

# 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 digital communication systems has significantly increased the reliance on cryptographic mechanisms to ensure data confidentiality, integrity, and secure authentication. Classical cryptographic algorithms, including symmetric and asymmetric techniques such as AES, RSA, and Elliptic Curve Cryptography (ECC), have long served as the foundation of modern security infrastructures. However, the emergence of quantum computing poses a substantial threat to these conventional systems, as quantum algorithms—particularly Shor's and Grover's algorithms—have the potential to compromise their underlying security assumptions. This research presents a comprehensive comparative analysis of classical encryption algorithms and post-quantum cryptographic (PQC) techniques within a quantum-aware threat model. The study adopts a qualitative and analytical research methodology, synthesizing findings from established literature, cryptographic standards, and recent advancements in PQC. Major categories of post-quantum cryptography, including lattice-based, code-based, hash-based, and multivariate schemes, are evaluated against classical approaches using multiple criteria such as security strength, computational complexity, key size, and performance efficiency. The analysis reveals that while classical cryptographic systems remain efficient and widely deployable, they are inherently vulnerable to quantum attacks. In contrast, PQC techniques offer enhanced resistance to quantum threats but introduce challenges related to increased computational overhead and resource requirements. The study highlights hybrid cryptographic approaches as a practical transition strategy and emphasizes the need for standardized benchmarking and optimization for real-world deployment.

**Key Words:** Cryptography, Post-Quantum Cryptography, Quantum Computing, Classical Encryption, Lattice-Based Cryptography, Security Analysis, Hybrid Cryptography

## 1. INTRODUCTION

The field of cryptography plays a pivotal role in securing modern digital infrastructures by ensuring confidentiality, integrity, authentication, and non-repudiation of information. With the exponential growth of interconnected systems, cloud computing, and online services, the demand for robust cryptographic solutions has increased

significantly. However, the emergence of quantum computing introduces new challenges that threaten the foundational assumptions of classical cryptographic algorithms. This section provides an overview of the background, evolution, problem statement, research objectives, and key contributions of the present study.

### 1.1 Background

The increasing dependence on digital communication systems has made cryptography an essential component of cybersecurity frameworks. From online banking and e-commerce to military communications and cloud storage, cryptographic techniques safeguard sensitive information against unauthorized access and cyber threats.

#### 1.1.1 Importance of Cryptography in Digital Systems

Cryptography ensures secure data transmission by converting plaintext into ciphertext using encryption algorithms and cryptographic keys. It supports essential security services such as confidentiality, data integrity, authentication, and non-repudiation, which are fundamental to modern digital ecosystems. The widespread adoption of protocols such as TLS, VPNs, and secure email systems demonstrates the critical role of cryptographic mechanisms in protecting digital communications (Stallings, 2017).

#### 1.1.2 Growth of Secure Communication Systems

The rapid expansion of internet-based applications and distributed systems has significantly increased the need for secure communication channels. Emerging technologies such as cloud computing, Internet of Things (IoT), and mobile networks rely heavily on cryptographic algorithms to maintain trust and data protection. As a result, scalable and efficient encryption mechanisms have become indispensable for ensuring secure information exchange across heterogeneous platforms (Katz and Lindell, 2020).

#### 1.1.3 Emergence of Quantum Computing Threat

Despite their effectiveness, classical cryptographic systems are increasingly threatened by advancements in quantum computing. Quantum computers leverage principles such as superposition and entanglement to perform computations beyond the capabilities of classical machines. Notably, Shor's

algorithm can efficiently solve integer factorization and discrete logarithm problems, thereby compromising widely used public-key cryptosystems such as RSA and ECC. This emerging threat necessitates the development of quantum-resistant cryptographic solutions (Bernstein, Buchmann and Dahmen, 2009).

## 1.2 Evolution of Cryptography

Cryptography has undergone significant transformation over time, evolving from simple manual ciphers to complex mathematically grounded algorithms designed to withstand sophisticated computational attacks.

### 1.2.1 Classical → Modern → Post-Quantum Transition

The evolution of cryptography can be broadly categorized into three phases: classical, modern, and post-quantum. Classical cryptography relied on substitution and transposition techniques, which were vulnerable to basic cryptanalysis. The advent of modern cryptography introduced mathematically secure algorithms based on computational hardness assumptions, forming the backbone of contemporary security systems. However, the emergence of quantum computing has led to the development of post-quantum cryptography, which aims to provide security against both classical and quantum adversaries (Goldreich, 2004).

### 1.2.2 Key Milestones in Cryptographic Development

Several milestones have shaped the development of cryptography. The Data Encryption Standard (DES), introduced in 1977, marked the first widely adopted symmetric encryption standard. The introduction of RSA in 1978 revolutionized secure communication by enabling public-key cryptography. Later, the Advanced Encryption Standard (AES) replaced DES in 2001, offering enhanced security and efficiency. A significant turning point occurred in 1994 with the introduction of Shor's algorithm, which demonstrated the vulnerability of classical public-key systems in a quantum computing environment (NIST, 2022).

## 1.3 Problem Statement

The advancement of quantum computing poses a fundamental challenge to the security of classical cryptographic systems that underpin modern digital communication infrastructures.

### 1.3.1 Vulnerability of Classical Cryptography to Quantum Attacks

Classical cryptographic algorithms, particularly public-key systems such as RSA and ECC, rely on mathematical problems that are computationally infeasible for classical computers. However, these problems can be efficiently solved using quantum algorithms such as Shor's algorithm, rendering these systems insecure in a quantum computing

environment. Although symmetric algorithms like AES remain relatively resilient, their security strength is reduced due to Grover's algorithm, necessitating larger key sizes for adequate protection (Mosca, 2018).

