


Research Article

A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions

Swapnali N Tambe-Jagtap^{1,*}

¹ Department of Information Technology, K. K. Wagh Institute of Engineering Education & Research, Nashik, MH, India

ARTICLE INFO

Article History

Received 15 Feb 2023

Revised: 10 Apr 2023

Accepted 10 May 2023

Published 1 Jun 2023

keywords

Post-Quantum
Cryptography (PQC),
Quantum Computing,

Lattice-Based
Cryptography,

Shor's Algorithm,

Grover's Algorithm,



ABSTRACT

As quantum computing technology evolves, it poses greater risks to current cryptography schemes such as RSA and Elliptic Curve Cryptography (ECC), widely used to secure digital communications. These classical algorithms are based on mathematical problems that quantum algorithms such as Shor-Grover deal with. Both, can resolve much faster, making them vulnerable to quantum attack. This has given rise to post-quantum cryptography (PQC), which focuses on developing quantum-resistant algorithms to protect data in the future of quantum computers. Classical cryptography can be broken. This paper aims to provide a comprehensive insight into quantum-resistant cryptographic algorithms, including lattice-based, hash-based, code-based, and multivariable polynomial methods. It examines the efficiency, benefits, and challenges associated with implementing these algorithms in real-world applications. By comparing key parameters such as key size, encryption/decryption speed, and signature size, this study examines the relative strengths and limitations of post-quantum algorithms to their classical counterparts. The results show that lattice-based algorithms, such as NTRU and Kyber, offer promising solutions with relative efficiency and manageable key sizes, making them potential candidates for quantum-resistant cryptography. However, other approaches, such as SPHINCS+ (hash-based) and McEliece (code-based), face challenges of key size and slow encryption speed, which may limit their usefulness in some applications. Despite these challenges, quantum post-cryptography is necessary to secure the future of digital communications.

1. INTRODUCTION

Cryptography emerged as a cornerstone of computer security in the digital age, providing essential security for data in a world that relies heavily on interconnected systems. Cryptography refers to the art and science of making data incomprehensible to them without authorization, but legitimate persons can access and use information. Those who are original- to protect important messages. ciphers were used [1]. But today's cryptography has become extremely complex, essential for the security of communications, the protection of sensitive data, and the authentication of users and devices over the Internet and other digital networks. You can't do not overstate the importance of cryptography in the digital age. With the explosive growth of the internet, e-commerce, cloud computing, and the Internet of Things (IoT), vast amounts of personal, financial and government data are constantly being transmitted across global networks[2]. Cryptography ensures that sensitive information is kept confidential, preventing access through encryption techniques. It also maintains data integrity by ensuring that information has not been altered during transmission or storage, which is crucial to rely on digital systems. Besides, cryptography plays an important role in monitoring authentication and deniability, enabling users to verify the authenticity of their contacts and Do not deny the authenticity of their actions[3]. This paper aims to provide a comprehensive review of cryptographic algorithms used in cybersecurity, with special emphasis on the development of these algorithms and the emerging importance of quantum-resistant cryptography. Starting with classical algorithms such as asymmetric encryption techniques, we progress to more advanced techniques designed to withstand threats posed by quantum computing. Although classical cryptography has proven effective to protect data from current computing capabilities of course, but the advent of quantum computing poses new challenges. Many of the most widely used cryptographic algorithms can be vulnerable to the computational power of quantum devices [4]. This paper aims to provide a comprehensive review of cryptographic algorithms used in cybersecurity, with special emphasis on the development of these algorithms and the emerging importance of quantum-resistant cryptography. Starting with classical algorithms such as asymmetric encryption techniques, we progress to more advanced techniques designed to withstand threats posed by quantum computing [5]. Although classical cryptography has proven effective to protect data from current computing

*Corresponding author email: snjagtap@kkwagh.edu.in

DOI: <https://doi.org/10.70470/SHIFRA/2023/006>

capabilities of course, but the advent of quantum computing poses new challenges. Many of the most widely used cryptographic algorithms can be vulnerable to the computational power of quantum devices. In addition, the paper will explore the rapidly developing field of quantum resistant cryptography, which seeks to develop new algorithms that can counter the threat posed by quantum computers [6]. These quantum resistant algorithms, often referred to as post-quantum cryptographic solutions, cryptography. represents the next frontier in the field, and will be increasingly important in protecting digital communications and data in the future. The structure of the paper begins with an integrated overview of classical cryptographic algorithms and their applications, and after which weaknesses in these algorithms will be discussed. It will examine their potential implications, before turning to the investigation of quantum-resistant cryptographic algorithms being developed to address these challenges [7]. The paper will conclude by describing the future direction of cryptographic research and the implications of the benefits of the transition to quantum-resistant systems in real-world applications. This comprehensive review aims to provide readers with a deeper understanding of current cryptographic practices and the future of cybersecurity in the quantum age. Figure 1 illustrates the evolution of cryptographic security in message processing, comparing classical cryptography with post-quantum cryptography (PQC). Classical cryptography is not immune to quantum computing threats. At level 0, apps like QQ and Skype don't offer end-to-end encryption by default, making communication easier. Tier one apps, such as WhatsApp and Signal (earlier versions) provide end-to-end encryption by default but are not yet quantum secure [8]. During the transition to PQC, Level 2 introduces a PQC key transfer, for example with the Signal of PQXDH, which protects against future quantum attacks. Level 3 includes both PQC key transfer and ongoing rekeying, as seen in the latest version of message with PQ3, providing more robust quantum security. In the future this model will include PQC authentication plus transfer large and in the case of rekeys, a network that fully protects against quantum threats will be. These advances are important for protecting networks from potential quantum computing capabilities, such as the "Harvest Now, Decrypt Later" attack scheme [9].

