Sri Lanka Institute of Information Technology

The Impact of Quantum Computing on Classical Cryptography Systems

Gunasekara D T
IT23621138

Introduction to Cyber Security - IE2022

June, 2025

Table of Contents

01. Abstract **3**

02. Introduction **4**

2.1 What is Cryptography 4

2.2 What is Quantum Computing 5

2.3 Principles of Quantum Computing 5

03. Evolution **7**

3.1 Evolution of Classical Cryptography 7

3.1.1 Earliest Cryptographic methods 7

3.1.2 Modern Algorithms 7

3.1.3 Why are They Secure? 9

3.2 Impact of Quantum Computing 9

3.2.1 The impact on Asymmetric Encryption 9

3.2.2 The impact on Symmetric Encryption 11

3.3 Real world risks 12

04. Future Developments **13**

4.1 Post-Quantum Cryptography (PQC) and standardization 13

4.1.1 What is Post-Quantum Cryptography (PQC) ? 13

4.1.2 NIST Post-Quantum Cryptography (PQC) initiative 15

4.1.3 Challenges of Post-Quantum Cryptography (PQC) Adoption 15

4.2 Quantum Key Distribution (QKD) and its Advantages 17

4.2.1 How Quantum Key Distribution (QKD) works 17

4.2.2 Entanglement based Quantum Key Distribution (QKD) 18

4.2.3 Limitations of Quantum Key Distribution (QKD) 19

4.3 Future of Cyber Security in the Quantum World 20

4.3.1 Transitioning to Hybrid Cryptography 20

4.3.2 Quantum-Resistant BlockChain and Digital Signatures 21

4.3.3 Quantum Readiness 21

05. Conclusion **22**

5.1 Summary 22

5.1 Future Recommendations 22

06. References **23**

01. Abstract

As quantum computing continues to evolve, it poses a significant threat to the foundational security principles of classical cryptographic systems. Algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are currently considered secure and widely implemented across digital communications, financial systems, and government infrastructure, may be considered outdated by powerful quantum algorithms like Shor's and Grover's. The ability of quantum computers to solve problems that are computationally infeasible for classical systems introduces a paradigm shift in cryptographic security.

This paper explores the evolution of classical cryptography and examines how quantum computing disrupts these mechanisms. It also analyzes key mitigation strategies, including the development of Post-Quantum Cryptography (PQC), which aims to create quantum-resistant algorithms, and the use of Quantum Key Distribution (QKD) for secure communication. Furthermore, the report also discusses real-world risks to various sectors and evaluates hybrid cryptographic approaches and the design of quantum-resilient systems. Overall, this paper stresses the need for proactive quantum readiness across industries, governments, and cybersecurity ecosystems.

02. Introduction

In today's digital landscape, cryptography functions as the backbone of cybersecurity, protecting sensitive information across financial transactions, online communications and national security systems. However, with the rapid advancements in quantum computing, modern cryptographic systems face an imminent threat. Algorithms that were once considered secure due to their computational complexity may soon become outdated, posing a significant threat to the confidentiality, integrity and availability on a global scale.

With the increasing computational power of quantum computers, the cybersecurity community faces a pressing need to adapt existing cryptographic protocols to safeguard digital infrastructure. This shift is critical as quantum technologies continue to evolve at an extraordinary rate, and the need for quantum-resistant solutions becomes more important than ever.

This paper aims to explore the evolution of cryptographic systems, the challenges posed by quantum computing, and the ongoing efforts to develop quantum-resistant encryption standards. Moreover, the report will dive into several future developments in quantum computing and cryptography, such as post-quantum cryptography (PQC) and quantum key distribution (QKD).

2.1 What is Cryptography?

By definition, cryptography is the transformation of data to hide its content and prevent unauthorized use [1]. The process involves creating algorithms and protocols to protect data and information in many situations, making sure that sensitive information remains confidential and unchanged during transmission. Cryptography is a key concept in Cybersecurity as it allows for secure communication in various sectors such as Online Banking and Email Encryption.

The primary purpose of cryptography is to ensure the security and trustworthiness of digital communications. This is achieved through four key principles:

- **Confidentiality**: Ensuring that data and information is accessible to authorized users
- **Integrity**: Confirming that data and information has not been altered or tampered with.
- **Authentication**: Verification of the identity of users and systems involved in communication
- **Non-repudiation**: Ensuring that the sender cannot deny having sent the message

2.2 What is Quantum Computing?

Quantum Computing uses the principles of quantum mechanics to process information in ways that classical computers cannot [2]. Unlike modern computers that process information in binary form using bits (that is 0's and 1's), quantum computers use quantum bits or qubits which can represent both 0 and 1 simultaneously.

These qubits are able to perform parallel calculations, allowing quantum computers to process vast amounts of data at once, enabling exponential speedup for solving problems that are computationally infeasible for classical computers. For example, quantum computers are able to factor large numbers more efficiently than classical computers as the latter takes up an impractical amount of time for such operations.

As quantum computing is still in its developmental stages, a quantum revolution may take some time to initiate, but it has the potential to transform fields such as cryptography, quantum secure communication, artificial intelligence and machine learning, optimization methods, financial analysis and various other fields, including logistics, climate modeling, and material science.

2.3 Principles of Quantum Computing

Several key principles of quantum mechanics are used as the building blocks of quantum computing.

Qubits: Qubits are the fundamental units of quantum computing. They can exist in multiple states simultaneously due to the principle of superposition, meaning they can represent both 0 and 1 at the same time. Qubits are created by changing the state of certain atoms and other quantum particles such as electrons, protons, neutrons and even photons. The process of changing state can be done using Laser Beams, Electro Magnetic fields or radio waves [2].