### 1.3.2 Lack of Unified Comparison Framework

Existing research primarily focuses on either classical or post-quantum cryptography in isolation, with limited efforts to provide a unified comparative framework. The absence of standardized evaluation metrics and benchmarking methodologies makes it difficult to assess trade-offs between security, computational complexity, and performance. This gap highlights the need for a systematic and comprehensive comparative analysis to guide future cryptographic migration strategies (Chen et al., 2016).

## 1.4 Research Objectives

The primary objective of this study is to conduct a systematic and comparative analysis of classical encryption algorithms and post-quantum cryptographic techniques under a quantum-aware threat model.

### 1.4.1 Analysis of Classical Algorithms

The study aims to examine widely used classical cryptographic algorithms, including both symmetric and asymmetric techniques, in terms of their operational principles, security assumptions, and performance characteristics. This analysis provides a baseline for evaluating their limitations in the context of emerging quantum threats.

### 1.4.2 Study of Quantum Impact

Another key objective is to investigate the impact of quantum computing on classical cryptographic systems. This includes analyzing the implications of quantum algorithms such as Shor's and Grover's algorithms on the security of existing encryption techniques.

### 1.4.3 Evaluation of Post-Quantum Cryptography Techniques

The research further aims to explore major categories of post-quantum cryptographic techniques, including lattice-based, code-based, hash-based, and multivariate approaches. These techniques are evaluated based on their resistance to quantum attacks and their practical feasibility for real-world deployment.

### 1.4.4 Comparative Analysis

A comprehensive comparative analysis is conducted to evaluate classical and post-quantum cryptographic approaches across multiple dimensions, including security strength, computational complexity, key size, and

performance efficiency. This objective is central to identifying the strengths and limitations of each approach.

## 2. LITERATURE REVIEW

The literature on cryptography reflects a rich evolution of theoretical foundations, algorithmic advancements, and security analyses across classical and emerging paradigms. This section critically examines prior research on classical cryptographic algorithms, the impact of quantum computing, post-quantum cryptographic techniques, and comparative studies. It also identifies key research gaps that motivate the present study.

### 2.1 Classical Cryptographic Algorithms

Classical cryptographic algorithms have been extensively studied and widely deployed in modern information security systems. These algorithms are broadly classified into symmetric and asymmetric cryptographic techniques, each serving distinct roles in secure communication.

#### 2.1.1 Symmetric Cryptographic Algorithms (AES, DES)

Symmetric encryption algorithms utilize a shared secret key for both encryption and decryption, making them highly efficient for bulk data processing. Early research focused on the Data Encryption Standard (DES), which introduced a Feistel structure and became a foundational encryption scheme. However, due to its relatively small key size, DES became vulnerable to brute-force attacks, leading to the development of the Advanced Encryption Standard (AES). AES employs a substitution-permutation network and offers enhanced security, scalability, and performance across various platforms. Extensive cryptanalytic studies have demonstrated AES's resilience against known attacks, making it the current standard for symmetric encryption in both academic and industrial applications (Daemen and Rijmen, 2002).

#### 2.1.2 Asymmetric Cryptographic Algorithms (RSA, ECC)

Asymmetric cryptographic algorithms rely on a pair of mathematically related keys, enabling secure communication without prior key exchange. RSA, one of the earliest public-key systems, is based on the computational difficulty of integer factorization. Elliptic Curve Cryptography (ECC), introduced later, provides equivalent security with significantly smaller key sizes, making it suitable for resource-constrained environments. Research in this area has focused on improving efficiency, reducing computational overhead, and formalizing security proofs. Despite their widespread adoption, these algorithms are fundamentally dependent on mathematical problems that are vulnerable to emerging computational paradigms (Rivest, Shamir and Adleman, 1978).

### 2.1.3 Security and Performance Studies

Numerous studies have evaluated classical cryptographic algorithms in terms of security strength, computational efficiency, and scalability. Symmetric algorithms are consistently shown to outperform asymmetric algorithms in terms of speed and resource utilization, making them ideal for encrypting large volumes of data. Conversely, asymmetric algorithms are primarily used for secure key exchange and digital signatures. Performance evaluations also highlight the importance of hardware acceleration and optimized implementations in enhancing cryptographic efficiency. However, these studies generally assume classical computational limitations, which may not hold in future quantum environments (Stallings, 2017).

## 2.2 Quantum Threat to Cryptography

The emergence of quantum computing introduces a new dimension to cryptographic security, challenging the assumptions that underpin classical encryption techniques.

### 2.2.1 Shor's Algorithm and Its Impact on RSA and ECC

Shor's algorithm represents a significant breakthrough in quantum computing, demonstrating that integer factorization and discrete logarithm problems can be solved in polynomial time using quantum machines. Since RSA and ECC rely on these problems for their security, the implementation of Shor's algorithm would effectively render these cryptographic systems obsolete. Theoretical analyses and simulation studies have confirmed the feasibility of this attack under sufficiently powerful quantum conditions, raising serious concerns about the long-term viability of classical public-key cryptography (Shor, 1994).

### 2.2.2 Grover's Algorithm and Its Impact on AES

In contrast to Shor's algorithm, Grover's algorithm provides a quadratic speedup for unstructured search problems, including brute-force key search. While this does not completely break symmetric encryption algorithms such as AES, it significantly reduces their effective security strength. For example, AES-128 would offer only 64-bit security under a quantum attack scenario. As a result, researchers recommend increasing key sizes, such as adopting AES-256, to maintain adequate security levels in a quantum computing environment (Grover, 1996).

## 2.3 Post-Quantum Cryptography Techniques

Post-Quantum Cryptography (PQC) has emerged as a proactive solution to counter the threats posed by quantum computing. These techniques are designed to remain secure against both classical and quantum adversaries.