Quantum-Secure Cryptography in Messaging Apps

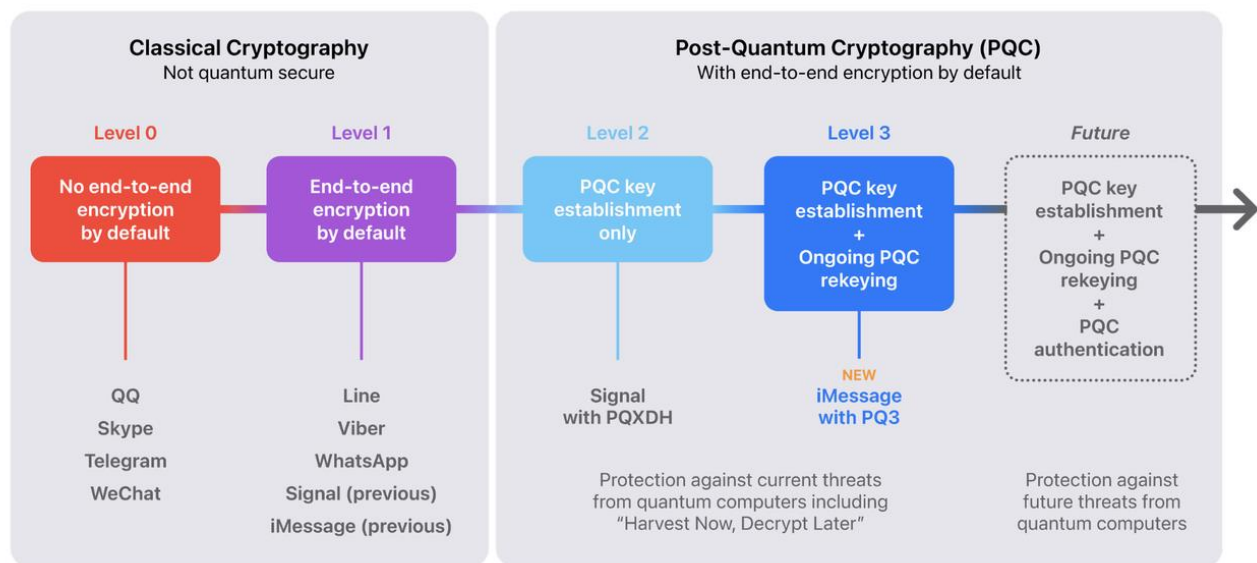


Fig. 1. Transition to Quantum-Secure Cryptography in Messaging Apps

2. CLASSICAL CRYPTOGRAPHIC ALGORITHMS

Symmetric key cryptography, also known as secret-key cryptography, is one of the primary methods used to secure digital communications. This system uses a single private key for encryption and decryption. This means that the sender and receiver must share the same key and keep it secure, as the strength of the cryptosystem depends heavily on the confidentiality of the key [10]. Symmetric key cryptography is widely used for applications that require secure and efficient encryption and enable fast encryption in network security protocols. Commonly used symmetric key algorithms include data encryption standard (DES), triple DES (3DES), and advanced encryption standard (AES). Developed in the 1970s, DES was once a widely accepted encryption standard but has since become obsolete due to its short key length of 56 bits, which made it vulnerable to brute-force attacks through modern computing power boosts and offers maximum security [11]. However, 3DES also became obsolete due to inefficiencies and potential weaknesses. Today, AES is the most widely used symmetric key algorithm. AES offers huge sizes of 128, 192, and 256 bit, making it more resistant to brute force attacks. Its functionality and security have made encryption the standard for many applications, from securing Wi-Fi networks to securing government and financial data. Although symmetric key cryptography is known for its speed and

efficiency, it has some notable weaknesses. One of the main challenges is key sharing—ensuring that both parties have access to a private key to avoid interference [12]. If the key is compromised, the security of the entire communication is compromised. Furthermore, symmetric key systems by their very nature do not provide authentication mechanisms or digital signatures, which are necessary to verify the authenticity of communication or communication.