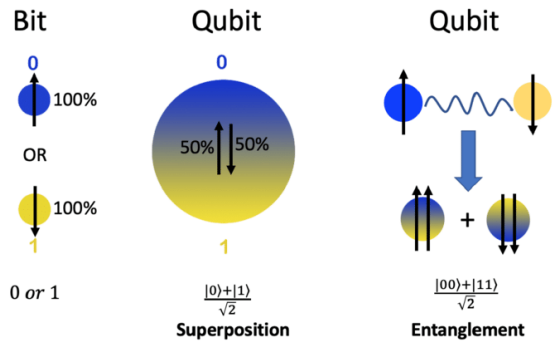

Figure 1: Illustration of a bit and qubit. Source: [37]

Superposition: Superposition is the ability of a qubit to exist in a combination of 0 and 1 states until measured. This allows quantum computers to process a larger amount of possibilities in a short amount of time [2].

Entanglement: Entanglement is a quantum phenomenon where two or more qubits become correlated, meaning the state of one qubit instantaneously influences the state of the other, regardless of the distance between them [2]. This property enhances quantum computing capabilities.

Quantum Interference: When qubits are processed in quantum algorithms, their probabilities of being in a particular state can interfere with one another; constructively or destructively [2]. Quantum interference aids quantum algorithms to handle probability amplitudes of different computational outcomes, strengthening correct solutions while canceling out incorrect ones.

03. Evolution

Throughout history, cryptography has evolved to meet emerging security challenges, transitioning from simple manual ciphers to highly complex mathematical encryption algorithms. Early cryptographic techniques mainly focused on securing written messages, whereas modern cryptography ensures digital security in nearly every aspect of technology. However, the emergence of quantum computing introduces entirely new challenges, posing significant risks to existing cryptographic systems and driving the need for developing quantum-resistant security measures.

3.1 Evolution of Classical Cryptography

The evolution of classical cryptography spans centuries, adjusting to the growing complexity of communication and security needs. From simple substitution ciphers used in ancient civilizations to more structured encryption techniques, early cryptographic methods have laid the foundation for modern encryption systems. Understanding these initial methods provides an insight into how cryptography has developed over time to address emerging threats.

3.1.1 Earliest Cryptographic methods

The earliest cryptographic methods, such as the Caesar cipher (introduced by King Julius Caesar of Rome) [3] and the Scytale cipher (first used by the Spartans of Ancient Greece) [4] are based on simple letter shifts or transposition methods to obscure messages. However, with adversaries using methods like frequency analysis to break these ciphers, they have become ineffective.

The introduction of the Vigenère cipher, first described by cryptographer Giovan Battista Bellaso in 1553, is a polyalphabetic cipher which temporarily improved security but again was eventually broken with the develop of statistical analysis techniques [5].

3.1.2 Modern Algorithms

The advent of computers enabled cryptographic methods to become more sophisticated, allowing the transition from manual ciphers to more difficult encryption mechanisms where they use complex mathematical algorithms to ensure data security. Modern encryption techniques fall into two primary categories: symmetric encryption and asymmetric encryption, each designed to address different security needs.

Symmetric encryption, or private-key encryption focuses on using a single key for both encryption and decryption purposes [6]. This method is mostly used for securing large amounts of data and is highly efficient. Data Encryption Standard (DES) was one of the earliest symmetric algorithms

and was widely adopted until the algorithm became vulnerable to advances in computing power. As a result, Advanced Encryption Standard (AES) was introduced, offering stronger security with key sizes of 128, 192, or 256 bits. Symmetric encryption is widely implemented in secure file storage, VPNs, and database encryption for its speed and efficiency. However, its primary constraint is key distribution, as securely sharing the secret key between both parties presents a challenge [7].

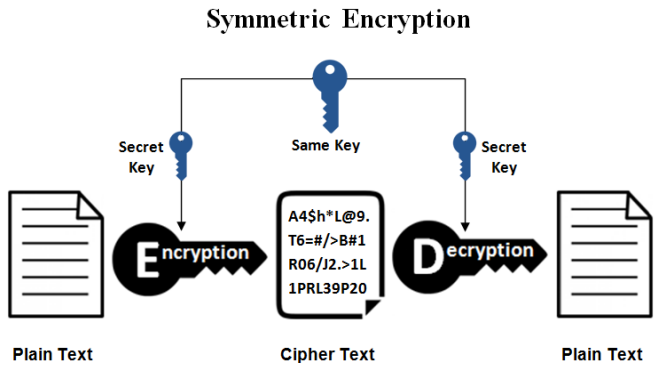

Figure 2: Symmetric encryption process using the same key for encryption and decryption. Source [38]

Asymmetric Encryption, or public-key encryption, focuses on the key distribution problem by using two mathematically related keys [8]. A public key for encryption and a private key for decryption. This method of encryption enables secure communication over untrusted networks and is vital to protocols such as SSL/TLS, which protect internet transactions. The Rivest-Shamir-Adleman (RSA) algorithm, based on the difficulty of factoring large prime numbers, has been a cornerstone of asymmetric cryptography for decades. More recently, Elliptic Curve Cryptography (ECC) has gained popularity due to its ability to provide strong security with smaller key sizes, making it more efficient for resource-scarce environments. Asymmetric encryption is widely used in digital signatures, secure email communications, and BlockChain technology [9].

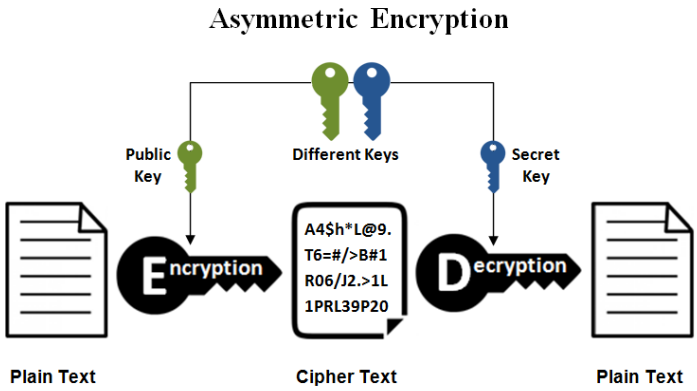

Figure 3: Asymmetric encryption process using a key pair for encryption and decryption. Source [38]

3.1.3 Why are They Secure?

The security of modern cryptographic algorithms relies on complex mathematical principles that make it computationally infeasible for attackers to break those using classical computers. Symmetric encryptions such as AES derives its strength from key length and algorithm complexity. AES-256, for instance, has 2 to the power 256 possible keys, making brute-force attacks practically impossible [10].