### 2.3.1 Lattice-Based Cryptography

Lattice-based cryptography is among the most promising PQC approaches due to its strong security foundations and versatility. It relies on hard mathematical problems such as the Learning With Errors (LWE) and Shortest Vector Problem (SVP), which are believed to be resistant to quantum attacks. Research has shown that lattice-based schemes support a wide range of cryptographic functionalities, including encryption, digital signatures, and homomorphic encryption. Additionally, their relatively efficient implementations make them suitable for practical deployment (Peikert, 2016).

### 2.3.2 Code-Based Cryptography

Code-based cryptography is based on the difficulty of decoding random linear error-correcting codes. The McEliece cryptosystem is a well-known example that has withstood decades of cryptanalysis. While code-based schemes provide strong security guarantees, their adoption is often hindered by large public key sizes, which can affect storage and transmission efficiency. Despite this limitation, they remain a reliable candidate for quantum-resistant encryption (Bernstein et al., 2009).

### 2.3.3 Hash-Based Cryptography

Hash-based cryptographic schemes primarily focus on digital signatures and derive their security from the collision resistance of cryptographic hash functions. These schemes are considered highly secure due to their minimal reliance on complex mathematical assumptions. However, some implementations are stateful, requiring careful management of key usage to prevent security vulnerabilities. Stateless variants have been developed to address these concerns, improving usability and deployment potential (Buchmann, Dahmen and Hülsing, 2011).

### 2.3.4 Multivariate Cryptography

Multivariate cryptography is based on solving systems of multivariate polynomial equations over finite fields, a problem known to be computationally difficult. These schemes are characterized by fast computation times, particularly for signature generation and verification. However, several proposed schemes have been broken due to weaknesses in parameter selection, highlighting the need for ongoing cryptanalysis and careful design (Ding and Schmidt, 2005).

## 2.4 Comparative Studies in Existing Literature

Comparative analyses of classical and post-quantum cryptographic techniques have gained increasing attention in recent years.

### 2.4.1 Existing Comparisons

Existing studies compare classical and PQC algorithms across dimensions such as security, computational efficiency, and resource requirements. These studies consistently highlight that classical cryptographic systems are highly efficient and well-optimized, whereas PQC algorithms provide stronger resistance to quantum attacks. Some research also explores hybrid cryptographic models that combine classical and post-quantum techniques to ensure backward compatibility and transitional security (Katz and Lindell, 2020).

### 2.4.2 Limitations of Existing Studies

Despite these contributions, existing comparative studies exhibit several limitations. Many analyses are conducted in isolation, focusing either on classical or PQC algorithms without providing a unified evaluation framework. Furthermore, differences in experimental setups, parameter choices, and evaluation metrics make it difficult to draw consistent conclusions. The lack of standardized benchmarking methodologies further complicates the comparison of algorithm performance across different studies (Chen et al., 2016).

## 2.5 Research Gaps

A critical review of the literature reveals several gaps that necessitate further investigation and form the basis of the present research.

One of the most significant gaps is the lack of a unified framework for comparing classical and post-quantum cryptographic techniques. Existing studies often evaluate algorithms using different criteria, leading to inconsistencies in analysis and interpretation. A standardized evaluation model is essential for meaningful comparison and decision-making.

Another key limitation is the absence of comprehensive empirical benchmarking under standardized conditions. Many studies rely on theoretical analysis without providing practical performance evaluations, limiting their applicability in real-world scenarios.

Hybrid cryptographic approaches, which combine classical and post-quantum algorithms, have been suggested as a transitional solution. However, limited research has been conducted on their performance, security trade-offs, and implementation challenges, indicating a need for deeper investigation (Mosca, 2018).

Finally, the practical challenges associated with deploying post-quantum cryptography—such as large key sizes, computational overhead, and integration with existing protocols—are not fully explored in the literature. Addressing these challenges is critical for enabling

widespread adoption of PQC in real-world systems (NIST, 2022).

### 3. RESEARCH METHODOLOGY

The research methodology defines the systematic approach adopted to analyze and compare classical encryption algorithms with post-quantum cryptographic techniques. This study follows a structured and analytical process to ensure that the evaluation is logically consistent, reproducible, and aligned with the research objectives. The methodology integrates qualitative analysis with a multi-criteria evaluation framework to examine cryptographic algorithms under a quantum-aware threat model.

#### 3.1 Research Design

The research design provides the overall structure that guides the investigation. It determines how data is collected, analyzed, and interpreted to address the research problem effectively.

##### 3.1.1 Qualitative and Analytical Approach

The present study adopts a qualitative and analytical research approach, as the primary objective is to examine and compare existing cryptographic techniques rather than develop new algorithms or conduct experimental simulations. The qualitative aspect focuses on understanding the theoretical foundations, security assumptions, and operational characteristics of both classical and post-quantum cryptographic algorithms. This involves an in-depth review of scholarly literature, cryptographic standards, and technical reports.

The analytical component complements this approach by systematically evaluating cryptographic algorithms based on predefined criteria such as security strength, computational complexity, and performance efficiency. By synthesizing insights from multiple sources, the research establishes a comprehensive comparative framework that highlights the strengths and limitations of each cryptographic paradigm. This approach ensures that the study remains conceptually rigorous while providing meaningful insights for real-world applications.

#### 3.2 Data Sources

The reliability and validity of the research findings depend heavily on the quality of data sources used in the analysis. This study utilizes both primary and secondary data sources to ensure a comprehensive and balanced evaluation.

##### 3.2.1 Primary Data Sources

Primary data sources consist of official cryptographic standards, technical specifications, and reports published by recognized standardization bodies. In this research, documents from organizations such as the National Institute

of Standards and Technology (NIST) play a crucial role. These include Federal Information Processing Standards (FIPS) and reports from the Post-Quantum Cryptography standardization process.