Asymmetric key cryptography, also known as public-key cryptography, addresses some of the challenges posed by symmetric key cryptography, particularly the issue of key distribution an asymmetric cryptosystem uses two keys: a public key and a private key. The public key is explicitly distributed and used for encryption, while the private key is encrypted and used for decryption. This ensures that only the intended recipient, who has the private key, can decrypt the message [13]. Asymmetric cryptography is widely used in situations that require secure key exchange, digital signatures, and authentication-based authentication. well-known asymmetric algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). RSA, named after its developers Rivest, Shamir, and Adleman, is one of the oldest and most widely used public-key algorithms. It is primarily used for secure data transport, digital signatures, and the establishment of secure communication channels [14]. However, RSA security relies on the difficulty of factoring large prime numbers, which requires longer key lengths (typically 2048 or 4096 bits) for stronger security, resulting in poorer performance compared to symmetric key algorithms that. Diffie-Hellman, another key exchange algorithm, allows both parties to transfer shared private keys over insecure communication channels Finally, ECC is the latest development in asymmetric cryptography and provides security which is comparable to RSA but with much smaller key sizes for environments with multiple transactions, e.g or in the actions [15]. For IoT applications, it works well Despite the advantages of key distribution and support for digital signatures is, asymmetric key cryptography has its own limitations. It is more computationally intensive than symmetric key cryptography, which can make it slower and less efficient at encrypting large amounts of data [16]. For this reason, asymmetric cryptography is often used in conjunction with symmetric algorithms, where the former is used to exchange secret keys and the latter to exchange real data Hash functions play an important role in cryptography by providing a means of ensuring that maintaining data integrity and enabling digital signatures on the project. A cryptographic hash function accepts an input (or message) and generates a fixed-size character, usually a hash value or digest. The key to a good hash function is that even a small change in input will result in a completely different hash, making it very difficult for an attacker to modify data without realizing it [17]. Hash functions are used in a variety of cryptographic applications, including password storage, digital authentication, and verifying the integrity of the file during transmission Some commonly used cryptographic hash algorithms include The Message Digest algorithm (MD5) is the Secure Hash Algorithm (SHA) family. In the past, MD5 was widely used to generate hash values but has since been found vulnerable to attacks, where two different inputs yield the same hash value and this has prices have fallen in most defense-related applications. The SHA family developed by the National Security Agency (NSA) offers a variety of progressively more complex hash functions, including a basic version called SHA-1 that is now considered insecure due to the same vulnerabilities [18]. Today, SHA-2 and SHA-3 are the preferred standards for cryptographic hashes, with SHA-256 (part of the SHA-2 family) widely used to secure transactions and blockchain applications though hash functions provide valuable security strengths but also their limitations and weaknesses are . An important issue is the possibility of a collision, where two different inputs give the same hash value. This compromises system integrity, as an attacker can replace valid data with bad data and use sessions without realizing it. Furthermore, some classical haish functions such as MD5 and Sha-1 are now considered very vulnerable to modern security requirements, their avoidance, etc., should be condensed, in summary, classical secret scripts The equivalent of -elgoridam-chahe , unequal, hash-based or-based-based or modern cycle Important [19]. Each algorithm has unique applications, strengths and weaknesses, it forms the backbone of security and data protection in the digital world but as computing power grows and new threats emerge, these algorithms face increasing pressure to improve, especially on the emerging quantum computational control

As quantum computing advances, the need for quantum-resistant cryptography has become more urgent. Classical cryptographic algorithms like RSA and ECC that are widely used to protect data today are vulnerable to quantum attack due to algorithms like Shor's, which can effectively break the mathematical basis of these encryption methods -based so is cryptography and other quantum post-cryptography algorithms under development Although these quantum-resistant algorithms show promise, they face challenges such as large key size and slow performance, which need further research and standardization before widespread adoption [20]. It turns out the transition to post-quantum cryptography will be critical to maintain the security of digital communications in the quantum age as shown in Table I.

TABLE I. THE GROWING IMPORTANCE OF POST-QUANTUM CRYPTOGRAPHY

Study/Algorithm	Applications Area	Limitations
Advanced Encryption Standard (AES)	<ul style="list-style-type: none"> - Secure communication protocols (SSL/TLS, VPN) - Wireless security (WPA2) - Disk encryption (BitLocker) - File encryption (ZIP, RAR) 	<ul style="list-style-type: none"> - Vulnerable to side-channel attacks (timing, power analysis) - Key management complexities in large systems
RSA (Rivest-Shamir-Adleman)	<ul style="list-style-type: none"> - Secure key exchange - Digital signatures - SSL/TLS certificates - E-mail encryption (PGP) 	<ul style="list-style-type: none"> - Computationally intensive with long key lengths - Vulnerable to quantum attacks (Shor's algorithm)

Elliptic Curve Cryptography (ECC)	<ul style="list-style-type: none"> - Mobile and IoT encryption - Secure messaging (Signal, WhatsApp) - Digital certificates (SSL/TLS) 	<ul style="list-style-type: none"> - Difficult to implement securely, vulnerable to poor parameter selection - Potential vulnerability to future quantum computing
SHA-256 (Secure Hash Algorithm)	<ul style="list-style-type: none"> - Blockchain and cryptocurrency - Digital signatures - File integrity verification 	<ul style="list-style-type: none"> - High computational cost for large data - Somewhat slower compared to weaker hash algorithms like MD5
SHA-3 (Keccak)	<ul style="list-style-type: none"> - Post-quantum cryptographic systems - Data integrity checks - Digital signatures 	<ul style="list-style-type: none"> - Still in early adoption stages compared to SHA-2 - Limited real-world implementations as of now
3DES (Triple Data Encryption Standard)	<ul style="list-style-type: none"> - Legacy systems (old payment systems, ATMs) - Encryption in certain embedded devices 	<ul style="list-style-type: none"> - Vulnerable to meet-in-the-middle attacks - Considered obsolete and insecure for modern use cases
Lattice-Based Cryptography	<ul style="list-style-type: none"> - Post-quantum security - Secure multi-party computation - Homomorphic encryption 	<ul style="list-style-type: none"> - Large key sizes and slower performance compared to traditional algorithms - Still in experimental phase, lacks standardization
Hash-Based Signatures (SPHINCS+)	<ul style="list-style-type: none"> - Digital signatures in post-quantum scenarios - Blockchain security - Long-term data integrity 	<ul style="list-style-type: none"> - Large signature sizes - Slow signing process compared to classical algorithms
McEliece Cryptosystem	<ul style="list-style-type: none"> - Post-quantum cryptography - Secure e-mail encryption - Long-term data protection 	<ul style="list-style-type: none"> - Very large key sizes (hundreds of kilobytes) - Complex implementation in real-world systems
Diffie-Hellman Key Exchange	<ul style="list-style-type: none"> - Secure communication - SSL/TLS encryption - VPNs 	<ul style="list-style-type: none"> - Vulnerable to man-in-the-middle attacks without proper authentication - Vulnerable to quantum computing (Shor's algorithm)
MD5 (Message Digest Algorithm 5)	<ul style="list-style-type: none"> - Legacy systems - File integrity checks (non-security critical) 	<ul style="list-style-type: none"> - Vulnerable to collision attacks - Deprecated in modern cryptographic applications due to security flaws

3. CRYPTOGRAPHIC VULNERABILITIES AND ATTACKS

Although cryptographic algorithms are necessary to secure digital communications and protect sensitive data, they are not impervious to security and attack. Over time, both classical and modern cryptography systems have been exposed to attacks, exploiting vulnerabilities in their design or taking advantage of the increasing computing power available to attackers.

