International Insurance Law Review
ISSN: 0968-2090
Vol 34 S1 (2026): Special Issue
https://lumarpub.com/iilr

Quantum Cryptanalysis: A Survey of Threats and Post-Quantum Countermeasures

Raja Shree[1]*, Bhuvan Unhelkar[2], Siva Shankar [3], Nagarajan[4]
[1]Associate Professor, Department of CSE, Sathyabama Institute of Science and Technology
[2]Professor, Muma College of Business (Sarasota-Manatee Campus), University of South Florida
[3]Professor, KG Reddy College of Engineering and Technology, Hyderabad
[4]Professor, Department of CSE, Sathyabama Institute of Science and Technology
[1]*rajijce@gmail.com, [2]bunhelkar@usf.edu, [3]drsivashankars@gmail.com,
[4]gnagarajan.cse@sathyabama.ac.in
*Corresponding Author: Raja Shree

Abstract

Quantum computing will revolutionize the power of computation, solving problems that currently have no solution classically. Such a jump in computational power presents an existential threat to modern cryptography, particularly public-key systems that rely on factoring and discrete logarithmic problems. This paper presents the emerging area of PQC countermeasures and gives a survey of quantum cryptanalysis methods. A literature review of progress from 2010 to 2025 is also provided, specifically addressing the advancement of algorithms, standards and applications. For universal security of data in the quantum age, they add, it will be critical to transition to quantum-resistant infrastructures.

Keywords: Quantum cryptanalysis, Shor's algorithm, Post-quantum cryptography, Lattice cryptography, NIST PQC, Quantum threat, Quantum algorithms.

1. Introduction

Once an exercise in theory, quantum computing is rapidly becoming a disruptive juggernaut in the world of IT; with processing capabilities far surpassing what we've seen thus far. Unlike classical computers, quantum machines harness the weirdness of quantum mechanics—superposition, entanglement and quantum parallelism—to "search for solutions to complex problems that would otherwise take longer than the lifetime of the universe to measure accurately". Today's society is witnessing the birth of what has been called the Noisy Intermediate-Scale Quantum (NISQ) era, in which quantum devices with a number of qubits in the hundred range are becoming real, thanks to major tech corporations such as IBM, Google, and Rigetti making prototypes.

Even with all this pace, careful trials become familiar with the substance of digital security. Contemporary public-key cryptosystems, for example, RSA [33], DSA [28], and ECC [19], are based on the well-established computational intractability of discrete logarithms as well as integer factoring—paradigms that have become uncertain with the development of quantum algorithms. In 1994, Shor's pioneering research and Grover's later process in 1996 demonstrated that quantum computers could expertly exploit these weak spots, severely compromising the security of block-structured encryption and digital signing. Trusted

Citation: Shree, R.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). Quantum Cryptanalysis: A Survey of Threats and Post-Quantum Countermeasures. *International Insurance Law Review*, 34 (S1), 309-318.

communication, Privilaged transactions and secured digital intractions becomes a real concern in quantum world.

Due to the emerging threats in quantum computing ,the community of global cryptographic becomes highly active. Researchers are not only trying to understand how current security mechanisms is being broken by quantum computing and also building new defense mechanisms to withstand that security breaches. Outside of the traditional maths, the researchers are exploring algebraic lattices, error-correcting codes, and multivariate polynomials knowns as Post-Quantum Cryptography (PQC).This paper focuses on the quantum hacking evolution and how the defenses are designed to stop the hacking. It also focusses on how to tackle the practical challeneges of standardizing and positioning the tools in the real world.

2. Literature Survey

The view of cryptography have been shifted intensily between the year 2010 and 2025 which drives a breakthrough in the urgent need of both theoretical and practical security. In 1990 Shor and Grover demonstrates how the quantum computers breaks the standard encryption like RSA and ECC—this turns into a warning about the security issues. Researchers started focussing on when and how the quantum attacks will happen.

Bernstein, Chen, and others created an organized framework for Post-Quantum Cryptography (PQC). The authors categorize the new defences mechanisms into four main families such as lattice-based system, code-based system, multivariate system, and hash-based systems. Out of these four , lattice-based systems like CRYSTALS-Kyber and Dilithium became the favourite based on speed, security and robustness. In the meantime, approaches like code-based and hash-based systems have also evolved, they provide security by using the key sizes and also providing essential backup options .

