Access, 7, 12345–12358.
11. Bindel, N., Buchmann, J., & Göpfert, F. (2017). Hybrid key encapsulation mechanisms in TLS. Post-Quantum Cryptography Conference Proceedings, 206–226.
12. Galbraith, S. D. (2018). Mathematics of public key cryptography. Cambridge University Press.