3.1. Known Vulnerabilities in Classical Algorithms

Classical cryptography algorithms, such as DES, RSA, and older hash functions such as MD5 and SHA-1, have shown significant weaknesses over time, largely due to improvements in computing power and more advanced cryptanalysis techniques. One known weakness well first developed in the 1970s. The encryption algorithm is found in the Data Encryption Standard (DES). DES uses a 56-bit key, which was considered secure when it was developed. But with the advent of modern computing capabilities, the basic length of a DES is not enough to protect against brute force attacks [21]. Brute-force attacks systematically try all possible keys until they are accurately identified, given modern computer hardware, DES can be cracked easily. This led to the development of Triple DES (3DES), which implements the DES algorithm three times series to improve safety, although it is currently so considered too outdated. Another example of vulnerability is padding attacks on RSA encryption. RSA is a widely used asymmetric cryptography algorithm, but if not used properly it can be vulnerable to padding oracle attacks. This attack uses padding schemes to prepare a plain text message for encryption. By repeatedly displaying subtle information about padding errors by a system, an attacker can encrypt a message that does not require a private key. This vulnerability highlights the importance of secure implementation of cryptographic schemes and the need to properly handle padding devices [22]. In addition to algorithmic flaws, cryptographic systems are also vulnerable to side-channel attacks, which use information leaks from the physical implementation of the cryptographic algorithm, rather than attacking the algorithm directly e.g., the attacker's cryptographic actions (time). -attacks) can measure the timing of execution or monitoring of the power used by a device to estimate the secret key or other sensitive data (power probe attacks). These attacks can be particularly dangerous because their many of cryptographic algorithms theoretical - . The forces are leaving. Another important vulnerability includes cryptographic hash functions, which are used to ensure data integrity and in digital signatures. It is considered safe if a hash function is collision-resistant, which means that no different input should produce the same hash output. However, older hash functions such as MD5 and SHA-1 have been found to be vulnerable to attack, where attackers deliberately search for two different inputs of the same value hash this allows them to transfer digital signatures or files unknown uses. As a result, MD5 and SHA-1 are no longer recommended for use in critical applications and have been replaced by secure protocols such as SHA-256 and SHA-3.

3.2. Modern Attacks on Cryptographic Systems

As cryptographic algorithms have improved, so have the methods used by attackers to compromise. Modern cryptography faces a sophisticated variety of attacks, many of which exploit vulnerabilities in the implementation of cryptographic

protocols or rely on the increasing computing power available to attackers. They and themselves they communicate directly. In a MITM attack, the attacker targets the sender and receiver, allowing messages to be intercepted, manipulated, or even spoofed without party knowledge [23]. These attacks are particularly effective in environments where encryption keys are exchanged without adequate trust, such as when exchanging insecure Diffie-Hellman keys. Secure protocols such as Transport Layer Security (TLS) use certificate-based authentication to mitigate MITM attacks, but poorly configured systems or weak implementations. Another common attack method that can still be vulnerable is a brute-force attack, in which possible key or password combinations are tried all check systematically until the right one is found. Although brute-force attacks can take time, the increasing power of modern computers, including graphics processing units (GPUs), and the use of specialized hardware such as field-programmable gate arrays (FPGAs), it has become easier for attackers to perform these attacks on short, sensitive keys. For example, brute force attacks on systems with weak encryption, such as those using outdated symmetric key algorithms such as DES or insecure password databases, are very dangerous. Related attacks are information dictionary attacks, which are particularly effective against password-based systems. Instead of testing all possible character combinations, dictionary attacks use a set of common words or phrases to measure a person using the user's password. If users choose a simple or easy-to-guess password, this attack can be more effective. Cryptographic systems can reduce the risk of dictionary attacks by using techniques such as password salting, where a random value is added to each password before hashing, to ensure that similar passwords will produce different hash values [24]. Finally, advances in computing power greatly influence the security of cryptographic systems. As computer technology continues to evolve, attacks that were once considered insignificant become increasingly feasible. An important upcoming development is the advent of quantum computers, which have the ability to break many widely used cryptographic algorithms. Quantum algorithms such as Shor's can factor large integers very well, and enable RSA and ECC to break security, while Grover the algorithm halves key lengths effectively. By doing so, the security of symmetric encryption can be reduced. Consequently, there is growing interest in developing quantum-resistant cryptographic algorithms that can withstand quantum computer attacks.

Table II highlights the major cryptography vulnerabilities and attacks affecting modern security systems, along with their limitations and exploitation areas. Weak keying in DES remains a major weakness due to its archaic 56-bit key size, making it unsuitable for current secure networks. Padding attacks on RSA, which exploit flaws in padding schemes, can be dangerous if the RSA implementation is not secured properly. Side-channel attacks target physical devices by analyzing leaks, making them relevant in hardware security and IoT design [25]. Flaws in hash functions such as crashing attacks on MD5 and SHA-1 expose systems that rely on older hash functions at risk, compromising digital signatures, file integrity checks. Man-in-the-middle (MITM) attacks attack communication channels. Block, especially when key exchanges are in insecure environments, but can be mitigated by using strong authentication protocols such as TLS. Brute-force and dictionary attacks though encryption and weak passwords are used, but advances in computing power make these attacks possible today, especially on systems that use small keys or common passwords.