Asymmetric encryption, on the other hand, is based on hard mathematical problems. RSA security depends on the difficulty of factoring large prime numbers, while ECC relies on the elliptic curve discrete logarithm problem (ECDLP). These problems are computationally costly to solve, ensuring that decrypting encrypted messages without the private key remains impossible [11].

The emergence of quantum computing poses a threat to both asymmetric and symmetric encryption. Shor's algorithm can efficiently break RSA and ECC, making current public-key encryption insecure. Similarly, Grover's algorithm speeds up brute-force attacks on symmetric encryption, reducing the effective security of the AES algorithm. This highlights the need for quantum-resistant cryptographic methods.

3.2 Impact of Quantum Computing

The rise of quantum computing presents a significant challenge to modern cryptographic systems. Almost all encryption techniques rely on mathematical problems that are infeasible for classical computers to solve within a reasonable timeframe. However, quantum algorithms such as Shor's and Grover's exploit the concept of quantum parallelism to break these cryptographic defenses efficiently. This poses a severe risk to both asymmetric encryption, which secures digital signatures and key exchange mechanisms, and symmetric encryption, which protects data confidentiality and integrity.

3.2.1 The Impact on Asymmetric Encryption

Asymmetric encryption supports various security aspects such as secure communications, authentication, and digital signatures. The security implementations are based on complex mathematical problems that are computationally exhaustive for classical computers [8]. Quantum computing introduces new threats to these encryption systems.

Threat from Shor's Algorithm

Developed by American Computer Scientist Peter Shor in 1994, Shor's algorithm efficiently factors large numbers and computes discrete logarithms using a quantum computer. This capability directly threatens widely used asymmetric encryption schemes like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography).

For example, while classical computers would require an impractical amount of time to factor a 2048-bit RSA key, a sufficiently powerful quantum computer running Shor's algorithm could accomplish this in computationally efficient time, making RSA and ECC-based security vulnerable [12-13].

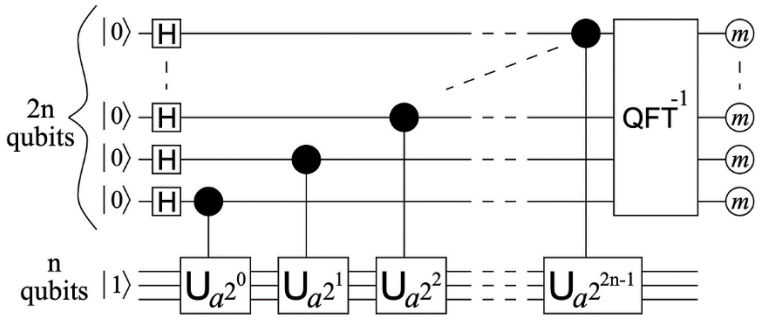

Figure 4: Quantum circuit diagram of Shor's Algorithm. Source: [39]

Impact on Digital Signatures and Secure Communications

A digital signature is a cryptographic technique used to verify the authenticity, integrity, and origin of a digital message or document. Public key cryptography systems like RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) are used to sign documents, authenticate users, and secure protocols such as TLS, SSH, and VPNs.

If quantum computers can effectively implement Shor's algorithm, attackers could forge digital signatures, leading to identity spoofing and man-in-the-middle attacks, thereby compromising internet security, online transactions, and sensitive communications [14-15].

Risk to Blockchain Security

Simply defined, Blockchain technology is a secure and decentralized digital ledger that records transactions in linked blocks, making it tamper-proof and transparent. BlockChain relies heavily on asymmetric encryption for transaction security. Cryptographic methods like ECDSA and SHA-256 hashing generate wallet addresses and validate transactions.

If quantum computers become capable of breaking these encryption schemes, attackers could forge transactions, steal assets, and undermine the integrity of BlockChain networks such as Bitcoin and Ethereum. [16].

3.2.2 The Impact on Symmetric Encryption

Symmetric encryption is generally considered more resistant to quantum attacks compared to asymmetric encryption due to the usage of the same key for both encryption and decryption purposes. However, quantum computing still poses risks, particularly through Grover's algorithm, which accelerates brute-force attacks on encryption keys and weakens cryptographic hash functions.

Threat from Grover's Algorithm

Founded in 1996 by Indian-American Computer Scientist Lov Kumar Grover, Grover's algorithm is a quantum search algorithm that reduces the time complexity of brute-force attacks. In classical computing, breaking an 'n'-bit encryption key requires 2 to the power 'n' operations, making brute-force attacks impractical for sufficiently large keys.

However, Grover's algorithm reduces this complexity to $2^{n/2}$ operations. This means that an AES-256 encryption key, which is currently considered highly secure, would have its security reduced to that of a 128-bit key in the presence of a quantum computer. While this does not make AES immediately insecure, it implicates that longer key sizes, such as AES-512 may be essential for future quantum-resistant encryption [17-18].

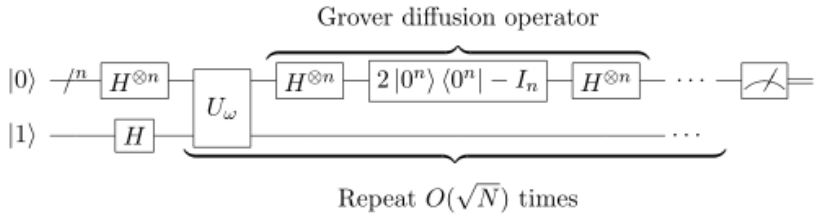

Figure 5: Quantum circuit diagram of Grover's Algorithm. Source: [40]

Vulnerability of Hash Functions

Cryptographic hash functions like SHA-256 and SHA-3 are vital for digital integrity checks and password hashing. Grover's algorithm weakens these hash functions by enabling collision attacks with quadratic speedup (faster than a classical algorithm but not exponentially faster).

