IJHSR
ijhighschoolresearch.org
REVIEW ARTICLE

A Review of the Post-Quantum Cryptographic Landscape

Devyansh Lilaramani

Emirates International School Jumeirah, Al Thanya St - Umm Al Sheif - Dubai, Dubai, 00000, UAE; devyanshlilaramani3008@gmail.com

ABSTRACT: As the development of quantum computing systems advances, the integrity of current public-key and symmetric-key cryptographic systems, such as RSA, ECC, and AES, faces unprecedented threats. These systems rely on mathematical problems like integer factorization and discrete logarithms, which quantum algorithms like Shor's can solve exponentially faster than classical ones. This review examines the vulnerability of widely used cryptographic systems and evaluates how close quantum hardware is to breaching real-world encryption. It also discusses the development of post-quantum cryptographic algorithms, specifically lattice-based, code-based, and multivariate polynomial systems designed to resist quantum attacks. This paper will also assess the strengths, limitations, and standardization progress of these post-quantum solutions to provide an understanding of the modern cryptographic landscape.

KEYWORDS: Computer Science and Software Engineering, Post-Quantum Cryptography, Quantum Computing, Shor's Algorithm, Grover's Algorithm, NIST PQC Standardization, Quantum Threats.

Introduction

Quantum computing, once thought to be a distant or theoretical concept, now threatens to unravel the mathematical foundations of modern cryptography, rendering technologies like RSA and ECC obsolete.[1] Used for over 25 years now, protocols like RSA, Advanced Encryption Standard (AES), and elliptic curve cryptography (ECC) have been the backbone of digital security systems applied to a large part of the Internet, from online banking to secure messaging, relying on the presumed impossibility of classical computers to feasibly solve integer factorization and discrete logarithm computational problems. Peter Shor's 1994 algorithm shattered these assumptions, positing that a sufficiently powerful quantum computer could solve both problems in polynomial time as a result, regulatory bodies, such as the NIST have released publications evaluating range of primitive quantum resistant systems such as lattice based, code based, multivariate, and hash based methods with the goal of replacing these vulnerable standards before they are compromised.[1,2] Proof of concept systems, such as Google's New Hope key Exchange in Chrome provides feasibility to the idea of a global switch to quantum-resistant systems.[3]

This paper thus investigates to what extent current public and symmetric key cryptographic techniques and systems are vulnerable to quantum attacks, and how emerging post-quantum algorithms are addressing these risks.

The first primary concern that this paper will address is the threat of the "harvest-now, decrypt-later" model, which suggests that malicious actors could store encrypted data today with the idea that they will be able to one day, with sufficient advances in quantum hardware, break today's encryption standards.[4]

The second issue lies with the logistical and technical complexities of transitioning to quantum-safe systems, more specifically the challenge of orchestrating mass cryptographic protocol updates across millions of devices and services while avoiding systemic failures, made all the more urgent by the fact that recent analyses show that large scale quantum attacks could become feasible within the next decade, adding a time factor to a coordinated transition to resilient cryptographic standards.[5]

This paper argues that while quantum computing poses an imminent threat to the mathematical foundations of today's cryptography standards, a pivot to post-quantum standards can help preserve and safeguard digital infrastructure. Lattice-based schemes, such as New Hope and Kyber, as well as code-based constructions, have demonstrated strong security proofs while remaining suitable for real-world deployment.[3,6] Although large-scale quantum computers, capable of breaking current encryption like RSA or ECC, are not yet fully operational, consistent advances in quantum technologies suggest that they may realistically be realized within the next decade.[6] Even today, small-scale quantum devices have proven capable of executing simplified versions of Shor's algorithm, demonstrating the feasibility of quantum attacks.[7] This paper also states that addressing the threats posed by quantum computing systems requires two steps: the first of which is establishing global consensus on standardized algorithms, and the second is managing a coordinated transition of existing cryptographic systems to quantum-resistant solutions.