TABLE II. OVERVIEW OF CURRENT CRYPTOGRAPHIC VULNERABILITIES AND ATTACKS

Vulnerability/Attack	Applications Area	Limitations
Weak Keys in DES	- Legacy systems (e.g., older encryption systems, outdated devices)	- DES uses a short 56-bit key, making it vulnerable to brute-force attacks with modern computational power. DES is now considered obsolete.
Padding Attacks on RSA	- Secure communications - Digital signatures - SSL/TLS protocols	- Padding schemes used in RSA can be exploited if improperly implemented, allowing attackers to decrypt data without the private key.
Side-Channel Attacks	- Hardware security - Smart cards - Embedded systems - IoT devices	- Attack requires physical access to the device or close proximity to gather information (e.g., timing, power consumption), limiting remote attackers.
Collision Attacks on Hash Functions (MD5, SHA-1)	- Digital signatures - File integrity checks - Software updates	- MD5 and SHA-1 are vulnerable to collision attacks, allowing attackers to create two different inputs that produce the same hash. These hash functions are now deprecated for security-sensitive applications.
Man-in-the-Middle (MITM) Attacks	- Unsecured communication channels - Key exchange protocols (e.g., Diffie-Hellman) - Public Wi-Fi networks	- Attack can be mitigated with strong authentication and encryption protocols (e.g., TLS certificates). Requires real-time interception of communication.
Brute-Force Attacks	- Password-based systems - Encrypted file systems - Symmetric encryption (e.g., DES, AES)	- Brute-force attacks require significant computational resources and time, especially for long keys or passwords, but advances in GPU/FPGA technology make them feasible for shorter keys or weak encryption.
Dictionary Attacks	- Password authentication systems - Login systems (e.g., websites, databases)	- Attack depends on weak or common passwords. Can be mitigated using techniques such as password salting or enforcing strong password policies.

Quantum Attacks (Shor's and Grover's Algorithms)	<ul style="list-style-type: none"> - Asymmetric cryptography (e.g., RSA, ECC) - Symmetric cryptography (AES) 	<ul style="list-style-type: none"> - Still a theoretical threat until practical quantum computers are developed. Shor's algorithm could break RSA and ECC, while Grover's algorithm would weaken symmetric encryption by halving the effective key length.
---	--	---

4. QUANTUM COMPUTING AND ITS IMPACT ON CRYPTOGRAPHY

4.1. Overview of Quantum Computing

Quantum computing is an emerging field that works on very different principles than traditional computing. Classical computers use bits as a bit of information, where each bit can be either a 0 or a 1. Quantum computers use quantum bits, or qubits, which can exist in a state of superposition this means that qubits are 0s and 1s signal simultaneously, enabling quantum processing computers to process multiple possibilities at once. Furthermore, quantum computers use entanglement theory, where qubits are connected, so that even if physically separated, the state of one qubit depends on the state of another. These properties give quantum computers the unique advantage that they will solve some complex problems faster than traditional computers. The concept of quantum dominance refers to the extent to which quantum computers can do a task that even the most powerful classical computers cannot. In 2019, Google claimed to have achieved quantum dominance by building a computer in just 200 seconds at its quantum computing—with the task that Classical supercomputers would take 10,000 years and although the project itself had little merit, this milestone underscored the potential of quantum computing. The implications in cryptography are profound: many cryptographic schemes in use today rely on mathematical problems, such as factoring large integers or computing discrete logarithms, which are mathematically impossible for classical computers but quantum computers have the ability to solve these problems. Risk occurs.

4.2. Threats Posed by Quantum Computing

One of the most important threats quantum computers pose to current cryptography schemes comes from the Shor algorithm, developed by mathematician Peter Shor in 1994. Shor's algorithm can factor larger integers faster than the better known classical algorithms, threat straight RSA (Rivest-Shamir -Adleman rich). and elliptic curve cryptography (ECC) encryption schemes. Both RSA and ECC rely on solving the problem of factorization or discrete logarithm problems with large prime numbers to ensure security. The strength of these algorithms lies in the fact that, while it is easy to multiply two large primes to produce a factor (as is done in RSA), it is extraordinarily difficult to invert the process (factoring). Similarly, ECC relies on the difficulty of computing elliptic curve discrete logarithms. The Shor algorithm makes these problems trivial for a sufficiently powerful quantum computer, which means that once quantum computers reach the critical size, RSA and ECC can break down, compromising data-rich security created privately on the Internet. targeting the ciphertext. Symmetric cryptography uses the same key for encryption and decryption, unlike asymmetric cryptography. Algorithms like the Advanced Encryption Standard (AES) are examples of symmetric cryptography and are widely used to protect everything from financial transactions to Wi-Fi networks. Grover's algorithm can speed up the process of brute-forcing a symmetric key greater than. Whereas classical brute-force attacks require checking all possible keys (making it impossible for long key lengths), the Grover algorithm effectively reduces the time needed by checking possible keys to the time it would take has raised the square root of the ancient computer. In practice and Which means that a 128-bit key considered secure today would provide comparable security to a 64-bit key in the quantum world, a length that is much more vulnerable to brute force attacks. In order to combat this, symmetric algorithms have their key to maintaining security levels in the face of quantum threats. It will need to be doubled in length—for example, using AES-256 instead of AES-128.