Typically, finding a collision in a 256-bit hash function requires 2 to the power 256 attempts, but with a quantum computer, this is reduced to 2 to the power 128 attempts, making it significantly easier to break.

This vulnerability could lead to tampered digital certificates and compromised password storage. To mitigate this risk, security experts recommend using longer hash outputs, such as SHA-384 or SHA-512, or adopting post-quantum cryptographic hashing techniques [19].

3.3 Real World Risks

The emergence of quantum computing brings serious security risks across multiple industries. Many encryption methods currently used to protect sensitive data and critical infrastructure could become outdated, leaving governments, businesses, and individuals exposed to cyber threats. This section explores several real-world risks associated with quantum advancements [20-21].

Digital Harvesting:
Digital harvesting is the practice of collecting and storing encrypted data now with the intent of decrypting it once quantum computers become powerful enough. Sensitive information such as financial records, medical data, and classified communications could be exposed in the future.
Cybercriminals and state-sponsored threat actors may already be intercepting encrypted transmissions, hoping that quantum decryption will eventually render them readable.

Impact to Financial Systems:
Financial institutions rely on cryptographic protocols for securing transactions, online banking, and digital payments. Quantum computing could compromise encryption methods like RSA and ECC, allowing attackers to forge digital signatures, intercept transactions, and manipulate banking systems. A successful quantum attack could lead to large-scale fraud, financial instability, loss of trust in digital banking, and even manipulate global stock markets, potentially triggering economic instability.

Impact to Healthcare Systems:
Healthcare systems store large amounts of sensitive patient data, including medical histories and genomic information. If quantum computers break current encryption methods, medical records could be exposed, leading to privacy violations and the potential exploitation of health data. Medical devices such as pacemakers and insulin pumps rely on secure authentication and the manipulation of such devices can cause harm to patients as well. Furthermore, secure communication between hospitals, insurance companies, and pharmaceutical firms could be at risk, along with security to pharmaceutical research data, which if stolen can lead to the loss of intellectual property and stalled medical innovation.

Impact to Military and National Security:
Governments and defense agencies rely on encryption to protect classified intelligence, military operations, and national security communications. A quantum-capable adversary could decrypt sensitive information, exposing defense strategies, surveillance data, and diplomatic communications. This can lead to serious geopolitical concerns, cyber warfare, national security breaches and attempts on accessing nuclear defense systems that control nuclear codes, drone communications and satellite communications.

04. Future Developments

As quantum computing continues to evolve, it provides both opportunities and challenges for the future of cybersecurity. The security of classical cryptographic systems is at risk of being challenged by the computational power of quantum computers, which could break popular encryption techniques like RSA and ECC. However, the rise of quantum computing also brings forth a new path for developing stronger, quantum-resistant encryption methods.

This section will explore several developments that are shaping the future of cybersecurity in the quantum era, including post-quantum cryptography (PQC), quantum key distribution (QKD), and the transition towards quantum-safe systems.

4.1 Post-Quantum Cryptography (PQC) and Standardization

The emergence of quantum computing has made it critical for cryptographic systems to evolve. Post-Quantum Cryptography (PQC) is defined as cryptographic algorithms that are designed to be secure against both quantum and classical computational attacks [22]. These algorithms deal with mathematical problems that quantum computers are not expected to solve efficiently, offering a promising solution to the looming threat posed by quantum computing.

However, to ensure that these algorithms provide total security and interoperability to any system, they must undergo a rigorous standardization process. Organizations such as NIST (National Institute of Standards and Technology) conduct efforts to evaluate, select and standardize various quantum-resistant cryptographic algorithms. This standardization ensures that these newly created cryptographic methods are tested for real world applicability before they are deployed and implemented in critical domains such as finance, healthcare and national security [23].

4.1.1 What is Post-Quantum Cryptography (PQC)?

Post-Quantum Cryptography (PQC) is a cybersecurity domain dedicated to developing cryptographic systems that remain secure in the presence of quantum computing [22]. Unlike current cryptographic protocols that rely on mathematical problems like integer factorization or discrete logarithms which quantum computers can efficiently solve, PQC aims to mitigate this risk by creating quantum-resistant cryptographic algorithms based on mathematical problems that remain difficult for both classical and quantum computers to solve efficiently. These algorithms are currently being evaluated for standardization by organizations such as NIST (National Institute of Standards and Technology)**.**

Types of Post-Quantum Cryptographic Algorithms:

Currently there are several classes of cryptographic algorithms identified that are believed to be resistant to quantum attacks [24]:

1. **Lattice-based Cryptography**

    - Uses high-dimensional lattices where solving problems like the Shortest Vector Problem is hard for both classical and quantum computers.

    - Known for strong security, efficiency, and scalability.

    - Some examples are Kyber (used Post-Quantum Key Encapsulation) and Dilithium (used in digital key signatures).

2. **Code-based Cryptography**

    - Based on the problem of decoding random linear codes, code-based cryptography has been developed. These Error-correcting codes are used to encrypt the messages, making decryption without the proper key very difficult.

    - Long history of security, but large key sizes make practical use challenging.

    - The McEliece cryptosystem is a famous code-based cryptographic method that has been used for over 40 years, but is quite impractical due to large key sizes.

3. **Multivariate Polynomial Cryptography**

    - The usage of multivariate quadratic equations that are hard to solve without the private key.

    - Solving them without the knowledge of the secret key is extremely difficult, and this cryptographic method works well for digital signatures.

    - The Rainbow scheme was a promising example until it was cracked during the NIST PQC selection process.