In 2017, NIST Post-Quantum Cryptography Standardization Program was launched. CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+ are standardized in 2022 through various cryptanalytic methods, by assessing the performance through various parameters, and by real world testing. Other than this various algorithms are still being tested for specific applications. ISO and ETSI have established global standards along with NIST that provides interoperability and compatibility.

From (2020–2025) researchers mainly focusing on performance measurement in transport layer security (TLS), virtual private networks (VPNs), and cloud infrastructure. Integration between the classical and post quantum schemes emerges the hybrid encryption technique. For example RSA is encrypted with Kyber , Elliptic curve cryptography is integrated with Dillithium enables a steady migration from traditional to conventional method. Researchers focus shifted to hybrid encryption models that combines classical schemes and post-quantum schemes (e.g., RSA with Kyber, ECC with Dilithium), that enables slow shifting to quantum by maintaining the backward compatibility in the ecosystem of cryptography. Industry experts made some wide spread of implementations such as Cloudflare, Google, and Cisco which provides the awareness about the security system, meanwhile ongoing research investigates side-channel resistance, optimization of hardware, and IoT resource adaptation settings.

Modern research examines about obstacles facing while implementation that includes extensive key selection, size of the cipher text ,elasticity against side-channel attacks, and acceleration of hardware , while also exploring compression methodologies, enhancements in modular arithmetic, and "lightweight" alternatives for embedded applications. Predictions on practical research finds that integration in interdisciplinary along with hybrid quantum protocols, quantum key distribution (QKD), and secure multi-party computation (MPC) providing robustness in future ecosystems.

The literature survey shows that there is a prominent shift from assesment of theoretical vulnerability to standardized solutions in practical side.To safeguard the information security in the era of quantum, there is a real world migration

3. Impact of Quantum Computing on Conventional Cryptographic Schemes

3.1 Shor's Algorithm

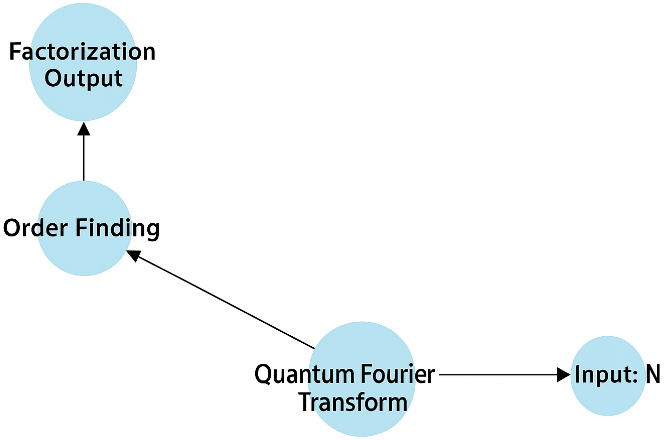

Fig 1. Illustration of How Shor's Algorithm Compromises RSA and ECC

In 1994,Peter Shor's introduces Shor's algorithm that characterize a substantial advancement in the cryptanalysis and quantum computing domain. It factorize the large integers in polynomials time and also compute the discrete logarithms. The basics of the foundation of the algorithm is quantum Fourier transform, which is used to establish the connection to modular exponentiation—plays a vitol role in integer factorization process. Operationally, Shor's algorithm solves the algorithm effectively using quantum principles that becomes a challenge to the classical models.

Random Base Selection: Choose a random integer aaa that is lesser than the number NNN to be factored.

- Period Finding: Use the quantum Fourier transform to find the period rrr of the function f(x)=axmod Nf(x) = a^x \mod Nf(x)=axmodN.
- Classical Post-processing: Given the period rrr, compute the greatest common divisor between ar/2±1a^{r/2} \pm 1ar/2±1 and NNN to obtain nontrivial factors of NNN. The utilization of quantum parallelism allows the period to be uncovered exponentially faster than with any known classical algorithm, resulting in an overall runtime that is polynomial in the number of digits of the number being factored (O((log⁡N)3)O((\log N)^3)O((logN)3)).

In terms of cryptographic impact, Shor's algorithm directly undermines the security of schemes dependent on the hardness of factoring or discrete logarithms. The security assumptions of RSA, ECC, and most Diffie–Hellman schemes are rendered obsolete in the presence of scalable quantum computers, as these systems can be "broken" within hours or days, as opposed to the billions of years required classically. Figure 1 in your work illustrates how Shor's algorithm breaks RSA/ECC by reducing the factoring problem to polynomial time, emphasizing the necessity for post-quantum cryptographic alternatives.modified.docx

The practical realization of Shor's algorithm is contingent on the development of large, fault-tolerant quantum computers, with current prototypes demonstrating small-scale factorizations but advancing rapidly. Post-quantum cryptography standardization protects from Shor's algorithm threat and driving us to towards the quantum safe infrastructures.