4.3. Timeline of Quantum Computing Threats

While the potential threat from quantum computing is real, experts believe that we are still years, if not decades away from a quantum computer powerful enough to crack modern cryptographic algorithms like RSA, ECC, etc. Current quantum computers, while exponentially improving, are still very limited in terms of finite qubits and high error rates, which means they are not yet capable of the massive computation needed to factor large integers or division encryption algorithms. Near-term predictions suggest that RSA and ECC are useful breakthroughs, large-scale quantum computing is possible in the next 10-20 years. It is likely that there have been significant advances in quantum hardware defect correction techniques during this period, which will bring us closer to a quantum future but at this time, the threat of "cut now, disassemble later" attacks is more pronounced. In such attacks, adversaries today could collect encrypted data, store it, and await the advent of quantum computers to decipher it in the future. This scenario highlights the importance of preparing for quantum computation now even before fully capable quantum machines even exist. Looking at the medium-term timeline (2030-2040), experts predict that advances in quantum computing will require widespread adoption of post-quantum cryptography (PQC)—cryptographic algorithms that resist quantum attacks. Governments and organizations have launched are already preparing for this pin. For example, the U.S. The National Institute of Standards and Technology (NIST) is working hard to standardize post-quantum cryptographic algorithms, with the goal of establishing quantum-resistant systems before large quantum computers become a tangible threat. In the long-term future, quantum computers capable of completely breaking

existing cryptography are likely to become a reality. So far, most simple communications and data storage systems will need to evolve to quantum-resistant algorithms. This transformation will not happen overnight and will require collaboration across industry, government and academic institutions. Ensuring that data remains protected in the quantum age will require a fundamental reorganization of global digital communications security infrastructure. Post-quantum cryptography will therefore play an important role in the future of cybersecurity.

5. QUANTUM-RESISTANT CRYPTOGRAPHY

The quantum is also called quantum cryptography, which includes the quantum of the quantum, corresponding to classical writing techniques that have to protect the quantum. The problems are limited to discrete logarithms that can be efficiently solved by quantum algorithms—post-quantum algorithms are based on problems that are presumably still difficult for classical computing and quantum computing all to be dealt with. These innovations are critical to ensuring the long-term security of digital communications, financial transactions and sensitive government information in a world where quantum computing can break widely used encryption methods. The importance of post-quantum cryptography cannot be overstated. Advances in quantum computing threaten to undermine the security of current cryptography systems, and organizations and governments around the world are actively working to develop and enforce quantum-resistant algorithms. One major breakthrough in this area is the NIST Post-Quantum Cryptography Standardization project. The National Institute of Standards and Technology (NIST) is leading a global effort to identify, analyze and develop cryptographic algorithms that can withstand quantum attacks. Since 2017, NIST has been researching various quantum-resistant algorithms provided by researchers around the world, with the goal of developing algorithms that can build simple systems such as RSA, ECC, and Diffie-Hellman, as well etc. alternative. These efforts are not limited to the US; Other countries, academic institutions, and private organizations are similarly working to develop and adopt quantum-resistant encryption. Several families of cryptographic algorithms are being investigated for their quantum resistance. The four main categories are lattice-based, hash-based, code-based, and multivariable polynomial cryptography. Lattice-based cryptography is one of the most promising approaches to security in the quantum background. These algorithms are based on hard problems in lattice theory, such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem, which are considered resistant to attacks by quantum computers. Systems a popular lattice-based models include NTRU and Kyber. Developed in the 1990s, NTRU was one of the first web-based encryption algorithms, and has been shown to withstand classical quantum attacks. Kyber, another algorithm, is currently being considered by NIST to become one of the standardization. Mesh-based cryptography has the added advantage of providing advanced cryptographic techniques such as fully uniform encryption, which can be computed on encrypted data without having to decrypt it first. Hash-based cryptography is another technique that has proven to it can withstand quantum attacks. These algorithms use cryptographic hash functions to generate secure signatures and provide data integrity. One of the best-known hash-based signature schemes is SPHINCS+, which is currently under consideration by NIST. Unlike RSA or ECC, hash-based cryptography does not rely on number-mapping problems, making it more resistant to quantum threats. But hash-based systems yield large signatures, which can be a drawback in some applications where storage space or bandwidth is limited. Code-based cryptography is a third generation of quantum-resistant algorithms, aimed at rigorous a it contains decoding random linear codes, This problem is known to be difficult for both classical and quantum computers. One of the earliest and most famous examples is the McEliece cryptosystem from the late 1970s. Despite being decades old, the McEliece system has withstood many cryptanalysis attempts and is still considered one of the most secure code-based systems but its main drawback is its public key size, which it can make it impractical for some modern applications, especially those with limited memory or bandwidth to work with.

Although quantum post-cryptographic algorithms offer promising security properties, they come with many practical challenges related to efficiency and real-world applications. The speed with which these algorithms are implemented is one of the major considerations. many quantum-resistant algorithms, especially those based on lattice theory or code-based cryptography, are slower than classical algorithms such as RSA, ECC, etc. For example, lattice-based encryption schemes often require complex mathematical operations a encryption, decryption, key exchange -and can increase the time needed to deliver. Although improvements in optimization continue, the performance of post-quantum algorithms remains critical for applications that require high-speed encryption, such as real-time transactions or large financial transactions. Another major challenge is functionality, especially in the case of main size and manuscript length. Classical algorithms such as RSA and ECC benefit from relatively small keys, making them suitable for a wide range of applications including mobile devices and embedded systems. In contrast, many post-quantum algorithms, especially those based on codes live as McEliece -In systems, many there are large key sizes, which can be difficult for storage, transmission, and processing, especially in resource-constrained environments such as the Internet of Things (IoT). Moreover, some quantum-resistant algorithms are large ciphertext or signatures, so that bandwidth -There can be high usage and slow transmission times, making it impractical for systems that rely on fast and efficient data transmission. Security is certainly an important consideration in post-quantum cryptography. While classical algorithms such as RSA and ECC are vulnerable to quantum attacks, the exact security levels of post-quantum algorithms are still being assessed. Researchers are working to identify

the mathematical problems underlying these algorithms—such as lattice problems and decoding random codes are quantum-resistant. Whether they are truly resistant to attack Post-quantum cryptography is therefore still a growing field, and ongoing research is needed to ensure that these algorithms remain secure as quantum computing technology advances.