Discussion

I. A brief history of quantum cryptography:

The origins of quantum cryptography can be traced back to the seminal work of Charles Bennett and Gilles Brassard, who in 1984 released their BB84 protocol, a groundbreaking framework that utilized principles of quantum mechanics, specifically the no-cloning theorem and Heisenberg's uncertainty principle, to ensure that any attempt to make a copy of information on the quantum channel would create disturbances.[2,8]

DOI: 10.36838/IJHSR811.1

By grounding security in the laws of quantum mechanics, the BB84 protocol laid the conceptual foundation for a new era in secure communications, though practical implementation seemed unfeasible at the time.

The need for quantum secure methods gained immense momentum with the introduction of Shor's algorithm, developed by its namesake Peter Shor in 1994, capable of factoring large integers and calculating discrete logarithms in polynomial time, revealing that public key systems such as RSA and ECC could theoretically be rendered vulnerable once sufficiently powerful quantum hardware became available.[1] Shor's algorithm has not only catalyzed research into physical layer defenses like quantum key distribution (QKD) but also prompted further exploration of post-quantum cryptographic primitives, cryptographic methods designed to remain secure against attacks from quantum computers, while being able to be implemented by classical hardware and infrastructure.[2,9]

From the late 1990s and early 2000s, discussions on quantum cryptography gradually progressed from theoretical concepts to how they could be applied and implemented in real-world settings. Research groups began demonstrating basic implementations of quantum key exchange over short distances, using fiber optic infrastructure, marking a significant milestone in validating QKD. Soon after, organizations like ETSI began releasing documentation guiding migration from classical encryption systems to quantum-safe approaches, highlighting the practical and infrastructural challenges involved in such a transition.[10] Adding to this urgency is the "harvest now, decrypt later" attack vector, which posits that malicious actors may already be capturing encrypted traffic today, with the intention of storing it until quantum computers reach a level of capability such that they would be able to decrypt it.[4]

Table 1: Key milestones in the development of quantum cryptography and quantum computing.

Year	Event	Explanation	Significance
1984	BB84 Protocol	Bennet and Brassard published the BB84 protocol, the start of quantum key distribution as a field.	The world's first quantum key distribution protocol
1991	E91 Protocol	Ekert proposes entanglement-based quantum key distribution (QKD) using Bell inequality checks.	Introduced entanglement-based QKD and applied Bell-inequality tests, showing that quantum correlations can be used to detect eavesdropping.
1992	First QKD lab demo	Bennet, Brassard, *et al.* report successful implementation of the BB84 protocol in a laboratory environment.	Demonstrated that QKD was practically feasible rather than purely theoretical.
1994	Shor's algorithm	Peter Shor publishes his algorithm proposing polynomial-time for factoring and discrete logarithm problems on an ideal quantum machine.	Illustrated that a quantum computer could solve integer factoring and discrete log problems in polynomial time, threatening classical cryptography.
1996	Grover's algorithm	Grover's algorithm was published, positing a quadratic speedup in the time taken to search an unsorted array.	Showed that even non-factorization problems benefit from quantum computing.
1998	First QEC demonstrations	The early lab demonstrations of quantum error-correcting code (QEC) were the first step towards fault-tolerant quantum computing.	Began the transition from experimentation to the development of fault-tolerant quantum architectures by showing that quantum error-correcting code could be physically realized.
2001	Shor's algorithm applied to N = 15	A nuclear magnetic resonance quantum computing device was used for the first-ever implementation of Shor's algorithm to factor the number 15.	The first physical demonstration of Shor's algorithm confirmed that quantum algorithms could be implemented rather than just theorized.
2007	QKD implemented over a 200km distance using fiber	Decoy-state BB84 QKD over 200km standard telecom fiber, demonstrating practical implementation.	A real-world scale implementation of QKD, establishing the viability of quantum cryptography in long-distance classical infrastructure.
2010	Tokyo QKD network goes live	Multi-vendor, city-wide QKD network launched, demonstrating interoperability for city-scale QKD.	Established that quantum communications could scale in urban environments with interoperability.
2017	Satellite QKD achieved	Entanglement distribution and QKD achieved over 1200km via the Micius satellite.	Demonstrated that quantum communications could be implemented globally.
2023	IBM Condor	IBM announced and operated a 1121-qubit quantum superconducting processor, marking a breakthrough in quantum hardware.	Marked the first gate-model quantum processor to surpass 1,000 qubits, setting a new benchmark for scale in quantum hardware.