3.2 Grover's Algorithm

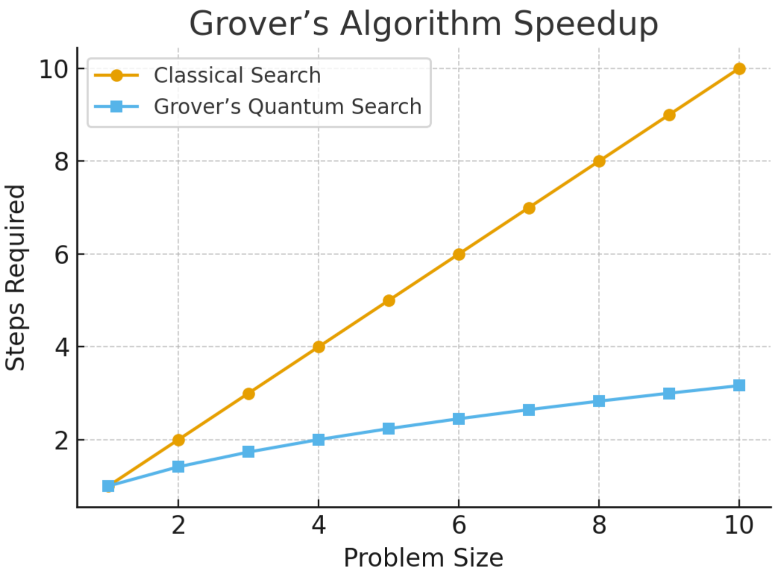

Fig 2: Grover's algorithm search speedup visualization

A spotlight comes in quantum computing when Lov Grover Grover's algorithm introduces quadratic speed for unstructured search problems in 1996.Reducing the complexity of exhaustive key search reduces from O(N) to O(√N),where N is the size of keyspace that shows an important impact on cryptographic hash function.Shor's algorithm shows threat to public key cryptosystem. In order to improve search performance, Grover's algorithm essentially depends on the concepts of superposition and interference. It uses a quantum oracle and a series of unitary operations known as "Grover iterations" to repeatedly increase the probability amplitude of marked (or "solution") states within an unsorted database. This procedure guarantees that a measurement will yield the solution with high probability after approximately π/4√N iterations.By reducing the number of searches to 256 bit for symmetric cipher algorithm like AES done by Grover's algorithm

Symmetric cryptography is purposeful, but not threatened by the quadratic speedup terribly.

- **Key Length Doubling**: Because Grover's algorithm effectively halves the strength of a key, modern guidance is to double symmetric key sizes for quantum-resistant security.

To maintain an equivalent security margin against quantum adversaries, AES must switch from AES-128 to AES-256.

- Hash Function Impact: Collision resistance is reduced for the hash functions such as SHA-2,SHA-3 in a quantum environment and also demanding the larger output size inorder to maintain the preimage resistance.
  Even though Grover's algorithm does not break the symmetric algorithm just like what Shor's algorithm did for RSA and ECC ,Grover's algorithm has an important effects on designing the system,selection of cryptographic protocols and long-term security planning . Table 1 and Grover speedup figure shows the importance of using quantum based parameters for encryption and authentication process.
- Research on quantum oracle models, bounded-error quantum search, and new attack vectors on symmetric primitives continues to build on Grover's method, which is guiding the development of quantum-resilient cryptography techniques.

3.3 Quantum Oracle Models

By providing quantum access to encryption and decryption oracles, quantum oracle models extend attack scenarios. The security presumptions of MAC and traditional authenticated encryption are called into question by this framework. These models are used by researchers to assess the resilience of PQC protocols against adversaries based on superposition.

4. Vulnerable Cryptosystems

Table 1: Vulnerable classical cryptosystems vs quantum attacks

Cryptosystem	Quantum Threat	Status
RSA	Shor's Algorithm	Broken
ECC	Shor's Algorithm	Broken
AES	Grover's Algorithm	Reduced security
SHA-2	Grover's Algorithm	Reduced security

The susceptibility of classical cryptosystems to known quantum attacks is summed up in the table above.While symmetric algorithms like AES and hash functions like SHA-2 have shorter effective key lengths, Shor's algorithm completely breaks RSA and ECC. It is therefore essential to switch to quantum-resistant primitives.

