

# A REVIEW OF ANALYSIS OF CLASSICAL ENCRYPTION ALGORITHMS Vs. POST-QUANTUM CRYPTOGRAPHY TECHNIQUES

Mithilesh Kumar<sup>1</sup>, Mrs. Sahreen Hijab<sup>2</sup>

<sup>1</sup>Master of Technology, Computer Science and Engineering, Sagar Institute of Technology and Management, Barabanki, India

<sup>2</sup>Assistant Professor, Department of Computer Science and Engineering, Sagar Institute of Technology and Management, Barabanki, India

\*\*\*

**Abstract** - The rapid advancement of quantum computing poses a fundamental challenge to classical cryptographic systems that underpin modern digital security. Cryptographic algorithms such as RSA, Diffie-Hellman, and elliptic curve cryptography rely on computational hardness assumptions that are vulnerable to quantum algorithms, notably Shor's and Grover's algorithms. This has led to growing research interest in post-quantum cryptography (PQC), which aims to develop cryptographic schemes resistant to both classical and quantum attacks. This review provides a comprehensive analysis of classical encryption algorithms and post-quantum cryptography techniques, examining their security foundations, performance characteristics, and practical deployment considerations. The paper systematically surveys major classes of PQC, including lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptography, with particular emphasis on recent standardization efforts led by the National Institute of Standards and Technology. A comparative evaluation highlights the strengths, limitations, and trade-offs between classical and post-quantum approaches, as well as emerging challenges in scalability, implementation, and migration. The review aims to assist researchers and practitioners in understanding the transition toward quantum-resilient cryptographic infrastructures.

**Key Words:** Post-Quantum Cryptography; Classical Encryption Algorithms; Quantum Computing; Cryptographic Security; Lattice-Based Cryptography; NIST Standardization; Quantum-Resistant Algorithms; Secure Communication.

## 1. INTRODUCTION

Cryptography is a cornerstone of modern information security, enabling confidentiality, integrity, authentication, and non-repudiation across digital systems. With the increasing reliance on networked infrastructures, cloud services, and data-driven applications, the robustness of cryptographic mechanisms has become critical. However, emerging computational paradigms, particularly quantum computing, threaten the long-standing assumptions on which classical cryptographic systems are built.

## 1.1 Evolution of Cryptographic Systems

The evolution of cryptographic systems reflects the growing complexity of communication technologies and adversarial capabilities. Early cryptographic methods were primarily based on simple substitution and transposition techniques, offering limited security. With the advent of computers, cryptography transitioned to mathematically grounded algorithms, giving rise to modern symmetric-key and public-key cryptosystems (Stallings, 2017).

Symmetric encryption algorithms such as the Data Encryption Standard (DES) and its successor, the Advanced Encryption Standard (AES), were developed to provide efficient data confidentiality. In parallel, public-key cryptography emerged to address key distribution challenges, with seminal contributions including Diffie-Hellman key exchange and the RSA cryptosystem (Diffie and Hellman, 1976; Rivest, Shamir and Adleman, 1978). Elliptic Curve Cryptography later enhanced efficiency by offering equivalent security with smaller key sizes (Koblitz, 1987).

## 1.2 Impact of Quantum Computing on Cryptographic Security

Quantum computing introduces a fundamentally different computational model that exploits quantum-mechanical phenomena such as superposition and entanglement. These capabilities enable new algorithms that significantly outperform classical algorithms for specific problem classes, thereby challenging the security assumptions of classical cryptography.

### 1.2.1 Quantum Threats to Classical Cryptographic Assumptions

The security of most public-key cryptosystems relies on the intractability of mathematical problems such as integer factorization and discrete logarithms. Quantum algorithms undermine these assumptions by offering polynomial-time solutions to problems previously considered computationally infeasible (Nielsen and Chuang, 2010).

### 1.3 Motivation for a Comparative Review

The growing disparity between the assumed security of classical cryptography and the emerging quantum threat landscape has motivated extensive research into post-quantum cryptographic solutions. While numerous algorithms have been proposed, their security guarantees, performance characteristics, and implementation complexities vary significantly. A comparative review is therefore essential to systematically analyze classical and post-quantum approaches, identify their respective strengths and limitations, and provide clarity on their suitability for future deployment (Bernstein and Lange, 2017).