4. **Hash-based Cryptography**

    - Hash functions are mathematical algorithms that take and input and produce a fixed length output, making it nearly to impossible reverse-engineer the original data [25]. This secure method is intertwined with cryptography to create Hash-based cryptography.

- Excellent for Digital Signatures, as the security relies on the one-way nature of hash functions rather than mathematical problems that are vulnerable to quantum attacks.

- The SPHINCS+ stateless hash-based scheme is a great implementation of Hash-based cryptography that is considered for the NIST PQC initiative.

5. **Isogeny-based Cryptography**

- Solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), which involves finding a value in a specific set, is used in Elliptic Curve Cryptography [26]. Isogeny-based cryptography builds on this concept where isogenies, which are special mathematical functions that maps one elliptic curve to another, making this method computationally hard to solve.

- This cryptographic method has very small key sizes, making it appropriate for real world applications.

- SIKE (Supersingular Isogeny Key Encapsulation) is one example of a promising isogeny-based cryptographic scheme that was broken in 2022.

4.1.2 NIST Post-Quantum Cryptography (PQC) initiative

The National Institute of Standards and Technology (NIST) has taken a principal role in the development of quantum-resistant cryptographic algorithms. Since 2016, NIST has lead an open competition to evaluate and standardize PQC algorithms, aiming to identify algorithms that can replace current systems that are vulnerable to quantum attacks. The competition has gone through multiple phases, with several candidates now in the final stages of being standardized.

NIST's initiative is vital for the global adoption of PQC because it provides a framework for governments, industries, and institutions to transition to secure cryptographic methods. The resulting standards will guide the future of cybersecurity by offering secure and widely accepted cryptographic protocols that resist both classical and quantum computational attacks [27].

4.1.3 Challenges of Post-Quantum Cryptography (PQC) Adoption

While the benefits of PQC in securing systems against quantum threats are clear, its implementation does not come without challenges. Some of the pressing matters in PQC adoption are [28]:

1. **Lack of Knowledge and Expertise**

- Many cybersecurity professionals lack a background in quantum cryptography as it requires an extensive knowledgebase of both classical cryptographic principles and advanced quantum mechanics.

- PQC technologies are highly complex, making implementation and integration into existing systems a daunting task.

- As there is a shortage of specialized talent in the field, quantum security experts are high in demand, leading to a skills gap in organizations.

2. Lack of Education and awareness

- Organizations struggle with the problem of where to start their PQC transition, as clear roadmaps and best practices for replacing current cryptographic systems are not clearly defined and set.

- Companies require expert guidance to implement such transitions as improper deployment could lead to vulnerabilities or inefficient solutions that do not provide the intended security.

- There is a lack of industry-wide training programs, meaning that institutions have to rely on limited resources or consultants to build expertise within the institution.

3. Lack of Clear regulations and standards

- Currently there are no universally accepted guidelines for PQC adoption, which has caused an uncertainty among organizations about which cryptographic algorithms to trust and implement.

- Issues meeting compliance requirements slows down PQC implementation as companies want to ensure that the PQC solutions that they adopt are able to meet future regulatory frameworks.

- There is an urgent need for clearer frameworks to integrate PQC to existing systems, as migrating to quantum-resistant cryptography require significant upgrades, testing and validation to ensure efficiency and security.

4.2 Quantum Key Distribution (QKD) and its Advantages

Quantum Key Distribution (QKD) is a quantum cryptographic technique that uses the principles of quantum mechanics to secure communication channels [22]. Unlike traditional methods of key distribution that rely on the security of the encryption algorithm, Quantum Key Distribution provides an additional layer of security by using the innate properties of quantum states.

4.2.1 How Quantum Key Distribution (QKD) works

Quantum Key Distribution allows two parties – for example, Alice and Bob, to securely exchange cryptographic keys over an insecure channel by encoding the key in quantum states. Unlike traditional key exchange methods that rely on mathematical complexity for security, QKD leverages the fundamental principles of quantum mechanics (that is Superposition, Entanglement and Quantum Interference).

One of the most widely implemented QKD protocols is the BB84 protocol, where the key bits are encoded into polarized photons (that is, particles of light that are able to exist in different quantum states). The encoding process is as follows [29]:

1. **Key encoding and transmission** - Alice creates a random sequence of bits (0s and 1s) and encodes them into the polarization states of individual photons. Each photon can be polarized in different ways, such as horizontal, vertical, or diagonal orientations, corresponding to different bit values.

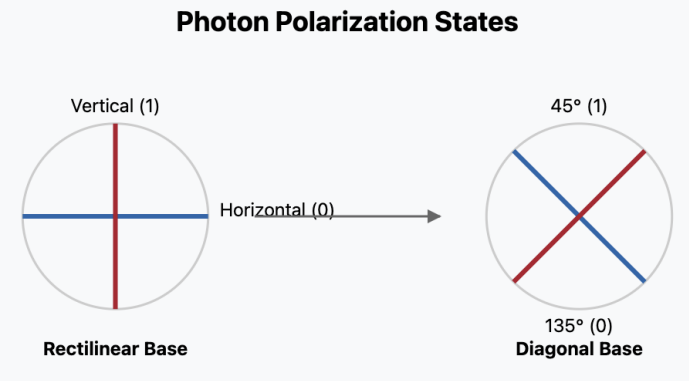

Figure 6: Diagram representing photon polarization states. Source [41]

2. **Key reception and measurement** - Bob receives these photons and randomly chooses a measurement method (horizontal/vertical or diagonal) to determine their polarization. Due to the quantum nature of photons, his measurements may not always align with Alice's original encoding.