5. Post-Quantum Cryptographic Approaches

5.1 Lattice-Based Cryptography

Because lattice-based cryptography strikes a balance between security, efficiency, and mathematical hardness, it serves as the foundation for PQC research. Strong resistance to quantum attacks is provided by schemes based on the Learning with Errors (LWE) and Ring-LWE problems, such as CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (signatures), which have been chosen for NIST standardization in 2022. Additionally, lattice structures offer flexibility for sophisticated applications such as zero-knowledge proofs and homomorphic encryption.

Citation: Shree, R.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). Quantum Cryptanalysis: A Survey of Threats and Post-Quantum Countermeasures. *International Insurance Law Review*, 34 (S1), 309-318.

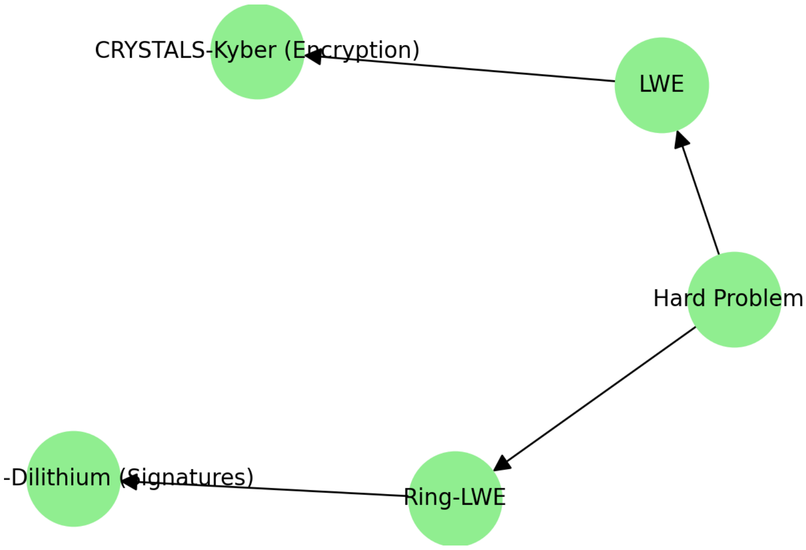

Fig 3: Structure of lattice-based cryptography (LWE, Ring-LWE)

5.2 Code-Based Cryptography

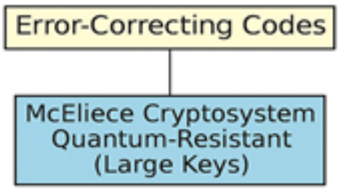

Fig 4:Code-based encryption concept

The decoding problem of random linear codes, which quantum algorithms have not yet substantially accelerated, is the source of code-based cryptography's security. The McEliece and BIKE cryptosystems are the best examples of this family. Their quantum robustness and decades-long security record make them useful for specialized applications like secure email and VPNs, despite their large key sizes.

5.3 Multivariate Polynomial Cryptography

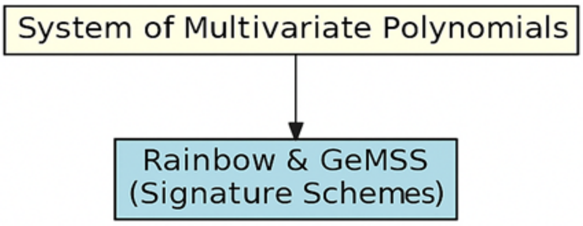

Fig 5: Polynomial-based signature scheme concept

Multivariate polynomial cryptography uses NP-hard multivariate quadratic equations over finite fields.Even though cryptanalytic uses some weak parameter set,digital authentication uses signature schemes like Rainbow and GeMSS . The objective of the current research is to maintaian the quantum resistance the key sizes are reduced,so that signing efficiency has been improved.

5.4 Hash-Based Signatures

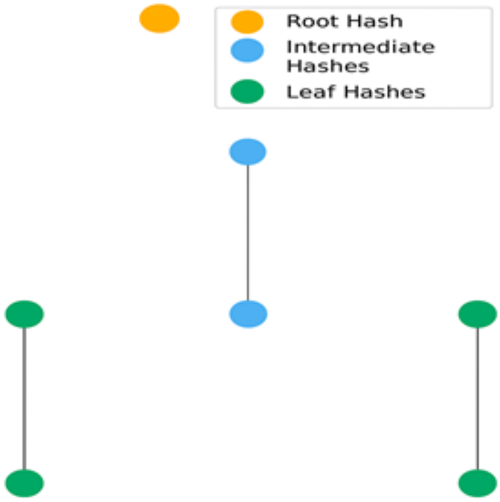

Fig 6: Hash-based signature tree (SPHINCS+)]

Quantum attacks are resistant to hash-based signatures that use only cryptographic hash functions. Because of their provable security and ease of implementation, stateless schemes like SPHINCS+ are preferred for standardization.