Such sources provide authoritative information regarding algorithm design, security parameters, and performance benchmarks. Additionally, technical documentation of post-quantum algorithms—such as CRYSTALS-Kyber, Dilithium, and SPHINCS+—offers detailed insights into key sizes, computational complexity, and implementation characteristics. These primary sources form the empirical foundation for the comparative analysis conducted in this study.

##### 3.2.2 Secondary Data Sources

Secondary data sources include peer-reviewed journal articles, conference proceedings, and academic publications available through platforms such as IEEE Xplore, ACM Digital Library, and SpringerLink. These sources provide theoretical interpretations, comparative analyses, and critical evaluations of cryptographic algorithms.

Secondary literature is essential for understanding the evolution of cryptographic techniques, identifying research trends, and analyzing existing findings related to classical and post-quantum cryptography. By integrating insights from both primary and secondary sources, the study ensures a well-rounded and academically rigorous analysis.

#### 3.3 Analytical Framework

The analytical framework serves as the core component of the research methodology, enabling a structured comparison of cryptographic algorithms based on multiple evaluation criteria. This framework ensures consistency and objectivity in the analysis.

##### 3.3.1 Evaluation Parameters

To conduct a comprehensive comparison, the study defines a set of key evaluation parameters that capture both theoretical and practical aspects of cryptographic performance.

###### 3.3.1.1 Security Strength

Security strength refers to the ability of a cryptographic algorithm to resist attacks from both classical and quantum adversaries. This parameter evaluates whether the underlying mathematical problem remains computationally infeasible under different threat models. Classical algorithms are assessed based on their resistance to traditional attacks, while post-quantum algorithms are evaluated for their robustness against quantum algorithms such as Shor's and Grover's.

### 3.3.1.2 Computational Complexity

Computational complexity measures the efficiency of cryptographic operations, including key generation, encryption, decryption, signing, and verification. Algorithms with lower computational overhead are generally preferred for real-time applications. This parameter helps assess the practicality of deploying cryptographic techniques in environments with limited computational resources.

### 3.3.1.3 Key Size

Key size is an important factor that influences both security and resource requirements. Larger key sizes typically provide higher security but increase memory usage and communication overhead. This parameter evaluates the impact of key size on storage requirements and bandwidth consumption, particularly in large-scale systems.

### 3.3.1.4 Performance

Performance refers to the speed and efficiency of cryptographic operations. It includes metrics such as execution time, throughput, and latency. High-performance algorithms are essential for applications requiring fast and secure data processing, such as real-time communication systems and financial transactions.

### 3.3.1.5 Scalability

Scalability assesses the ability of cryptographic algorithms to perform efficiently in large-scale and distributed environments. This includes evaluating their suitability for applications such as cloud computing, IoT networks, and enterprise systems. Algorithms that scale well are more adaptable to evolving technological demands.

## 3.4 Research Phases

To ensure a systematic and logical progression, the research is divided into multiple phases. Each phase corresponds to a specific objective and contributes to the overall analysis.

### 3.4.1 Classical Algorithm Analysis

The first phase focuses on analyzing classical cryptographic algorithms, including both symmetric and asymmetric techniques. This phase examines their operational principles, security assumptions, and performance characteristics, establishing a baseline for comparison with post-quantum approaches.

### 3.4.2 Quantum Threat Evaluation

The second phase investigates the impact of quantum computing on classical cryptographic systems. It involves analyzing how quantum algorithms affect the security of widely used encryption techniques and identifying potential vulnerabilities in current systems.

### 3.4.3 Post-Quantum Cryptography Classification

In this phase, major categories of post-quantum cryptographic techniques are examined, including lattice-based, code-based, hash-based, and multivariate approaches. Each category is analyzed based on its mathematical foundation and resistance to quantum attacks.

### 3.4.4 Comparative Evaluation

The fourth phase represents the core of the research, where classical and post-quantum cryptographic algorithms are compared using the defined evaluation parameters. This phase provides a detailed assessment of trade-offs between security, performance, and resource requirements.

### 3.4.5 Practical Challenges Analysis

This phase focuses on identifying practical challenges associated with the implementation and deployment of post-quantum cryptography. Issues such as large key sizes, computational overhead, and integration with existing systems are examined in detail.

### 3.4.6 Insight Synthesis

The final phase synthesizes the findings from all previous stages to derive meaningful insights and recommendations. This includes identifying suitable cryptographic approaches for different application scenarios and proposing strategies for transitioning from classical to post-quantum cryptography.

## 4. CLASSICAL CRYPTOGRAPHIC ALGORITHMS ANALYSIS

Classical cryptographic algorithms form the backbone of modern information security systems and are widely used in applications ranging from secure communication to digital signatures. These algorithms are broadly categorized into symmetric and asymmetric encryption techniques, each designed to address specific security requirements. This section provides a detailed analysis of these algorithms, highlighting their operational characteristics, strengths, and inherent limitations, particularly in the context of emerging quantum threats.

### 4.1 Symmetric Encryption

Symmetric encryption algorithms utilize a single shared secret key for both encryption and decryption processes. These algorithms are known for their high computational efficiency and are commonly used for encrypting large volumes of data in real-time applications.

#### 4.1.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is the most widely adopted symmetric encryption algorithm and is considered

highly secure under classical computational models. It operates on a substitution-permutation network and supports key sizes of 128, 192, and 256 bits. AES is extensively used in applications such as secure web communication, file encryption, and wireless security due to its balance of security and performance.