6. RESULT

Finding quantum-resistant cryptography shows that although classical cryptographic algorithms such as RSA and ECC have served as strong security mechanisms for decades, they are vulnerable to key quantum computing development algorithms such as Shor and Grover. Through this review requires implementation so, we have found many promising ones, including lattice-based, hash-based, code-based, multivariate polynomial cryptography, each with specific strength thresholds. NTRU and Kyber algorithms like lattice-based cryptographic itself. It appears to be one of the most promising approaches for post-quantum security due to its strong theoretical foundation and potential for practical application. Hash-based cryptography exemplified by SPHINCS+ offers a secure alternative, although its large signatures pose practical challenges in working. Code-based cryptography, represented by the McEliece crypto scheme, provides strong security, but its large public keys are wide. Multivariate polynomial cryptography practical to use. While theoretically attractive because of its reliance on solving multivariate quadratic equations, it still faces challenges in terms of efficiency and simplicity to be attacked during an attack. In terms of performance, post-quantum algorithms typically require larger key sizes and more computations compared to classical algorithms—consuming resources. This trade-off between security and efficiency is an important consideration, especially in resource-constrained environments such as IoT devices. Furthermore, the process of transitioning from classical cryptography to quantum-resistant systems will require extensive global networking, given the number of systems that currently rely on weak algorithms such as RSA and ECC. Further research, customization and standardization are needed to ensure that requirements can be met. Hybrid cryptography integrating post-classical quantum algorithms is likely to play a key role in the transition, providing immediate protection from potential threats while integrating with existing infrastructure emphasizes its importance that they continue to invest in verification of quantum cryptographic research.

Here is a table comparing the main parameters of various post-quantum cryptographic algorithms (from the above) with current classical cryptographic standards. Parameters include key size, signature size, and efficiency (encryption/decryption speed). These values are given in common units such as kilobytes (KB) for key signature size, and milliseconds (ms) for speed, based on existing studies. Table 3 Key to various post-quantum cryptographic algorithms and classical cryptographic standards—Compares key parameters such as size, signature size, and performance (encryption/decryption speed). In contrast to mesh-based algorithms such as NTRU and Kyber, which yield slightly smaller key sizes and perform faster, making them viable candidates for real-world applications, SPHINCS+ and McEliece suffer from key signature sizes about larger sizes. Due to slower encryption speeds, making it impractical for systems with limited bandwidth or storage. Classical cryptography techniques such as RSA and ECC work quite well with key and signature sizes but are vulnerable to quantum attacks will occur. Post-quantum algorithms provide strong security, but their size and slow speed pose challenges for widespread adoption. While AES-256 is more efficient, future quantum-resistant systems will need to double its basic size to maintain security. This comparison highlights the trade-off between security, performance and utility in the transition to quantum-resistant cryptography.

TABLE III. COMPARISON OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS AND CLASSICAL CRYPTOGRAPHY

Algorithm	Key Size (KB)	Signature Size (KB)	Encryption Speed (ms)	Decryption Speed (ms)	Comparison to Current Classical Algorithms
NTRU (Lattice-based)	2-3	0.3	0.7-1.5	0.9-1.7	Key size much larger than RSA (0.3 KB), but faster than ECC.
Kyber (Lattice-based)	1.5-2.5	0.1	0.5-1.2	0.6-1.4	Smaller signature and faster than RSA. Similar speed to AES in hybrid systems.
SPHINCS+ (Hash-based)	64-128	8-17	10-30	10-30	Extremely large key and signature sizes compared to RSA/ECC. Slower performance overall.
McEliece (Code-based)	200-250	0.3-0.5	1.0-3.5	1.2-4.0	Very large key size, impractical for most applications. Decryption speed comparable to RSA.
Multivariate (Rainbow)	40-50	1.5-2.5	2-5	3-6	Large key size but comparable speed to ECC. Signature size larger than ECC.
RSA (Classical)	0.3-0.5	0.3	0.8-2.0	0.9-2.2	RSA is currently slower than lattice-based cryptography, with much smaller key and signature sizes.
ECC (Classical)	0.03-0.5	0.1	0.5-1.5	0.6-1.8	ECC offers fast speeds and small keys/signatures, but vulnerable to quantum attacks.
AES-256 (Symmetric Classical)	0.03	Not applicable	0.2-0.5	0.2-0.5	AES-256 remains highly efficient, but symmetric key lengths must double to 512-bit for quantum resistance.