They are especially useful for long-term archival integrity and firmware authentication.

6. Standardization and Implementations

The NIST Post-Quantum Cryptography Standardization Project has played a pivotal role in global PQC adoption. In July 2022, the following algorithms were selected for standardization:
-Encryption/KEM: CRYSTALS-Kyber
-Signatures: CRYSTALS-Dilithium, Falcon, SPHINCS+
The project's 2024–2025 phases continue to evaluate additional candidates such as Classic McEliece and Saber. International agencies, including ETSI and ISO, have also aligned their frameworks for interoperability.

6.1 Hybrid Schemes

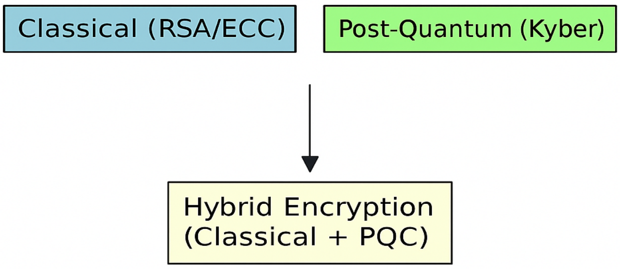

Fig 7: Classical + PQC hybrid encryption model

Hybrid encryption blends post-quantum and classical algorithms to provide transitional security. For instance, RSA paired with Kyber or ECC paired with Dilithium guarantee compatibility while maintaining the longevity of data exchange. Well-known firms like Cloudflare, Google, and Cisco are looking into hybrid TLS handshakes to gradually implement post-quantum cryptography (PQC).

6.2 Implementation Challenges

Despite encouraging advancements, side-channel attack resistance, large key and ciphertext dimensions, and hardware optimization problems make post-quantum cryptography difficult to implement. Effective implementations are necessary in resource-constrained environments, such as the Internet of Things. Lattice compression, modular arithmetic acceleration, and lightweight variants are still undergoing extensive research.

7. Quantum Readiness and Adoption

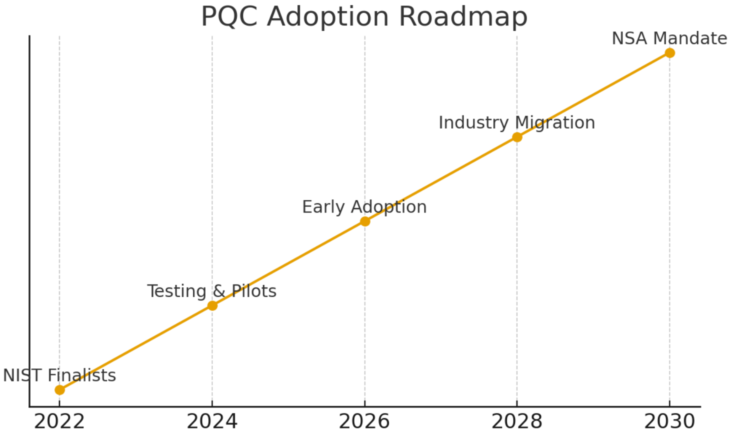

Fig 8: PQC adoption roadmap timeline

Quantum-safe security is no longer just a theoretical concern—it's quickly becoming a practical priority for governments and large organizations around the world. With powerful quantum computers on the horizon, programs like the EU's Post-Quantum Cryptography (PQC) Migration Plan and the NSA's CNSA 2.0 are pushing organizations to transition by 2030.

Many are already taking steps in the right direction. We're seeing post-quantum algorithms being rolled out in everyday technologies such as TLS 1.3, VPNs, and even blockchain platforms, showing that the technology is maturing and ready for real-world use.

That said, technology alone isn't enough. To make this transition truly successful, the global community still needs to align on standards, build trusted certification frameworks, and develop key management systems that can scale across industries and borders. In short, the tools are emerging—but collaboration and coordination will be what ultimately make quantum-resistant security a reality.