#### 4.1.2 Data Encryption Standard (DES) and Triple DES (3DES)

The Data Encryption Standard (DES) was one of the earliest standardized symmetric encryption algorithms, based on a Feistel network structure. However, its 56-bit key size makes it vulnerable to brute-force attacks. To address this limitation, Triple DES (3DES) was introduced, which applies the DES algorithm three times to enhance security. Although 3DES improves resistance to attacks, it suffers from reduced efficiency and is gradually being phased out in favor of AES.

#### 4.1.3 Strengths and Weaknesses of Symmetric Encryption

Symmetric encryption algorithms offer significant advantages in terms of speed and computational efficiency, making them suitable for high-throughput systems. However, they also present challenges, particularly in secure key distribution and management, as both communicating parties must share the same secret key in advance.

Table 1: Analysis of Symmetric Encryption Algorithms

Algorithm	Key Size	Structure	Strengths	Weaknesses
AES	128/192/256 bits	Substitution-Permutation	High security, fast, efficient	Key distribution challenge
DES	56 bits	Feistel Network	Simple design	Vulnerable to brute-force attacks
3DES	112/168 bits	Triple Feistel	Improved security over DES	Slow, high computational cost

## 4.2 Asymmetric Encryption

Asymmetric encryption algorithms, also known as public-key cryptography, use a pair of keys—a public key for encryption and a private key for decryption. These algorithms play a crucial role in secure key exchange, digital signatures, and authentication mechanisms.

#### 4.2.1 RSA Algorithm

RSA is one of the earliest and most widely used asymmetric encryption algorithms. It is based on the computational difficulty of factoring large integers. RSA is extensively used in secure communication protocols such as SSL/TLS and

digital signature schemes. Despite its robustness under classical assumptions, RSA requires large key sizes to maintain security, which can impact performance.

#### 4.2.2 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) offers similar security to RSA but with significantly smaller key sizes, making it more efficient in terms of computation and storage. ECC is widely used in mobile devices, IoT systems, and blockchain technologies due to its lightweight nature. It is based on the difficulty of solving the elliptic curve discrete logarithm problem.

#### 4.2.3 Strengths and Weaknesses of Asymmetric Encryption

Asymmetric encryption provides a secure mechanism for key exchange and eliminates the need for pre-shared keys. However, these algorithms are computationally more intensive than symmetric encryption and are particularly vulnerable to quantum computing attacks, which can break their underlying mathematical assumptions.

## 4.3 Security Assumptions

The security of classical cryptographic algorithms is fundamentally based on the computational difficulty of specific mathematical problems. These assumptions are critical for ensuring that encryption schemes remain secure against adversaries with classical computational capabilities.

#### 4.3.1 Computational Hardness

Classical cryptographic systems rely on problems such as integer factorization, discrete logarithms, and brute-force key search being computationally infeasible within a reasonable time frame. For example, RSA depends on the difficulty of factoring large composite numbers, while ECC relies on the hardness of the elliptic curve discrete logarithm problem. Symmetric algorithms like AES depend on the infeasibility of exhaustive key search attacks.

#### 4.3.2 Limitations under Quantum Computing

The emergence of quantum computing challenges these foundational assumptions. Quantum algorithms such as Shor's algorithm can efficiently solve integer factorization and discrete logarithm problems, thereby compromising RSA and ECC. Similarly, Grover's algorithm reduces the effective security of symmetric algorithms by accelerating brute-force search. As a result, classical cryptographic systems are no longer considered future-proof, highlighting the urgent need for quantum-resistant alternatives.

## 5. QUANTUM COMPUTING IMPACT ON CRYPTOGRAPHY

Quantum computing represents a paradigm shift in computational capabilities, posing significant challenges to traditional cryptographic systems. Unlike classical computers, which process information in binary form, quantum computers exploit quantum mechanical phenomena to perform complex computations more efficiently. This section examines the fundamental principles of quantum computing, key quantum algorithms, and their implications for cryptographic security.

### 5.1 Fundamentals of Quantum Computing

Quantum computing is based on principles derived from quantum mechanics, enabling new forms of information processing that are fundamentally different from classical approaches.

#### 5.1.1 Qubits

The basic unit of quantum computation is the quantum bit, or qubit. Unlike classical bits that exist in a definite state of either 0 or 1, qubits can exist in a combination of both states simultaneously. This property allows quantum systems to process a vast number of possibilities in parallel, significantly enhancing computational power.

#### 5.1.2 Superposition

Superposition enables a qubit to exist in multiple states at once, allowing quantum computers to evaluate many possible solutions simultaneously. This capability is particularly advantageous in solving complex mathematical problems that are infeasible for classical systems.

#### 5.1.3 Entanglement

Entanglement is a quantum phenomenon in which two or more qubits become correlated in such a way that the state of one qubit instantly influences the state of another, regardless of distance. This property enables highly efficient information processing and plays a crucial role in quantum algorithms.

### 5.2 Quantum Algorithms

Quantum algorithms leverage the unique properties of quantum systems to solve problems more efficiently than classical algorithms. Two of the most significant algorithms impacting cryptography are Shor's and Grover's algorithms.

#### 5.2.1 Shor's Algorithm

Shor's algorithm provides an efficient method for solving integer factorization and discrete logarithm problems in polynomial time. Since the security of widely used public-key cryptographic systems such as RSA and ECC is based on the

computational hardness of these problems, Shor's algorithm effectively breaks these systems when executed on a sufficiently powerful quantum computer.

#### 5.2.2 Grover's Algorithm

Grover's algorithm offers a quadratic speedup for unstructured search problems, including brute-force key search. While it does not completely break symmetric encryption algorithms such as AES, it reduces their effective security strength by half. For instance, a 128-bit key effectively provides only 64-bit security under a quantum attack, necessitating the use of larger key sizes.