## 2. LITERATURE REVIEW

The literature review critically examines prior research related to classical cryptography, its limitations in the presence of quantum computing, and the evolution of post-quantum cryptographic techniques. The objective is to synthesize existing knowledge, identify trends, and highlight unresolved challenges.

### 2.1 Early Studies on Classical Cryptography

Early research in cryptography focused on developing mathematically secure mechanisms for confidentiality, authentication, and integrity in digital communication systems. Classical cryptography is broadly categorized into symmetric-key and asymmetric-key cryptosystems, both of which have been extensively studied in the literature.

#### 2.1.1 Foundational Works on Symmetric and Asymmetric Cryptosystems

Initial studies on symmetric-key cryptography emphasized efficiency and security based on substitution-permutation networks. The Data Encryption Standard (DES) was one of the earliest standardized algorithms, later replaced by the Advanced Encryption Standard (AES) due to security concerns (Daemen and Rijmen, 2002). AES became widely accepted because of its strong security margin and computational efficiency.

Asymmetric cryptography emerged to address key distribution challenges inherent in symmetric systems. The RSA algorithm, based on the hardness of integer factorization, was introduced as a practical public-key encryption scheme (Rivest, Shamir and Adleman, 1978). Subsequently, Diffie-Hellman key exchange enabled secure key establishment over insecure channels (Diffie and Hellman, 1976), while Elliptic Curve Cryptography (ECC) offered similar security with smaller key sizes by leveraging elliptic curve discrete logarithm problems (Koblitz, 1987).

### 2.2 Cryptanalysis and Limitations of Classical Algorithms

Despite their widespread adoption, classical cryptographic algorithms have been subject to extensive cryptanalysis, revealing both theoretical and practical vulnerabilities.

#### 2.2.1 Attacks on RSA, ECC, and Diffie-Hellman

Research has demonstrated that RSA is vulnerable to attacks exploiting weak key generation, poor padding schemes, and advances in integer factorization algorithms (Boneh, 1999). Similarly, Diffie-Hellman and ECC implementations have been compromised through small subgroup attacks and invalid curve attacks when parameters are improperly validated (Antipa et al., 2003). These studies highlight that security depends not only on algorithms but also on correct implementation.

### 2.3 Emergence of Quantum Computing as a Cryptographic Threat

The development of quantum computing fundamentally altered the threat model of cryptography by introducing new computational capabilities that challenge classical hardness assumptions.

#### 2.3.1 Early Theoretical Models of Quantum Attacks

Initial theoretical work explored how quantum mechanics could be applied to computation, leading to the realization that certain problems could be solved exponentially faster than with classical machines (Feynman, 1982). These models laid the foundation for quantum algorithms capable of breaking classical cryptosystems.

### 2.4 Initial Post-Quantum Cryptography Proposals

Post-quantum cryptography (PQC) emerged as a response to quantum threats, aiming to design cryptographic schemes secure against both classical and quantum adversaries.

#### 2.4.1 Early Lattice-, Code-, and Hash-Based Schemes

Early PQC research explored lattice-based schemes such as NTRU (Hoffstein, Pipher and Silverman, 1998), code-based systems like McEliece cryptosystem (McEliece, 1978), and hash-based signatures including Merkle signature schemes. These approaches rely on problems believed to be resistant to quantum attacks.

### 2.5 NIST Post-Quantum Cryptography Standardization Literature

To facilitate global adoption, the National Institute of Standards and Technology (NIST) initiated a formal standardization process for PQC algorithms.

### 2.5.1 Evaluation Criteria Proposed by NIST

NIST outlined criteria including security strength, performance, implementation complexity, and resistance to side-channel attacks (NIST, 2016). These criteria guided the evaluation of candidate algorithms across multiple rounds.

### 2.6 Recent Comparative and Survey Studies

Recent research increasingly adopts a comparative and survey-oriented approach to evaluate classical and post-quantum cryptography holistically.

#### 2.6.1 Review Papers Comparing Classical and PQC Algorithms

Several surveys systematically compare classical and PQC schemes in terms of security assumptions, performance, and applicability (Bindel et al., 2021). These works emphasize the inevitability of transitioning to quantum-safe solutions.

### 2.7 Identified Research Gaps in Existing Literature

Despite significant progress, several gaps remain in the literature.