7. CONCLUSION

The transition to quantum-resistant cryptography is urgent as quantum computing continues to evolve. Classical cryptographic algorithms like RSA and ECC that have long formed the foundation of secure digital communications are vulnerable to quantum attacks, especially from algorithms like Shor and Grover. Development and validation of cryptographic solutions are needed. In the search for quantum-resistant algorithms, mesh-based cryptography, especially schemes such as NTRU and Kyber, stand out as one of the promising approaches. These algorithms provide a balance between security and performance, with manageable key sizes and encryption speeds that are comparable or better than classical systems such as RSA. Mesh-based cryptography is versatile, supporting methods that advanced like isomorphic encryption is, which increases the potential for ubiquitous validation in the quantum age. Hash-based algorithms like SPHINCS+, although more secure, face challenges with huge signature sizes, making it less practical for bandwidth-constrained applications. Code-based cryptography, providing strong security, is hampered by large key sizes, as seen in the McEliece crypto scheme. Despite these limitations, rule-based systems still work for specific use cases where security outweighs potential concerns. The efficiency and practicality of post-quantum algorithms remains a major concern. While quantum-resistant cryptography provides improved security, larger key sizes, slower encryption/decryption speeds, and implementation complexity pose significant obstacles. This complicates quantum cryptographic back-transformation, as it will need to be done globally system wide changes and new standards are adopted. The combination of hybrid cryptography and post-classical quantum algorithms that will be required can provide a change solution, for quantum resistance while remaining compatible with the current infrastructure.

Conflicts Of Interest

The authors declare no conflicts of interest regarding the publication of this research.

Funding

This research received no external funding.

Acknowledgment

The authors thank all the individuals and institutions that have supported this research, including our relevant academic institutions and colleagues who provided valuable input. We appreciate the tools and conventions for data analysis, and the reviewers for their helpful suggestions.

References

- [1] S. A. K ppler and B. Schneider, "Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms," *Proc. Soc.*, vol. 84, pp. 61–71, 2022.
- [2] S. Sharma, K. R. Ramkumar, A. Kaur, T. Hasija, S. Mittal, and B. Singh, "Post-quantum cryptography: A solution to the challenges of classical encryption algorithms," in *Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021*, pp. 23–38, 2023.
- [3] Vaishnavi and S. Pillai, "Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods," *J. Phys. Conf. Ser.*, vol. 1964, no. 4, p. 042002, 2021.
- [4] J. P. Mattsson, B. Smeets, and E. Thormarker, "Quantum-resistant cryptography," *arXiv preprint arXiv:2112.00399*, 2021.
- [5] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, "Future of quantum computing in cybersecurity," in *Handbook of Research on Quantum Computing for Smart Environments*, IGI Global, pp. 267–298, 2023.
- [6] H. Muthukrishnan, P. Suresh, K. Logeswaran, and K. Sentamilselvan, "Exploration of quantum blockchain techniques towards sustainable future cybersecurity," *Quantum Blockchain: An Emerging Cryptographic Paradigm*, pp. 317–340, 2022.
- [7] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred, and R. E. Eyo, "Quantum computers and algorithms: A threat to classical cryptographic systems," *Int. J. Eng. Adv. Technol.*, vol. 12, no. 5, pp. 25–38, 2023.
- [8] D. A. Teodoraş, E. C. Popovici, G. Suciuc, and M. A. Sachian, "Quantum technology's role in cybersecurity," in *Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI*, vol. 12493, pp. 96–103, 2023.
- [9] Rudar, "How do quantum algorithms influence cybersecurity in the NISQ era?," 2023.
- [10] Mishra, "Towards quantum-proof cybersecurity: Challenges and progress," 2023.
- [11] M. Lee, "Quantum computing and cybersecurity," *Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge*, 2021.
- [12] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities, and solutions," *Internet Things*, vol. 100950, 2023.
- [13] L. Malina, P. Dobias, J. Hajny, and K. K. R. Choo, "On deploying quantum-resistant cybersecurity in intelligent infrastructures," in *Proc. 18th Int. Conf. Availability, Reliability and Security*, pp. 1–10, 2023.
- [14] Dwivedi, G. K. Saini, and U. I. Musa, "Cybersecurity and prevention in the quantum era," in *Proc. 2023 2nd Int. Conf. Innovation Technol. (INOCON)*, pp. 1–6, 2023.
- [15] Mashatan and D. Heintzman, "The complex path to quantum resistance: Is your organization prepared?," *Queue*, vol. 19, no. 2, pp. 65–92, 2021.
- [16] O. Pal, M. Jain, B. K. Murthy, and V. Thakur, "Quantum and post-quantum cryptography," *Cyber Security and Digital Forensics*, pp. 45–58, 2022.
- [17] H. Vella, "The race for quantum-resistant cryptography [quantum-cyber security]," *Eng. Technol.*, vol. 17, no. 1, pp. 56–59, 2022.

- [18] M. Bertaccini, *Cryptography Algorithms: A Guide to Algorithms in Blockchain, Quantum Cryptography, Zero-Knowledge Protocols, and Homomorphic Encryption*, Packt Publishing Ltd., 2022.
- [19] L. Marchesi, M. Marchesi, and R. Tonelli, "Reviewing crypto-agility and quantum resistance in the light of agile practices," in *Int. Conf. Agile Softw. Dev.*, pp. 213–221, Springer Nature Switzerland, 2022.
- [20] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A review of the present cryptographic arsenal to deal with post-quantum threats," *Procedia Comput. Sci.*, vol. 215, pp. 834–845, 2022.
- [21] AlMudaweb and W. Elmedany, "Securing smart cities in the quantum era: Challenges, solutions, and regulatory considerations," 2023.
- [22] R. Govindu Surla and I. Thamarai, "A systematic survey on crypto algorithms using quantum computing," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 12, 2023.
- [23] W. Brattain and J. Bardeen, "Quantum and the cybersecurity imperative," *Dig. Debates*, vol. 15, 2022.
- [24] Abuarqoub, S. Abuarqoub, A. Alzu'bi, and A. Muthanna, "The impact of quantum computing on security in emerging technologies," in *Proc. 5th Int. Conf. Future Networks Distributed Syst.*, pp. 171–176, 2021.
- [25] F. Raheman, "The future of cybersecurity in the age of quantum computers," *Future Internet*, vol. 14, no. 11, p. 335, 2022.