Table 2: Impact of Quantum Algorithms on Cryptography

Quantum Algorithm	Target Problem	Affected Cryptography	Impact
Shor's Algorithm	Factorization, Discrete Logarithm	RSA, ECC	Complete break
Grover's Algorithm	Brute-force search	AES, symmetric encryption	Security reduction (50%)

### 5.3 Cryptographic Implications

The development of quantum computing has far-reaching implications for the future of cryptographic security, particularly in the context of data protection and secure communication.

#### 5.3.1 "Harvest Now, Decrypt Later"

One of the most critical concerns is the "harvest now, decrypt later" attack model. In this scenario, adversaries collect encrypted data today with the intention of decrypting it in the future once quantum computing becomes sufficiently advanced. This poses a serious risk to sensitive information with long-term confidentiality requirements, such as government records, financial data, and healthcare information.

#### 5.3.2 Collapse of Public-Key Security

Public-key cryptographic systems form the backbone of secure communication protocols, including TLS, VPNs, and digital signatures. The ability of quantum algorithms to break these systems implies a potential collapse of current security infrastructures. This necessitates an urgent transition toward quantum-resistant cryptographic techniques to ensure long-term data security.

## 6. POST-QUANTUM CRYPTOGRAPHY TECHNIQUES

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to remain secure against both classical and quantum adversaries. These techniques are based on mathematical problems that are believed to be resistant to

quantum attacks. This section explores the major categories of PQC and their characteristics.

### 6.1 Lattice-Based Cryptography

Lattice-based cryptography is widely regarded as one of the most promising approaches to post-quantum security due to its strong theoretical foundations and practical efficiency.

#### 6.1.1 Learning With Errors (LWE) and Shortest Vector Problem (SVP)

Lattice-based schemes rely on hard mathematical problems such as the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP). These problems involve finding solutions within high-dimensional lattices and are considered resistant to both classical and quantum attacks.

#### 6.1.2 Example: CRYSTALS-Kyber

CRYSTALS-Kyber is a lattice-based encryption scheme selected by NIST for standardization. It offers strong security guarantees along with relatively efficient performance, making it suitable for real-world applications. Its moderate key sizes and computational efficiency make it one of the leading candidates for replacing classical public-key encryption.

### 6.2 Code-Based Cryptography

Code-based cryptography is one of the oldest post-quantum approaches and is based on the hardness of decoding random linear error-correcting codes.

#### 6.2.1 McEliece Cryptosystem

The McEliece cryptosystem is a well-known example of code-based cryptography that has remained secure for decades. It provides strong resistance to quantum attacks and is considered highly reliable. However, its practical adoption is limited by extremely large public key sizes, which can create challenges in storage and transmission.

### 6.3 Hash-Based Cryptography

Hash-based cryptography focuses primarily on digital signatures and derives its security from the strength of cryptographic hash functions.

#### 6.3.1 SPHINCS+

SPHINCS+ is a stateless hash-based signature scheme that provides strong security guarantees without relying on complex mathematical assumptions. It is resistant to quantum attacks and eliminates issues related to key reuse. However, it produces relatively large signatures and involves higher computational overhead, which can affect performance in resource-constrained environments.

### 6.4 Multivariate Cryptography

Multivariate cryptography is based on solving systems of multivariate polynomial equations over finite fields, which is a computationally difficult problem.

#### 6.4.1 Performance and Security Considerations

Multivariate schemes are known for their fast computation, particularly in signature generation and verification. This makes them attractive for high-performance applications. However, several proposed schemes have been broken due to structural weaknesses, raising concerns about their long-term security. As a result, careful design and ongoing cryptanalysis are required to ensure their reliability.

Table 3: Comparison of Post-Quantum Cryptographic Techniques

Technique	Security Basis	Strengths	Weaknesses
Lattice-Based	LWE, SVP	Strong security, efficient	Moderate key sizes
Code-Based	Error-correcting codes	Proven security	Very large keys
Hash-Based	Hash functions	High security, simple	Large signatures
Multivariate	Polynomial equations	Fast computation	Security concerns

## 7. COMPARATIVE ANALYSIS: CLASSICAL VS POST-QUANTUM CRYPTOGRAPHY

The comparative analysis between classical and post-quantum cryptographic techniques is essential to understand their relative strengths, limitations, and suitability for future secure systems. This section evaluates both approaches across multiple dimensions, including security, performance, resource requirements, and practical applicability. The analysis highlights the trade-offs involved in transitioning from traditional cryptographic systems to quantum-resistant alternatives.

### 7.1 Security Comparison

Security remains the most critical factor in evaluating cryptographic algorithms, particularly in the context of emerging quantum threats.

#### 7.1.1 Quantum Resistance

Classical cryptographic algorithms, especially public-key systems such as RSA and ECC, offer strong security under classical computational assumptions but are highly vulnerable to quantum attacks. Quantum algorithms, particularly Shor's algorithm, can efficiently break these systems, rendering them insecure in a quantum computing environment. In contrast, post-quantum cryptographic

(PQC) techniques are specifically designed to resist both classical and quantum attacks, making them more suitable for long-term security.

### 7.1.2 Security Model

The security model of classical cryptography is based on computational hardness assumptions that hold true only for classical adversaries. PQC, on the other hand, adopts a quantum-aware security model, ensuring resilience against both classical and quantum computational capabilities.

Table 4: Security Comparison

Aspect	Classical Cryptography	Post-Quantum Cryptography
Quantum Resistance	Low	High
Security Model	Classical-based	Quantum-aware

## 7.2 Performance Comparison

Performance evaluation focuses on the efficiency of cryptographic algorithms in terms of speed and computational requirements.