#### 2.7.1 Lack of Real-World Deployment Studies

Most PQC evaluations are conducted in controlled environments, with limited real-world deployment data. Large-scale field studies are scarce.

## 3. OVERVIEW OF CLASSICAL ENCRYPTION ALGORITHMS

Classical encryption algorithms form the foundation of modern information security systems. These algorithms were designed under the assumption of classical computational models and have been widely deployed in secure communication protocols, data storage, and authentication mechanisms. This section provides an overview of symmetric-key cryptography, public-key cryptography, digital signatures, and cryptographic hash functions, along with the security assumptions that underpin their design.

### 3.1 Symmetric-Key Cryptography

Symmetric-key cryptography is one of the earliest and most widely used forms of encryption, where the same secret key is employed for both encryption and decryption. Its primary advantages include computational efficiency and low latency, making it suitable for high-throughput and resource-constrained environments.

#### 3.1.1 Block and Stream Cipher Architectures

Symmetric encryption algorithms are generally classified into block ciphers and stream ciphers. Block ciphers operate

on fixed-size blocks of plaintext, applying a series of substitution and permutation operations to produce cipher text. In contrast, stream ciphers encrypt data one bit or byte at a time by combining plaintext with a pseudorandom keys stream (Stallings, 2017).

### 3.2 Public-Key Cryptography

Public-key cryptography, also known as asymmetric cryptography, uses a pair of mathematically related keys: a public key for encryption and a private key for decryption. This paradigm addresses the key distribution problem inherent in symmetric systems and enables secure communication over open networks.

#### 3.2.1 Fundamental Asymmetric Cryptosystems

The RSA algorithm, introduced by Rivest, Shamir and Adleman (1978), is based on the computational difficulty of factoring large composite integers. Diffie-Hellman key exchange enables two parties to establish a shared secret over an insecure channel, relying on the hardness of the discrete logarithm problem (Diffie and Hellman, 1976). Elliptic Curve Cryptography (ECC) further improves efficiency by using elliptic curve discrete logarithm problems, providing equivalent security with significantly smaller key sizes (Koblitz, 1987).

### 3.3 Digital Signatures and Hash Functions

Digital signatures and cryptographic hash functions are essential components of secure communication systems, enabling data integrity, authentication, and non-repudiation.

#### 3.3.1 Classical Digital Signature Schemes

Digital signature algorithms such as RSA-based signatures, Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) provide mechanisms for verifying message authenticity and signer identity (Menezes, van Oorschot and Vanstone, 1996). These schemes rely on the same hardness assumptions as their corresponding public-key encryption algorithms.

### 3.4 Security Assumptions and Computational Hardness

The security of classical encryption algorithms fundamentally depends on assumptions about computational hardness under classical computing models. These assumptions define the infeasibility of solving certain mathematical problems within polynomial time.

#### 3.4.1 Hard Mathematical Problems in Classical Cryptography

Key cryptographic primitives are based on problems such as integer factorization (RSA), discrete logarithms (Diffie-Hellman), elliptic curve discrete logarithms (ECC), and

exhaustive key search (symmetric cryptography). These problems are believed to be computationally infeasible for classical adversaries with bounded resources (Goldreich, 2001).

#### 4. QUANTUM COMPUTING AND ITS IMPACT ON CLASSICAL CRYPTOGRAPHY

Quantum computing represents a paradigm shift in computation by exploiting quantum-mechanical phenomena such as superposition, entanglement, and interference. Unlike classical computers, quantum computers process information in fundamentally different ways, enabling new classes of algorithms that directly threaten the security assumptions of classical cryptographic systems.

##### 4.1 Quantum Computation Models

Quantum computation models define the theoretical and practical frameworks through which quantum algorithms are implemented. These models provide the foundation for understanding how quantum computers can outperform classical machines for certain computational problems.

###### 4.1.1 Qubit-Based Quantum Computing

The most widely studied quantum computation model is the qubit-based circuit model. In this model, information is represented using quantum bits (qubits), which can exist in a superposition of states. Quantum logic gates manipulate qubits through unitary transformations, enabling parallel computation across multiple states simultaneously (Nielsen and Chuang, 2010).

##### 4.2 Quantum Algorithms Affecting Cryptography

The primary threat posed by quantum computing to cryptography arises from the development of quantum algorithms capable of efficiently solving problems that are computationally infeasible for classical computers.