3. **Key Reconciliation** - After transmission, Alice and Bob compare a subset of their results over a public channel to determine which measurements were showed in matching bases. The bits from these matching measurements form the key**.**

Some advantages of this method of key exchange are;

- **Unconditional Security:** QKD is based on the laws of quantum mechanics, making secure even against quantum computers.
- **Eavesdropping Detection:** Interception attempts alters the quantum state of photons, creating detectable errors, making easdropping impossible.
- **Resistance to Man-in-the-Middle Attacks:** As the quantum state of photons collapse upon observation, attackers cannot alter the key exchange without being detected.

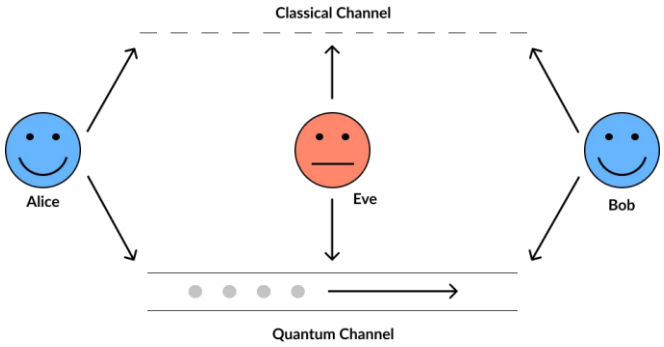

Figure 7: General representation of a QKD setup. Source [42]

4.2.2 Entanglement based Quantum Key Distribution (QKD)

While BB84 and other QKD protocols function over an insecure communication channel, entanglement-based QKD provides an alternative approach that fundamentally secures the channel using quantum entanglement.

Entanglement is a fundamental principle of quantum mechanics, where two quantum particles—typically photons—become linked in such a way that the state of one particle is directly related to the state of the other, no matter how far apart they are. When two particles are entangled, their properties, such as polarization, are correlated in a manner that is not observed in classical physics. For example, if one photon is measured and found to be in a certain polarization state, the other photon will instantaneously "know" its state, even if the two photons are separated by vast distances, theoretically even across the known universe. This phenomenon is often referred to as "spooky action at a distance", a term famously coined by Albert Einstein [22].

In entanglement-based QKD protocols, such as protocol E91, pairs of entangled photons are generated and distributed between the sender (Alice) and the receiver (Bob). The key feature of entanglement is that measuring one entangled photon alters the state of its partner**.** This unique property ensures that if an eavesdropper (Eve) attempts to intercept or measure one of the photons in the entangled pair, the act of measurement will disturb the entanglement. The disturbance will be immediately detectable by Alice and Bob, the communicating parties. This approach strengthens security by ensuring that the key exchange process is inherently protected at the quantum level.

Compared to protocols like BB84, entanglement-based QKD provides a stronger security foundation. However, it also presents its own technical challenges, particularly in the creation, transmission, and detection of entangled particles over long distances [30].

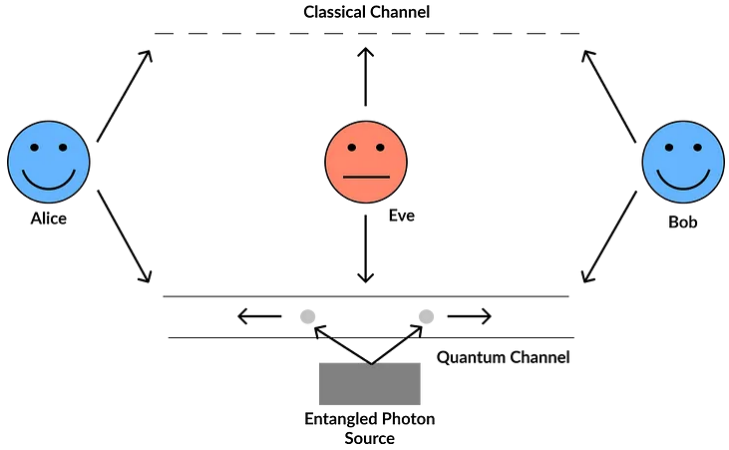

Figure 8: Simple setup representation of the E91 protocol. Source [30]

4.2.3 Limitations of Quantum Key Distribution (QKD)

While Quantum Key Distribution offers high levels of security, it is not without limitations. One of the primary challenges is the range over which QKD can be used. Quantum signals degrade over long distances due to losses in optical fibers, which limits the scalability of QKD in large networks. The existing technology is also expensive and complex to implement, needing specialized instruments like photon detectors and quantum repeaters.

Moreover, QKD is mainly focused on key exchange and does not provide a complete solution for securing data transmission, which means it must be combined with classical encryption algorithms to create a complete secure communication system [31]

4.3 Future of Cybersecurity in the Quantum World

As quantum computing progresses, it will revolutionize many aspects of cybersecurity. The future is expected be a blend of classical and quantum-resistant technologies that will be implemented to defend against emerging threats. It is essential for industries and governments to prepare for a quantum-driven world by adopting quantum-safe encryption protocols and understanding the new challenges that quantum computing has created.

4.3.1 Transitioning to Hybrid Cryptography

Hybrid cryptography is an approach that integrates classical cryptographic systems with quantum-resistant algorithms to provide a layered security model. The main goal of hybrid cryptography is to ensure continued data protection against both classical and quantum threats, especially in the transitional phase before fully quantum-secure cryptographic methods become more common and user-friendly [32].

In a hybrid system, traditional encryption protocols such as RSA, Elliptic Curve Cryptography (ECC), and AES, are combined with post-quantum cryptographic algorithms that have been created to resist attacks from quantum computers. This dual approach enables organizations to maintain compatibility with their existing systems while adopting quantum-resistant security implementations step-wise.

Some of the major advantages of hybrid cryptography are:

- **Fail-safe mechanism** – If a classical encryption method becomes vulnerable to quantum attacks, the quantum-resistant component ensures continued security.

- **Risk mitigation** – Reduces the risks related with a sudden transition to entirely new cryptographic standards.

- **Preventing unexpected vulnerabilities** – A gradual shift can minimize the chances of introducing new security flaws or operational challenges.