Table 1 illustrates how quantum cryptography and quantum computing have evolved alongside rising cryptographic threats; in the following section, we examine the current and emerging quantum-threat landscape.

II. Survey of quantum threats:

While the advent of quantum cryptography has opened new avenues for securing information, the rapid advancement of quantum hardware simultaneously endangers the classical cryptographic systems that secure the Internet, along with all of its related infrastructure. This section reviews the algorithms and hardware developments that drive these risks and illustrates how experimentation with these algorithms is gradually moving towards practical attacks.

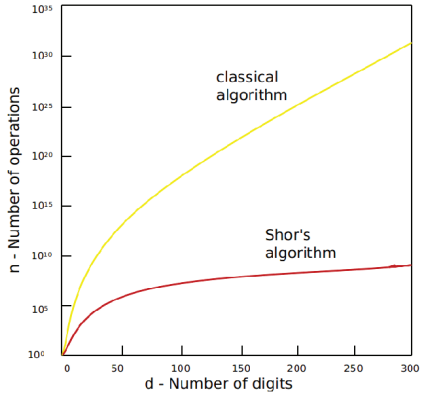

Figure 1: A visual comparison of the number of operations required by a classical algorithm in comparison to Shor's algorithm with respect to the number of digits. [11]

Even today, the primary theoretical threat to public key cryptography remains Shor's algorithm, being able to solve the integer factorization and discrete logarithm problems in polynomial time (as illustrated in Figure 1[1]). Because RSA and ECC rely on the complexity of these problems, the arrival of an amply powerful quantum computer would immediately invalidate the security that they provide. The viability of such an attack has been proven through numerous experiments in which teams have implemented a smaller-scale version of Shor's algorithm, factoring numbers such as 15 using only a small number of qubits.[5]

While Shor's algorithm targets public key cryptographic systems, Grover's algorithm, created initially to search unsorted arrays, poses a threat to symmetric ciphers by providing a quadratic speed-up of brute force key search, essentially halving the effective security of methods like AES.[12] When faced with an attack carried out by a quantum computer, a 128-bit key would be about as secure as 64 bits of security; such is the reason that bodies such as NIST and ETSI recommend doubling symmetric key sizes (e.g, moving to AES-256 from AES-128) to restore the original margin.[2,10]

In terms of hardware, progress remains incremental; quantum platforms are now reaching the low thousands of physical qubits, demonstrated by IBM's 1121-qubit Condor, the first ever quantum processor to surpass 1000 qubits, marking a significant milestone.[13] By contrast, leading superconducting and trapped ion systems from Google, Rigetti, and IonQ generally operate in the ranges of hundreds of physical qubits.[13] Despite these advances, present-day processors remain far from executing Shor's and Grover's algorithms in a way that would be threatening to modern-day cryptographic systems, largely due to their not yet supporting the levels of error correction required for cryptographic workloads. Executing Shor's algorithm, for example, on an RSA-2048 key is estimated to require thousands of highly logical qubits and trillions of tolerant gates, which implies requiring tens of millions of physical qubits running code error correction, considering today's error rates, as logical qubits are comprised of many physical qubits in order to suppress noise.[2,9,14]

Taken together, the progress in quantum computing, in addition to algorithmic breakthroughs, renders the quantum threat not only credible but time-sensitive. Even though present-day machines cannot yet crack internet-scale encryption, the demonstrated functionality of quantum attacks combined with the steady improvements in quantum hardware, as well as the ability to store encrypted data, underscores the need for immediate migration to quantum-resistant alternatives.

III. Overview of post-quantum algorithms:

This section examines the prominent examples of post-quantum algorithms, assessing their strengths, weaknesses, and current standardization status, aiming to provide a clear understanding of which algorithms are most likely to see widespread deployment as the threat of quantum attacks progresses.