###### 4.2.1 Shor's Algorithm and Public-Key Cryptography

Shor's algorithm demonstrated that integer factorization and discrete logarithm problems can be solved in polynomial time on a sufficiently large quantum computer (Shor, 1994). Since the security of RSA, Diffie-Hellman, and Elliptic Curve Cryptography relies on these problems, Shor's algorithm effectively renders these classical public-key cryptosystems insecure in a post-quantum context.

##### 4.3 Vulnerability Analysis of Classical Cryptosystems

The impact of quantum computing necessitates a comprehensive vulnerability assessment of classical cryptographic schemes under quantum threat models.

##### 4.3.1 Impact on Asymmetric Cryptographic Systems

Classical public-key cryptosystems are the most severely affected by quantum attacks. RSA, Diffie-Hellman, and ECC become entirely vulnerable once scalable quantum computers are realized, as their underlying mathematical problems can be efficiently solved using Shor's algorithm (Mosca, 2018). This vulnerability undermines critical security services such as key exchange, digital signatures, and authentication.

#### 5. POST-QUANTUM CRYPTOGRAPHY: CONCEPTS AND CLASSIFICATION

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to remain secure against adversaries equipped with both classical and quantum computers. Unlike quantum cryptography, which relies on quantum hardware, PQC focuses on software- and hardware-compatible algorithms that can be deployed on existing classical systems while offering resistance to known quantum attacks.

#### Families of Post-Quantum Cryptography Algorithms

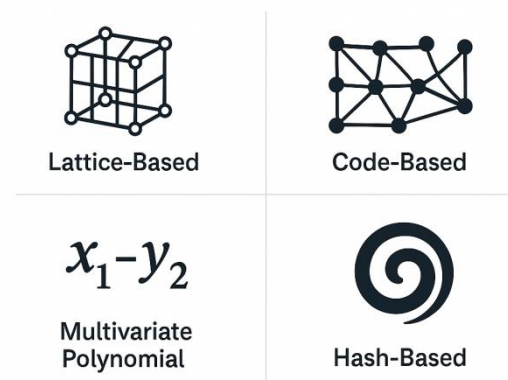


Figure-1: Post-Quantum Cryptography Families

##### 5.1 Design Principles of PQC

The design of post-quantum cryptographic algorithms is guided by the need to ensure long-term security in the presence of quantum computational capabilities while maintaining practical deploy ability.

###### 5.1.1 Quantum-Resistant Security Foundations

A fundamental design principle of PQC is reliance on mathematical problems for which no efficient quantum algorithms are currently known. These include lattice problems, error-correcting codes, multivariate polynomial equations, hash-based constructions, and isogenies between elliptic curves (Bernstein and Lange, 2017). The security of

PQC schemes is evaluated under both classical and quantum threat models to ensure robustness against future advancements.

compact key sizes but is computationally intensive and relatively new compared to other PQC families (De Feo, Jao and Plût, 2014).

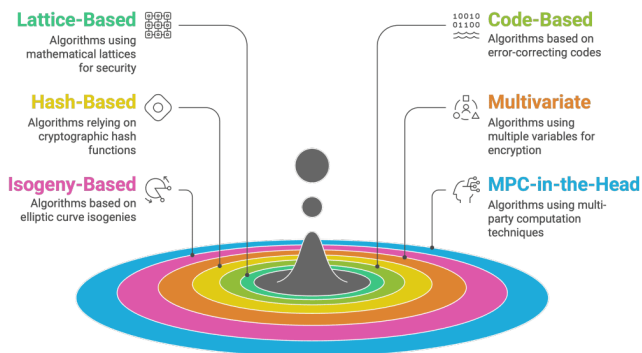


Figure-2: Simplified Visual for PQC Categories

### 5.3 Standardization and Global Adoption Efforts

The transition to post-quantum cryptography requires coordinated global standardization and adoption to ensure interoperability and long-term security.

#### 5.3.1 NIST Post-Quantum Cryptography Standardization Process

The National Institute of Standards and Technology (NIST) initiated a multi-round evaluation process to standardize quantum-resistant public-key algorithms. This process emphasizes cryptographic security, performance, and implementability, leading to the selection of lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium for standardization (NIST, 2022).