8. Future Outlook and Research Directions

By reducing the key size, improving the speed of an algorithm and integrating these features as an hardware make the system to run soomthly is the main focus of the, post-quantum cryptography research to make more practical and easier to implement. Rather than improving the individual algorithms, the researchers showing their interest in constructing the complete post-quantum security ecosystems. Researchers combining secure multi-party computation, quantum key distribution, and hybrid cryptography to get the optimized solution.

Achieving the security and win the race won't be a task of single field. Its the combined journey between engineers who constructs the systems, mathematicians who design the algorithms, and

Citation: Shree, R.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). Quantum Cryptanalysis: A Survey of Threats and Post-Quantum Countermeasures. *International Insurance Law Review*, 34 (S1), 309-318.

physicists who understand the quantum world itself. Only by working together by researchers in various fields can build a stromg defense against security attacks.

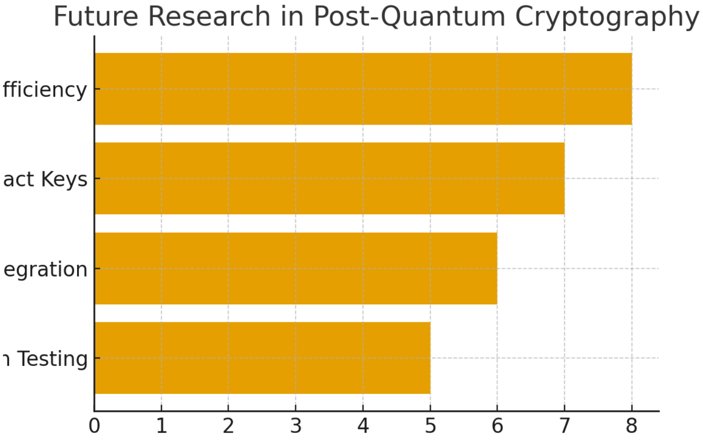

Fig 9: Research directions in post-quantum cryptography

9. Conclusion

Quantum computing breaks the myth with traditional cryptography techniques that remodel the digital security. This paper suggest that there should be a terrific shift from traditional methods to quantum world so that we can protect our data in a better way. The simultaneous growth of both Quantum threats and post quantum alternatives shows how important it is to transfer to quantum world. The emergence of NIST post-quantum cryptography standardization shows the sparkling wave in innovation and collaboration for both industry and academia .

The upcoming era will be a challenging one. The transition from traditional methods to quantum world requires major upgradation in the existing digital world and there is a need of strong certification and key management services. Current research focus mainly on deploying the real-world problems along with making the algorithms more scalable and reliable. Such focus build a strong layered security approaches that can be adopted over time.

A close integration across various disciplines such as from mathematics and physics to engineering and public policy is mandatory to protect the user data. Staying along with the ongoing quantum threats is not just a technical issue but it is a collective responsibility of the researchers. The society can ensure a secure digital future by determiningly work on the features such as without compromising the trust, privacy, and integrity of global information systems by transforming into the quantum computing world.

References

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM Journal on Computing, 26(5), 1484–1509.*

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search*. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), 212–219.*

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography*. Springer, Berlin, Heidelberg.*

Citation: Shree, R.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). Quantum Cryptanalysis: A Survey of Threats and Post-Quantum Countermeasures. *International Insurance Law Review*, 34 (S1), 309-318.

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography*. NISTIR 8105, National Institute of Standards and Technology.*

NIST. (2017). Post-Quantum Cryptography Standardization Program*. National Institute of Standards and Technology.*

Alagic, G., Alperin-Sheriff, J., Apon, D., et al. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process*. NISTIR 8413.*

Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., & Stehlé, D. (2018). CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM*. IEEE European Symposium on Security and Privacy.*

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS–Dilithium: Digital signatures from module lattices*. IEEE European Symposium on Security and Privacy.*

Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., & Schwabe, P. (2019). SPHINCS+: Submission to the NIST post-quantum project*. Cryptology ePrint Archive.*

McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory*. DSN Progress Report, Jet Propulsion Laboratory.*

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange*. ACM CCS.*

Langley, A., Hamburg, M., & Turner, S. (2016). Hybrid key exchange in TLS 1.3*. Internet Engineering Task Force (IETF), Internet-Draft.*

Perrin, T., & Gillmor, D. (2018). Introducing post-quantum cryptography in TLS with Kyber*. Cloudflare Blog.*

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16(5), 38–41.*

ETSI. (2020). Quantum-safe cryptography and security: An introduction, benefits, enablers and challenges*. ETSI White Paper No. 8.*