Post-quantum cryptography encompasses a range of cryptographic systems, even in the presence of large-scale quantum computers.[2] The ideal goal for the systems is that they should be able to replace vulnerable public algorithms, such as RSA and ECC, as well as strengthen symmetric encryption by facilitating secure key exchange and reliable authentication.

A prominent organization involved in the standardization of post-quantum algorithms is the NIST, which evaluates PQC candidates based primarily on cost, performance, and algorithmic and implementation characteristics.[15]

The first and one of the most prominent examples of post-quantum cryptography can be seen in lattice-based schemes.[2] Relying on the computational difficulty of problems defined over high-dimensional lattices or mathematical grids, such as the learning with errors (LWE) and short integer solution (SIS) problems. An example of a lattice-based solution can be seen in the CRYSTALS-Kyber method standardized under the name ML-KEM in the NIST FIPS 203 standard.[16] ML-KEM is a method for secure key exchange on an insecure channel, using mathematical transformations based on lattice problems to ensure that only the intended participants can derive the key, which can then be used to encrypt and decrypt subsequent communications.[3,16,17]

Another post-quantum cryptographic method is the use of hash-based signatures. This method achieves security by relying on the strength of cryptographic hash functions, instead of number-theoretic ones that a quantum algorithm could crack, specifically their resistance to pre-image and collision attacks.[2] SHPINCS+, standardized in FIPS 205 as SLH–DSA, implements this idea through a stateless multi-layered tree system that generates and verifies signatures without using keys.[18] Specifically, SHPINCS+ does this by deriving one-time and few-time signing keys from a master secret seed and organizing them under a Merkle "hypertree," wherein the public key acts as the top root hash.

Code-based cryptography secures communication, not by using a number-theoretic approach like RSA or ECC, but by using the difficulty of decoding a general linear error-correcting code without knowledge of its private structure.[15] McEliece, for example, hides structured Goppa code within a large public matrix, making recovery computationally infeasible for a malicious actor. These schemes offer high-speed encapsulation and decapsulation but require extremely large public keys. In 2025, NIST selected HQC, another code-based KEM, for standardization. HQC uses a different code structure that allows for smaller public keys than McEliece, making it more practical for systems in which storage or transmission size is a concern.

Multivariate cryptography is based on the difficulty of solving large systems of quadratic equations over finite fields (also known as "the MQ problem") for which no effective quantum speed up is known (NP hard).[19] In multivariate signature schemes, the public key is a set of quadratic polynomials. The signer uses a system that can be solved efficiently and then applies masking transformations to obfuscate the solvable system from external observers. Researchers, however, demonstrated a key recovery attack on the rainbow signature scheme, revealing more vulnerability than initially anticipated, resulting in the removal of the scheme from the NIST standardization process.

DOI: 10.36838/IJHSR811.1

Conclusion

In summary, the advancement of quantum computing technologies presents a direct and measurable threat to the mathematical foundations of widely deployed cryptographic standards, such as RSA, ECC, and AES. While present-day quantum hardware lacks the scale and error correction capacity required to execute Shor's or Grover's algorithms, continued progress in hardware capabilities makes the eventual realization of such an attack a plausible near-future outcome. Post-quantum cryptographic schemes, including lattice–based, code-based, hash-based, and multivariate-based methods, show promise, providing viable and standardized alternatives that are capable of withstanding the quantum threat, as demonstrated by their selection and evaluation by the NIST. However, the effectiveness of these solutions depends entirely on the coordination of large-scale migration efforts globally. The successful preservation of secure communications in the post-quantum era will therefore rely both on the adoption of mathematically resilient algorithms and their implementations. The transition strategy should thus prioritize phasing out both RSA and ECC in critical infrastructure. Looking ahead, research should concentrate on how post-quantum standards can be deployed and how hybrid infrastructures can bridge the gap between existing and emerging encryption systems.

Acknowledgments

I would like to express my thanks to Dr. Eric Sakk and Mr. Ahmed Shaaban, as well as the rest of the Indigo Research team, for guiding me through the process of writing this paper.