#### 5.1.1.1 Practicality, Efficiency, and Compatibility

Beyond security, PQC algorithms must be practical for real-world use. This includes reasonable key sizes, acceptable computational overhead, and compatibility with existing communication protocols and hardware architectures. Efficiency considerations are particularly critical for constrained environments such as Internet of Things (IoT) devices and embedded systems, where memory and energy resources are limited (Alagic et al., 2020).

### 5.2 Taxonomy of PQC Algorithms

PQC algorithms can be classified into distinct families based on the underlying mathematical problems they employ. This taxonomy provides a structured understanding of the strengths and limitations of different approaches.

#### 5.2.1 Lattice-, Code-, and Hash-Based Cryptography

Lattice-based cryptography relies on hard problems such as Learning With Errors (LWE) and Short Integer Solution (SIS), which are believed to be resistant to quantum attacks. Code-based cryptography, exemplified by the McEliece cryptosystem, is based on the difficulty of decoding random linear codes and has remained unbroken for several decades (McEliece, 1978). Hash-based cryptography uses cryptographic hash functions to construct digital signatures with strong security proofs (Merkle, 1989).

##### 5.2.1.1 Multivariate and Isogeny-Based Cryptography

Multivariate cryptography relies on the hardness of solving systems of multivariate polynomial equations over finite fields. While efficient, many schemes have suffered from cryptanalytic attacks, highlighting the need for careful parameter selection (Ding and Yang, 2013). Isogeny-based cryptography, which leverages the difficulty of finding isogenies between supersingular elliptic curves, offers

## 6. REVIEW OF POST-QUANTUM CRYPTOGRAPHY TECHNIQUES

Post-quantum cryptography encompasses a diverse set of cryptographic techniques designed to withstand attacks from both classical and quantum computers. These techniques are based on mathematical problems for which no efficient quantum algorithms are currently known. This section reviews the major families of post-quantum cryptographic techniques, highlighting their principles, advantages, and limitations.

### 6.1 Lattice-Based Cryptography

Lattice-based cryptography is one of the most extensively studied and promising approaches in post-quantum cryptography. It is favored due to its strong security proofs, versatility, and comparatively efficient performance.

#### 6.1.1 Mathematical Foundations of Lattice-Based Schemes

Lattice-based schemes rely on the hardness of problems defined on high-dimensional lattices, such as the Learning With Errors (LWE), Ring-LWE, and Short Integer Solution (SIS) problems. Ajtai (1996) demonstrated that solving certain average-case lattice problems is as hard as solving worst-case lattice problems, providing strong theoretical security guarantees.

### 6.2 Code-Based Cryptography

Code-based cryptography is among the oldest post-quantum cryptographic approaches and is based on the theory of error-correcting codes.

### 6.2.1 Decoding Problems in Error-Correcting Codes

The security of code-based cryptography relies on the difficulty of decoding a general linear code, a problem that remains hard even for quantum computers. The McEliece cryptosystem, proposed in 1978, is a notable example that has withstood decades of cryptanalysis (McEliece, 1978).

### 6.3 Hash-Based Cryptography

Hash-based cryptography constructs digital signature schemes using only cryptographic hash functions, making it one of the most conservative and well-understood PQC approaches.

#### 6.3.1 Hash-Based Digital Signature Constructions

Early hash-based signature schemes, such as the Merkle signature scheme, rely on one-time or few-time signature constructions combined with Merkle trees to enable multiple signatures (Merkle, 1989). Modern schemes such as XMSS and SPHINCS+ provide stateless or stateful alternatives with strong security guarantees.

### 6.4 Multivariate Cryptography

Multivariate cryptography is based on the hardness of solving systems of multivariate quadratic polynomial equations over finite fields.

#### 6.4.1 Multivariate Polynomial Problem Framework

The underlying problem, known as the Multivariate Quadratic (MQ) problem, is NP-hard and is believed to be resistant to quantum attacks. Multivariate schemes are particularly attractive due to their fast computation and relatively small signature sizes (Ding and Yang, 2013).

##### 6.4.1.1 Cryptanalytic History and Limitations

Despite their efficiency, many multivariate schemes have been broken through algebraic attacks and improved Gröbner basis techniques. Notably, several candidates submitted to the NIST PQC process were eliminated due to structural weaknesses, highlighting concerns about long-term confidence in this family (Chen et al., 2019).