As quantum computing capabilities advance, hybrid cryptographic systems will play a critical role in securing sensitive information, communication networks and financial transactions. Governments, financial institutions, and enterprises will likely begin hybrid cryptographic strategies to protect mission-critical data while allowing a seamless transition to fully quantum-safe cryptography. This approach can help to future-proof cybersecurity infrastructure against emerging quantum threats without disrupting any current operations [33].

4.3.2 Quantum resistant BlockChain and Digital Signatures

Blockchain technology and digital signatures depend on cryptographic algorithms such as SHA-256 and ECC for security. However, these methods could be compromised by quantum attacks, threatening the integrity of financial transactions, smart contracts, and identity verification systems.

To address this, researchers are developing quantum-resistant BlockChain protocols that utilize PQC algorithms to secure transactions. Moreover, digital signature which are essential for verifying the authenticity of transactions, are being updated to ensure their resilience in the face of quantum computing. These advancements will be critical in maintaining trust and security in digital systems.

Quantum-resistant BlockChain systems are being designed to incorporate lattice-based, hash-based, and multivariate cryptographic approaches to replace vulnerable traditional methods. These advancements aim to ensure that BlockChain networks remain tamper-proof and continue to offer decentralized security in a quantum era. Furthermore, quantum-secure digital signatures, such as those based on hash-based cryptographic systems like the Lamport signature [34], are being implemented to maintain authentication and integrity in distributed systems.

4.3.3 Quantum Readiness

Quantum readiness refers to the preparedness of organizations and systems to handle the challenges posed by quantum computing. This involves adopting quantum-resistant cryptographic algorithms, upgrading infrastructure to support quantum-safe protocols, and training cybersecurity professionals to understand quantum threats [22].

To ensure long-term cybersecurity, organizations must begin transitioning to quantum-safe technologies today, even though large-scale quantum computers may not be available for years. Organizations should start incorporating quantum-resistant cryptographic frameworks, collaborating with cybersecurity researchers, and implementing post-quantum security updates to ensure resistance against future threats.

Additionally, industries and governments must establish clear transition roadmaps for quantum readiness [35-36]. This includes:

- **Developing quantum-safe cybersecurity policies** to enforce the gradual adoption of quantum-resistant encryption.
- **Encouraging investment in quantum research** to stay ahead of potential security risks.
- **Training IT professionals and cybersecurity experts** to build expertise in post-quantum security frameworks.
- **Establishing quantum-safe communication networks** through early adoption of QKD and other quantum technologies.

Proactive adaptation today will ensure cybersecurity success in the quantum era, guaranteeing that sensitive data remains secure against both present and future threats.

05. Conclusion

5.1 Summary

This report explored the relationship between quantum computing and classical cryptographic systems, focusing on the vulnerabilities that emerging quantum technologies introduce. It discussed the evolution of cryptographic methods from early ciphers to modern symmetric and asymmetric algorithms such as AES, RSA, and ECC. The report highlighted how quantum algorithms like Shor's and Grover's can break or weaken these systems, posing serious threats to the confidentiality, integrity, and authenticity of digital communications.

To address these challenges, the report explored solutions such as Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and hybrid cryptographic approaches. Additionally, it investigated real-world implications across industries like finance, healthcare, and national security, underlining the critical need for proactive cybersecurity transformation.

5.2 Future Recommendations

As quantum computing continues to develop, the following actions are recommended:

- **Adoption of PQC standards**: Organizations should begin transitioning to NIST-recommended quantum-resistant algorithms as part of their long-term cryptographic scheme.

- **Investment in quantum research**: Governments and private sectors should assign sufficient funding toward the development and testing of QKD networks and post-quantum protocols.

- **Hybrid implementations**: In the short-term, hybrid encryption models that combine classical and quantum-resistant methods should be used to ensure layered security.

- **Awareness and training**: Cybersecurity professionals need updated training to understand quantum risks and implement secure migration plans.

Future research should focus on enhancing the efficiency of PQC schemes, overcoming infrastructure limitations in QKD, and developing international standards for post-quantum communication. With appropriate preparation, the transition to a quantum-secure future can be achieved while preserving trust and security in global digital infrastructure.

06. References

[1] National Institute of Standards and Technology, *a Framework for Designing Cryptographic Key Management Systems*, NIST Special Publication 800-130, 2013.

[2] J.Reichental, "*Introduction to Quantum Computing*", Microsoft partnered with LinkedIn, instructed by Dr. Jonathan Reichental, Accessed: Jan 2025 [Online]. Available: https://www.linkedin.com/learning/introduction-to-quantum-computing

[3] ScienceDirect, "*Caesar Cipher*". Accessed: Feb 2025. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/caesar-cipher

[4] National Science and Media Museum Blog, "*Top secret: Ciphers from ancient Greece to the Second World War*". Accessed: Feb 2025 [Online] [Online]. https://blog.scienceandmediamuseum.org.uk/top-secret-ciphers-from-ancient-greece-to-the-second-world-war/

[5] Britannica, "*Vigenère cipher*". Accessed: Feb 2025. [Online]. Available: https://www.britannica.com/topic/Vigenere-cipher

[6] Wikipedia, "*Symmetric-key Algorithm*". Accessed: Feb 2025. [Online]. Available: https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[7] GeeksforGeeks, "*Difference between DES and AES ciphers*". Accessed: Feb 2025. [Online]. Available: https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/

[8] Wikipedia, "*Asymmetric-key Algorithm*". Accessed: Feb 2025. [Online]. Available: https://en.wikipedia.org/wiki/Public-key_cryptography

[9] Tencent Cloud, "*What are the differences between RSA and ECC*?". Accessed: Feb 2025. [Online]. Available: https://www.tencentcloud.com/document/product/1007/39989

[10] Wikipedia, "*IEEE P1363*". Accessed: Feb 2025. [Online]. Available: https://en.wikipedia.org/wiki/IEEE_P1363