References

1. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review* **1996**, *41* (2), 303–332. https://doi.org/10.1137/s0036144598347011.
2. Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. Report on Post-Quantum Cryptography. *National Institute of Standards and Technology*, **2016**. https://doi.org/10.6028/nist.ir.8105.
3. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-Quantum Key Exchange—A New Hope. In *Proc. 25th USENIX Security Symposium (USENIX Security '16)*; USENIX Association: Austin, TX, 2016; pp 327-343. DOI: 10.5555/3241094.3241120.
4. DuBose, R.; Rao, M. M. *Harvest now, decrypt later: Why today's encrypted data isn't safe forever*. Hashicorp.com. https://www.hashicorp.com/en/blog/harvest-now-decrypt-later-why-today-s-encrypted-data-isn-tsafe-forever.
5. Monz, T.; Nigg, D.; Martinez, E. A.; Brandl, M. F.; Schindler, P.; Rines, R.; Wang, S. X.; Chuang, I. L.; Blatt, R. Realization of a Scalable Shor Algorithm. *Science* **2016**, *351* (6277), 1068–1070. https://doi.org/10.1126/science.aad9480.
6. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J. M.; Schwabe, P.; Seiler, G.; Stehlé, D. "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM." *Proc. IEEE European Symposium on Security and Privacy (EuroS&P)* **2018**, 353-367. DOI: 10.1109/EuroSP.2018.00032.
7. *Quantum Threat Timeline*. Global Risk Institute. https://globalriskinstitute.org/publication/quantum-threat-timeline/.
8. Bennett, C. H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing (Archive). *Theoretical Computer Science* **2014**, *560* (1), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
9. *Tibbetts, J. Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers*; **2019**. https://cgsr.llnl.gov/sites/cgsr/files/2024-08/QuantumComputingandCryptography-20190920.pdf.
10. *Quantum-safe Cryptography and Security an Introduction, Benefits, Enablers and Challenges*; **2015**. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.
11. Gupta, K. D.; Nag, A. K.; Rahman, Md. L.; Mahmud, M. A. P.; Sadman, N. Utilizing Computational Complexity to Protect Cryptocurrency against Quantum Threats: A Review. *IT Professional* **2021**, *23* (5), 50–55. https://doi.org/10.1109/mitp.2021.3089494.
12. Grover, L. K. A Fast Quantum Mechanical Algorithm for Database Search. *Proc. 28th Annual ACM Symposium on the Theory of Computing* (STOC '96), Philadelphia, PA, USA, July 1996; pp 212-219. DOI: 10.1145/237814.237866.
13. Gambetta, J. *IBM Quantum Computing Blog | The hardware and software for the era of quantum utility is here*. www.ibm.com. https://www.ibm.com/quantum/blog/quantum-roadmap-2033.
14. Gidney, C.; Ekerå, M. How to Factor 2048-Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. *Quantum* **2021**, *5*, 433. DOI: 10.22331/q-2021-04-15-433.
15. Alagic, G. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. **2025**. https://doi.org/10.6028/nist.ir.8545.
16. Gaithersburg, MD, NIST. Module-Lattice-Based Key-Encapsulation Mechanism Standard. *Module-Lattice-Based Key-Encapsulation Mechanism Standard* **2024**. https://doi.org/10.6028/nist.fips.203.
17. Gaithersburg, MD, NIST. Module-Lattice-Based Digital Signature Standard. **2024**. https://doi.org/10.6028/nist.fips.204.
18. Gaithersburg, MD, NIST. Stateless Hash-Based Digital Signature Standard. **2024**. https://doi.org/10.6028/nist.fips.205.
19. Beullens, W. Breaking Rainbow Takes a Weekend on a Laptop. **2022**, 464–479.https://doi.org/10.1007/978-3-031-15979-4_16.

Author

Devyansh Lilaramani is a high school student at EISJ, Dubai, aiming to study computer science and engineering. He hopes to specialize in the fields of artificial intelligence or cybersecurity.