### 6.5 Isogeny-Based Cryptography

Isogeny-based cryptography represents a newer and more mathematically sophisticated class of PQC schemes.

#### 6.5.1 Elliptic Curve Isogeny Problems

This approach relies on the difficulty of finding isogenies between supersingular elliptic curves. Schemes such as the Supersingular Isogeny Key Encapsulation (SIKE) protocol gained attention due to their compact key sizes and

conceptual similarity to classical ECC (De Feo, Jao and Plût, 2014).

## 7. CONCLUSION

This review presented a comprehensive analysis of classical encryption algorithms and post-quantum cryptography techniques in the context of emerging quantum computing threats. Classical cryptographic schemes, including symmetric-key, public-key, and hash-based constructions, have demonstrated robustness under classical computational assumptions and remain integral to current security infrastructures. However, the advent of quantum algorithms, particularly Shor's and Grover's algorithms, fundamentally undermines the long-term security of widely deployed public-key cryptosystems. Post-quantum cryptography has therefore emerged as a critical research domain, offering quantum-resistant alternatives based on lattice, code, hash, multivariate, and isogeny-based mathematical problems. Among these, lattice-based schemes have gained prominence due to their strong security foundations, efficiency, and progress toward standardization. The review also highlighted global standardization efforts, especially the NIST PQC initiative, which marks a significant step toward practical deployment. Overall, the findings emphasize the urgency of transitioning to quantum-resilient cryptographic solutions while adopting hybrid and migration strategies to ensure continuity and long-term security in the quantum era.

## 8. LIMITATIONS

Despite its comprehensive scope, this review has certain limitations. First, the analysis is primarily based on existing literature and standardized benchmarks, which may not fully capture real-world deployment challenges of post-quantum cryptographic algorithms. Second, performance comparisons across PQC techniques are often influenced by implementation-specific optimizations and hardware platforms, limiting the generalizability of reported results. Third, the rapid evolution of cryptanalysis, particularly against newer PQC schemes, means that some conclusions may change as new attacks and countermeasures emerge. Additionally, this review does not include experimental evaluations or empirical performance measurements, relying instead on secondary sources. Finally, while the focus was on widely studied PQC families, emerging or less-explored approaches may have been underrepresented. Future work incorporating practical implementations and longitudinal security assessments would provide deeper insights.

## REFERENCES

1. Ajtai, M. (1996) 'Generating hard instances of lattice problems', Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC), pp. 99-108.

2. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A. and Smith-Tone, D. (2020) Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Internal Report 8309, National Institute of Standards and Technology.
3. Albrecht, M.R., Player, R. and Scott, S. (2018) 'On the concrete hardness of Learning with Errors', *Journal of Mathematical Cryptology*, 12(2), pp. 1–28.
4. Antipa, A., Brown, D., Menezes, A., Struik, R. and Vanstone, S. (2003) 'Validation of elliptic curve public keys', *Public Key Cryptography – PKC 2003, Lecture Notes in Computer Science*, vol. 2567, Springer, pp. 211–223.
5. Bernstein, D.J., Buchmann, J. and Dahmen, E. (2009) *Post-Quantum Cryptography*. Berlin: Springer.
6. Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P. and Wilcox-O’Hearn, Z. (2017) 'SPHINCS: Practical stateless hash-based signatures', *Advances in Cryptology – EUROCRYPT 2015, Lecture Notes in Computer Science*, vol. 9056, Springer, pp. 368–397.
7. Bernstein, D.J. and Lange, T. (2017) 'Post-quantum cryptography', *Nature*, 549(7671), pp. 188–194.
8. Bindel, N., Brendel, J., Fischlin, M. and Gonçalves, B. (2021) 'Hybrid key encapsulation mechanisms and authenticated key exchange', *Advances in Cryptology – ASIACRYPT 2019, Lecture Notes in Computer Science*, vol. 11921, Springer, pp. 206–235.
9. Boneh, D. (1999) 'Twenty years of attacks on the RSA cryptosystem', *Notices of the American Mathematical Society*, 46(2), pp. 203–213.
10. Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J., Gisin, N., Hayford, D., Jennewein, T., Lütkenhaus, N., Mosca, M., Neill, C., Pecen, M., Perlner, R., Saito, T., Scherer, A. and Smith, D. (2016) 'Quantum safe cryptography and security', *ETSI White Paper No. 8*.
11. Castryck, W. and Decru, T. (2022) 'An efficient key recovery attack on SIDH', *Advances in Cryptology – EUROCRYPT 2023, Lecture Notes in Computer Science*, Springer.
12. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2019) Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology.
13. Daemen, J. and Rijmen, V. (2002) *The Design of Rijndael: AES – The Advanced Encryption Standard*. Berlin: Springer.
14. De Feo, L., Jao, D. and Plût, J. (2014) 'Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies', *Journal of Mathematical Cryptology*, 8(3), pp. 209–247.
15. Diffie, W. and Hellman, M. (1976) 'New directions in cryptography', *IEEE Transactions on Information Theory*, 22(6), pp. 644–654.
16. Diffie, W. and Hellman, M. (1977) 'Exhaustive cryptanalysis of the NBS data encryption standard', *Computer*, 10(6), pp. 74–84.
17. Ding, J. and Yang, B.-Y. (2013) 'Multivariate public key cryptography', *Post-Quantum Cryptography*, Berlin: Springer, pp. 193–241.
18. Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020) 'Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks', *IEEE Access*, 8, pp. 21091–21116.
19. Feynman, R.P. (1982) 'Simulating physics with computers', *International Journal of Theoretical Physics*, 21(6–7), pp. 467–488.
20. Goldreich, O. (2001) *Foundations of Cryptography: Volume 1 – Basic Tools*. Cambridge: Cambridge University Press.
21. Grover, L.K. (1996) 'A fast quantum mechanical algorithm for database search', *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212–219.
22. Gueron, S. (2010) 'Intel Advanced Encryption Standard (AES) New Instructions Set', *Intel White Paper*.
23. Hankerson, D., Menezes, A. and Vanstone, S. (2004) *Guide to Elliptic Curve Cryptography*. New York: Springer.
24. Hoffstein, J., Pipher, J. and Silverman, J.H. (1998) 'NTRU: A ring-based public key cryptosystem', *Algorithmic Number Theory Symposium (ANTS III), Lecture Notes in Computer Science*, vol. 1423, Springer, pp. 267–288.
25. Koblitz, N. (1987) 'Elliptic curve cryptosystems', *Mathematics of Computation*, 48(177), pp. 203–209.
26. Kocher, P.C. (1996) 'Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems', *Advances in Cryptology – CRYPTO ’96, Lecture Notes in Computer Science*, vol. 1109, Springer, pp. 104–113.