### 7.2.1 Speed

Classical cryptographic algorithms are highly optimized and benefit from decades of research and hardware acceleration. Symmetric algorithms like AES, in particular, offer high-speed encryption suitable for real-time applications. In contrast, many PQC algorithms involve more complex mathematical operations, leading to moderate execution speeds.

### 7.2.2 Computational Complexity

Classical algorithms generally have lower computational complexity, making them efficient for widespread deployment. PQC algorithms, however, often require higher computational resources due to complex underlying mathematical structures such as lattices and error-correcting codes. This increased complexity can impact performance, particularly in resource-constrained environments.

## 7.3 Key Size and Resource Analysis

Resource utilization is a critical factor in determining the practicality of cryptographic algorithms, especially in large-scale and distributed systems.

### 7.3.1 Key Size

Classical cryptographic algorithms typically use relatively small key sizes while maintaining strong security under classical assumptions. In contrast, PQC algorithms often require significantly larger key sizes to achieve quantum

resistance. For example, code-based cryptography may require keys that are several kilobytes in size, which can impact storage and transmission efficiency.

### 7.3.2 Memory Requirements

Due to larger key sizes and more complex computations, PQC algorithms generally require higher memory and storage resources compared to classical cryptographic systems. This can pose challenges for deployment in constrained environments such as IoT devices and embedded systems.

## 8. IMPLEMENTATION CHALLENGES AND PRACTICAL CONSIDERATIONS

Despite the advantages of post-quantum cryptography, several practical challenges must be addressed before its widespread adoption. This section discusses key implementation issues and potential solutions.

### 8.1 Key Size and Bandwidth Issues

One of the most significant challenges associated with PQC is the large size of cryptographic keys. Larger keys increase bandwidth consumption during data transmission and require additional storage capacity. This can be particularly problematic in networks with limited bandwidth or in applications requiring frequent key exchanges.

### 8.2 Computational Overhead

PQC algorithms typically involve more complex mathematical operations, resulting in increased computational overhead. This can lead to higher processing times and energy consumption, especially in devices with limited computational capabilities. Optimizing these algorithms for performance remains a critical area of research.

### 8.3 Integration Challenges

Integrating post-quantum cryptographic techniques into existing systems presents significant challenges. Current security protocols such as TLS, SSL, and VPNs are designed around classical cryptographic algorithms. Adapting these protocols to support PQC requires substantial modifications, including changes in key exchange mechanisms and certificate infrastructures.

### 8.4 Hybrid Cryptography

Hybrid cryptography has emerged as a practical solution for transitioning from classical to post-quantum systems.

#### 8.4.1 Classical and PQC Combination

Hybrid approaches combine classical cryptographic algorithms with post-quantum techniques to provide layered security. This ensures that even if one system is

compromised, the other remains secure, thereby enhancing overall resilience.

#### 8.4.2 Best Transition Strategy

Hybrid cryptography is considered the most viable transition strategy for organizations aiming to achieve quantum resistance without disrupting existing infrastructures. It allows gradual adoption of PQC while maintaining compatibility with current systems. This approach is particularly useful during the interim period before fully quantum-resistant standards are widely implemented.

### 9. CONCLUSION

This study presents a comprehensive comparative analysis of classical cryptographic algorithms and post-quantum cryptography (PQC) techniques within the context of emerging quantum computing threats. Classical encryption methods, including symmetric algorithms such as AES and asymmetric algorithms such as RSA and ECC, have long provided reliable and efficient security for digital systems. However, their underlying security assumptions are increasingly challenged by quantum algorithms, particularly Shor's and Grover's algorithms, which significantly weaken or completely break these traditional schemes.

In contrast, post-quantum cryptographic techniques—such as lattice-based, code-based, hash-based, and multivariate approaches—offer promising alternatives designed to resist both classical and quantum attacks. Despite their strong security guarantees, PQC methods introduce challenges related to increased key sizes, computational complexity, and performance overhead. The comparative analysis conducted in this study highlights the fundamental trade-off between efficiency and long-term security, emphasizing that no single cryptographic approach fully satisfies all requirements.

Furthermore, the research identifies hybrid cryptographic models as a practical transition strategy, enabling the coexistence of classical and quantum-resistant algorithms to ensure backward compatibility and enhanced resilience. As quantum computing continues to evolve, the adoption of PQC will become essential for safeguarding sensitive information. Therefore, ongoing research, standardization efforts, and optimization of PQC algorithms are crucial for achieving secure and scalable cryptographic solutions in future digital infrastructures.

### 10. LIMITATIONS OF THE STUDY

This study is primarily based on qualitative and analytical evaluation of existing cryptographic algorithms and does not include experimental implementation or empirical benchmarking. The absence of real-world performance testing limits the ability to measure practical efficiency, latency, and scalability under diverse operational conditions. Additionally, the analysis relies on currently available

literature and standards, which may evolve rapidly due to ongoing advancements in quantum computing and post-quantum cryptography.

Another limitation is the generalized comparison framework, which may not capture application-specific requirements such as constraints in IoT or embedded systems. Furthermore, hybrid cryptographic approaches are discussed conceptually without detailed implementation analysis. Future research should incorporate experimental validation, simulation-based benchmarking, and domain-specific evaluations to provide deeper insights into practical deployment challenges.