[11] Wikipedia, "*Brute Force Attack*". Accessed: Feb 2025. [Online]. Available: https://en.wikipedia.org/wiki/Brute-force_attack

[12] Wikipedia, "*Shor's Algorithm*". Accessed: Feb 2025. [Online]. Available: https://en.wikipedia.org/wiki/Shor%27s_algorithm

[13] GeeksforGeeks, "*Shor's Algorithm Factorization*". Accessed: Feb 2025. [Online]. Available: https://www.geeksforgeeks.org/shors-factorization-algorithm/

[14] Wikipedia, "*Digital Signatures*". Accessed: Mar 2025. [Online]. Available: https://en.wikipedia.org/wiki/Digital_signature

[15] Ascertia, "*How digital signatures evolve in the post quantum word*". Accessed: Mar 2025. [Online]. Available: https://blog.ascertia.com/how-digital-signatures-will-evolve-in-a-post-quantum-world

[16] Builtin, "*BlockChain: What is it, how it works, why it matters*". Accessed: Mar 2025. [Online]. Available:https://builtin.com/blockchain#:~:text=Blockchain%20is%20an%20immutable%20digital,a%20block%20on%20the%20blockchain.

[17] Wikipedia, "*Grover's Algorithm*". Accessed: Mar 2025. [Online]. Available: https://en.wikipedia.org/wiki/Grover%27s_algorithm

[18] The Quantum Insider, "*Quantum Computing Threat to Classical Symmetric Cryptography*". Accessed: Mar 2025. [Online]. Available: https://thequantuminsider.com/2022/07/26/quantum-computing-threat-to-classical-symmetric-cryptography/

[19] Post Quantum, "*Grover's algorithm and its impact on Cybersecurity*". Accessed: Mar 2025. [Online]. Available: https://postquantum.com/post-quantum/grovers-algorithm/

[20] Booz | Allen | Hamilton, "*Cybersecurity in the quantum risk era*". Accessed: Mar 2025. [Online]. Available: https://www.boozallen.com/insights/ai-research/cybersecurity-in-the-quantum-risk-era.html

[21] ABA Banking Journal, "*G7 cybersecurity group urges financial institutions to prepare for quantum computing*". Accessed: Mar 2025. [Online]. Available: https://bankingjournal.aba.com/2024/09/g7-cybersecurity-group-urges-financial-institutions-to-prepare-for-quantum-computing/

[22] J.Reichental, "*Quantum Computing and the future of Cybersecurity*", Microsoft partnered with LinkedIn, instructed by Dr. Jonathan Reichental, Accessed: Jan 2025 [Online] Available: https://www.linkedin.com/learning/quantum-cryptography-and-the-future-of-cybersecurity

[23] Wikipedia, "*National Institute of Standards and Technology*". Accessed: Mar 2025. [Online]. Available: https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

[24] Wikipedia, "*Post-Quantum Cryptography*". Accessed: Mar 2025. [Online]. Available: https://en.wikipedia.org/wiki/Post-quantum_cryptography

[25] The SSL Store, "*What is a hash function in cryptography*? A beginner's guide". Accessed: Mar 2025. [Online]. Available:https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/

[26] KeyFactor, "*Elliptic Curve Cryptography: What is it? How does it work*?" . Accessed: Mar 2025. [Online]. Available: https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/

[27] NIST, "*What is post quantum cryptography*?". Accessed: Mar 2025. [Online]. Available: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

[28] IDEMIA group, "*Key obstacles to Post-Quantum Cryptography (PQC) Adoption*". I[Online]. Available: https://www.idemia.com/insights/key-obstacles-post-quantum-cryptography-pqc-adoption

[29] Wikipedia, "BB84". [Online]. Available: https://en.wikipedia.org/wiki/BB84

[30] Medium – Quantum Computing Group, IIT Roorkee, "*Fundamentals of Quantum Key Distribution – BB84, B92 & E91 protocols*". Accessed: Apr 2025. [Online]. Available: https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols

[31] NSA, "*Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*". Accessed: Apr 2025. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[32] Utimaco, "*NIST's Hybrid Mode Approach to Post-Quantum Computing – why crypto agility is crucial*". Accessed: Apr 2025. [Online]. Available: https://utimaco.com/news/blog-posts/nists-hybrid-mode-approach-post-quantum-computing-why-crypto-agility-crucial

[33] Cloud Security Alliance, "*Will Hybrid Cryptography Protect Us from the Quantum Threat?*" Accessed: Apr 2025. .[Online]. Available: https://cloudsecurityalliance.org/blog/2019/06/17/hybrid-cryptography-quantum-threat

[34]Wikipedia, "*Lamport Signature*". Accessed: Apr 2025. [Online]. Available: https://en.wikipedia.org/wiki/Lamport_signature

[35] National Security Agency (NSA), "*Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*". Accessed: Apr 2025. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[37] ResearchGate, "*The Difference between Bit and Qubit*". Accessed: Apr 2025. [Online]. Available: https://www.researchgate.net/figure/The-Difference-between-Bit-and-Qubit-4_fig1_268485652

[38] SSL2BUY, "*Symmetric vs. Asymmetric Encryption – What are differences?*". Accessed: Apr 2025. [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[39] Medium – Chaitanya Ravuri, "*A General Implementation of Shor's Algorithm*". Accessed: Apr 2025. [Online]. Available: https://medium.com/mit-6-s089-intro-to-quantum-computing/a-general-implementation-of-shors-algorithm-da1595694430

[40] Medium – QUANTUMPEDIA- The quantum encyclopedia, "*Quantum Algorithm (2): Grover's algorithm for unstructured search*". Accessed: Apr 2025. [Online]. Available: https://quantumpedia.uk/quantum-algorithm-2-grovers-algorithm-for-unstructured-search-bd91a7040371

[41] Gordon's STEM blog, "*Quantum Communications – part 3: Photon polarization and Superposition*". Accessed: Apr 2025. [Online]. Available: http://www.gordostuff.com/2024/