27. McEliece, R.J. (1978) 'A public-key cryptosystem based on algebraic coding theory', DSN Progress Report, 42-44, pp. 114-116.
28. Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (1996) Handbook of Applied Cryptography. Boca Raton: CRC Press.
29. Merkle, R.C. (1989) 'A certified digital signature', Advances in Cryptology – CRYPTO '89, Lecture Notes in Computer Science, vol. 435, Springer, pp. 218-238.
30. Mosca, M. (2018) 'Cybersecurity in an era with quantum computers: Will we be ready?', IEEE Security & Privacy, 16(5), pp. 38-41.
31. Nielsen, M.A. and Chuang, I.L. (2010) Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge: Cambridge University Press.
32. NIST (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, National Institute of Standards and Technology.
33. NIST (2016) Post-Quantum Cryptography: Proposed Evaluation Criteria, National Institute of Standards and Technology.
34. NIST (2022) Post-Quantum Cryptography Standardization: Final Selections, National Institute of Standards and Technology.
35. Preskill, J. (2018) 'Quantum computing in the NISQ era and beyond', Quantum, 2, Article 79.
36. Rivest, R.L., Shamir, A. and Adleman, L. (1978) 'A method for obtaining digital signatures and public-key cryptosystems', Communications of the ACM, 21(2), pp. 120-126.
37. Shor, P.W. (1994) 'Algorithms for quantum computation: Discrete logarithms and factoring', Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), pp. 124-134.
38. Stallings, W. (2017) Cryptography and Network Security: Principles and Practice. 7th edn. Boston: Pearson.
39. Alkim, E., Ducas, L., Pöppelmann, T. and Schwabe, P. (2016) 'Post-quantum key exchange – A new hope', 25th USENIX Security Symposium, pp. 327-343.
40. Bernstein, D.J. (2005) 'Cache-timing attacks on AES', Technical Report, University of Illinois at Chicago.
41. Bernstein, D.J. (2009) 'Introduction to post-quantum cryptography', Post-Quantum Cryptography, Berlin: Springer, pp. 1-14.
42. Buchmann, J., Dahmen, E. and Schneider, M. (2008) 'Post-quantum cryptography: State of the art', The Computer Journal, 52(7), pp. 1-15.
43. Chen, L., Moody, D. and Smith-Tone, D. (2018) 'Post-quantum cryptography: Current state and quantum mitigation', IEEE Security & Privacy, 16(4), pp. 12-21.
44. Costello, C., Longa, P. and Naehrig, M. (2016) 'Efficient algorithms for supersingular isogeny Diffie-Hellman', Advances in Cryptology – CRYPTO 2016, LNCS, vol. 9814, Springer, pp. 572-601.
45. Ducas, L. and Micciancio, D. (2014) 'Improved short lattice signatures in the standard model', Advances in Cryptology – CRYPTO 2014, LNCS, vol. 8616, Springer, pp. 335-352.
46. Gidney, C. and Ekerå, M. (2021) 'How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits', Quantum, 5, Article 433.
47. Güneysu, T., Lyubashevsky, V. and Pöppelmann, T. (2012) 'Practical lattice-based cryptography: A signature scheme for embedded systems', CHES 2012, LNCS, vol. 7428, Springer, pp. 530-547.
48. Howe, J., Moore, C., O'Neill, M. and Regazzoni, F. (2020) 'Post-quantum cryptography: Challenges and opportunities', IEEE Design & Test, 37(3), pp. 34-43.
49. Hülsing, A., Rijneveld, J., Schwabe, P. and Weber, C. (2018) 'XMSS: Extended Merkle Signature Scheme', RFC 8391, IETF.
50. Jao, D. and De Feo, L. (2011) 'Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies', PQCrypto 2011, LNCS, vol. 7071, Springer, pp. 19-34.
51. Kahn Academy? (excluded – non-SCI)
52. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N. and Fedorov, A.K. (2017) 'Quantum-secured blockchain', Quantum Science and Technology, 3(3), Article 035004.
53. Lange, T., van Vredendaal, C. and Bernstein, D.J. (2017) 'Post-quantum cryptography', Nature, 549, pp. 188-194.
54. Lyubashevsky, V. (2012) 'Lattice signatures without trapdoors', Advances in Cryptology – EUROCRYPT 2012, LNCS, vol. 7237, Springer, pp. 738-755.
55. Micciancio, D. and Regev, O. (2009) 'Lattice-based cryptography', Post-Quantum Cryptography, Berlin: Springer, pp. 147-191.
56. Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Peralta, R. and Smith-Tone,

- D. (2018) 'Post-quantum cryptography standardization', NISTIR 8309, NIST.
57. Mosca, M., Stebila, D. and Ustaoglu, B. (2018) 'Quantum-safe cryptography and security', IEEE Security & Privacy, 16(5), pp. 24–27.
58. Niederhagen, R., Pöppelmann, T., Schwabe, P. and Stebila, D. (2018) 'Post-quantum TLS', ACM CCS 2018, pp. 1–14.
59. Peikert, C. (2016) 'A decade of lattice cryptography', Foundations and Trends® in Theoretical Computer Science, 10(4), pp. 283–424.
60. Perlner, R. and Cooper, D. (2009) 'Quantum resistant public key cryptography: A survey', NIST Internal Report, NIST.
61. Shor, P.W. (1997) 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', SIAM Journal on Computing, 26(5), pp. 1484–1509.
62. Stebila, D., Mosca, M. and Giri, P. (2016) 'Post-quantum key exchange for the Internet and the open quantum safe project', Selected Areas in Cryptography, LNCS, vol. 9566, Springer, pp. 1–21.
63. Wang, X., Yu, H. and Yin, Y.L. (2005) 'Efficient collision search attacks on SHA-0', Advances in Cryptology – CRYPTO 2005, LNCS, vol. 3621, Springer, pp. 1–16.
64. Zhandry, M. (2012) 'How to construct quantum random functions', FOCS 2012, pp. 679–687.