### REFERENCES

1. Bernstein, D.J., Buchmann, J. and Dahmen, E. (2009) *Post-Quantum Cryptography*. Berlin: Springer.
2. Bernstein, D.J., Lange, T. and Peters, C. (2009) 'Attacking and defending the McEliece cryptosystem', in *Post-Quantum Cryptography*. Berlin: Springer, pp. 31–46.
3. Buchmann, J., Dahmen, E. and Hülsing, A. (2011) 'XMSS – A practical forward secure signature scheme based on minimal security assumptions', in *Post-Quantum Cryptography*. Berlin: Springer, pp. 117–129.
4. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlmutter, R. and Smith-Tone, D. (2016) *Report on Post-Quantum Cryptography*. Gaithersburg: National Institute of Standards and Technology (NIST).
5. Daemen, J. and Rijmen, V. (2002) *The Design of Rijndael: AES – The Advanced Encryption Standard*. Berlin: Springer.
6. Ding, J. and Schmidt, D. (2005) 'Rainbow, a new multivariable polynomial signature scheme', in *Applied Cryptography and Network Security*. Berlin: Springer, pp. 164–175.
7. Goldreich, O. (2004) *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge: Cambridge University Press.
8. Grover, L.K. (1996) 'A fast quantum mechanical algorithm for database search', in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212–219.
9. Katz, J. and Lindell, Y. (2020) *Introduction to Modern Cryptography*. 3rd edn. Boca Raton: CRC Press.
10. Mosca, M. (2018) 'Cybersecurity in an era with quantum computers: Will we be ready?', *IEEE Security & Privacy*, 16(5), pp. 38–41.

11. National Institute of Standards and Technology (NIST) (2022) Post-Quantum Cryptography Standardization Process. Available at: <https://csrc.nist.gov/projects/post-quantum-cryptography>
12. Peikert, C. (2016) 'A decade of lattice cryptography', *Foundations and Trends in Theoretical Computer Science*, 10(4), pp. 283–424.
13. 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.
14. Shor, P.W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', in *Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 124–134.
15. Stallings, W. (2017) *Cryptography and Network Security: Principles and Practice*. 7th edn. Pearson.
16. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.K., Miller, C., Moody, D., Peralta, R. and Perlner, R. (2020) Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST.
17. Alkim, E., Ducas, L., Pöppelmann, T. and Schwabe, P. (2016) 'Post-quantum key exchange – A new hope', in *25th USENIX Security Symposium*, pp. 327–343.
18. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., Stebila, D. and Struck, F. (2019) 'Hybrid key encapsulation mechanisms and authenticated key exchange', in *IACR Cryptology ePrint Archive*, pp. 1–34.
19. Bos, J.W., Costello, C., Naehrig, M. and Stebila, D. (2015) 'Post-quantum key exchange for the TLS protocol from the ring learning with errors problem', in *IEEE Symposium on Security and Privacy*, pp. 553–570.
20. Brakerski, Z. and Vaikuntanathan, V. (2014) 'Efficient fully homomorphic encryption from (standard) LWE', *SIAM Journal on Computing*, 43(2), pp. 831–871.
21. Chen, L., Moody, D., Regenscheid, A., Robinson, A. and Randall, K. (2019) Report on the Third Round of the NIST PQC Standardization Process. NIST.
22. Ducas, L. and Micciancio, D. (2015) 'Improved short lattice signatures in the standard model', in *CRYPTO 2015*, pp. 335–352.
23. Ekerå, M. and Håstad, J. (2017) 'Quantum algorithms for computing short discrete logarithms and factoring RSA integers', in *Post-Quantum Cryptography*, Springer, pp. 347–363.
24. Gidney, C. and Ekerå, M. (2021) 'How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits', *Quantum*, 5, p. 433.
25. Hoffstein, J., Pipher, J. and Silverman, J.H. (1998) 'NTRU: A ring-based public key cryptosystem', in *ANTS III*, pp. 267–288.
26. Hülsing, A., Rijneveld, J. and Song, F. (2018) 'Mitigating multi-target attacks in hash-based signatures', in *PKC 2018*, pp. 387–416.
27. Kobitz, N. and Menezes, A. (2015) 'The random oracle model: A twenty-year retrospective', *Designs, Codes and Cryptography*, 77(2–3), pp. 587–610.
28. Langlois, A. and Stehlé, D. (2015) 'Worst-case to average-case reductions for module lattices', *Designs, Codes and Cryptography*, 75(3), pp. 565–599.
29. Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.K., Miller, C., Peralta, R. and Perlner, R. (2022) NIST PQC Standardization: Final Round Candidates. NIST
30. NIST (2023) FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (Kyber). National Institute of Standards and Technology.
31. NIST (2023) FIPS 204: Module-Lattice-Based Digital Signature Standard (Dilithium). National Institute of Standards and Technology.
32. NIST (2023) FIPS 205: Stateless Hash-Based Digital Signature Standard (SPHINCS+). National Institute of Standards and Technology.
33. Peikert, C. (2014) 'Lattice cryptography for the internet', in *Post-Quantum Cryptography*, pp. 197–219.
34. Regev, O. (2009) 'On lattices, learning with errors, random linear codes, and cryptography', *Journal of the ACM*, 56(6), pp. 1–40.
35. Stebila, D., Mosca, M. and Lippold, D. (2016) 'Post-quantum key exchange for the internet and the Open Quantum Safe project', in *Proceedings of SAC*, pp. 14–37.
36. Van Oorschot, P.C. (2020) *Computer Security and the Internet: Tools and Jewels*. 2nd edn. Springer.
37. Bernstein, D.J. and Lange, T. (2017) 'Post-quantum cryptography', *Nature*, 549(7671), pp. 188–194.
38. Childs, A.M., Jao, D. and Soukharev, V. (2014) 'Constructing elliptic curve isogenies in quantum subexponential time', *Journal of Mathematical Cryptology*, 8(1), pp. 1–29.

39. Campagna, M. and Petcher, A. (2018) 'Quantum-safe cryptography: Why, when, and how', IEEE Security & Privacy, 16(4), pp. 74–77.
40. Saarinen, M.J.O. (2020) 'Cryptographic engineering of post-quantum TLS', IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 2–24.