GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

Quantum computing and wireless networks security: A survey

Abura Samson *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

GSC Advanced Research and Reviews, 2024, 20(03), 199–230

Publication history: Received on 10 July 2024; revised on 19 August 2024; accepted on 22 August 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.20.2.0308

Abstract

Quantum computing, with its potential to solve complex problems exponentially faster than classical computers, is poised to revolutionize various fields, including wireless networks security. This survey paper provides a comprehensive overview of the intersection between quantum computing and wireless networks security. We examine the potential threats quantum computing poses to classical encryption algorithms, such as RSA and ECC, which are foundational to the security of current wireless networks. Additionally, we explore emerging quantum-resistant cryptographic techniques designed to safeguard against these threats. The paper also discusses quantum key distribution (QKD) as a promising solution for achieving theoretically unbreakable encryption in wireless networks. Furthermore, we review the current state of research in applying quantum computing to wireless network security, including its implications for authentication, confidentiality, and integrity. Finally, we identify challenges and future directions for integrating quantum computing into wireless network security, emphasizing the need for continued research to ensure the resilience of wireless networks in the quantum era.

Keywords: Quantum Computing; Wireless Network Security; Quantum-Resistant Cryptography; Quantum Key Distribution (QKD); Post-Quantum Cryptography; Network Vulnerabilities

1. Introduction

The rapid advancement of quantum computing technology is reshaping the landscape of information security, with profound implications for wireless networks. As quantum computers progress from theoretical constructs to practical machines, they threaten to break the cryptographic algorithms that underpin the security of modern wireless networks [1], [2]. The block diagram of typical quantum and classical computers are shown in Figure 1. Classical encryption methods, such as RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography), which rely on the computational difficulty of certain mathematical problems, are vulnerable to quantum algorithms like Shor's algorithm [3], capable of factoring large integers and solving discrete logarithms exponentially faster than classical algorithms.

Wireless networks, which are increasingly pervasive in our daily lives, from personal devices to critical infrastructure, depend on these classical encryption techniques to ensure secure communication [4]-[6]. The advent of quantum computing thus presents a significant challenge to the confidentiality, integrity, and authenticity of wireless communication [7], [8]. Without adequate countermeasures, the security of wireless networks could be severely compromised, leading to potentially catastrophic consequences for both individuals and organizations.

This survey paper aims to provide a comprehensive overview of the intersection between quantum computing and wireless network security. It will explore the potential threats posed by quantum computing to current cryptographic methods used in wireless networks and examine the emerging field of quantum-resistant cryptography, which seeks to develop algorithms capable of withstanding quantum attacks. Additionally, the paper will delve into Quantum Key

* Corresponding author: Abura Samson

Distribution (QKD), a technology that leverages the principles of quantum mechanics to enable secure key exchange, offering a potential solution to the vulnerabilities exposed by quantum computing.

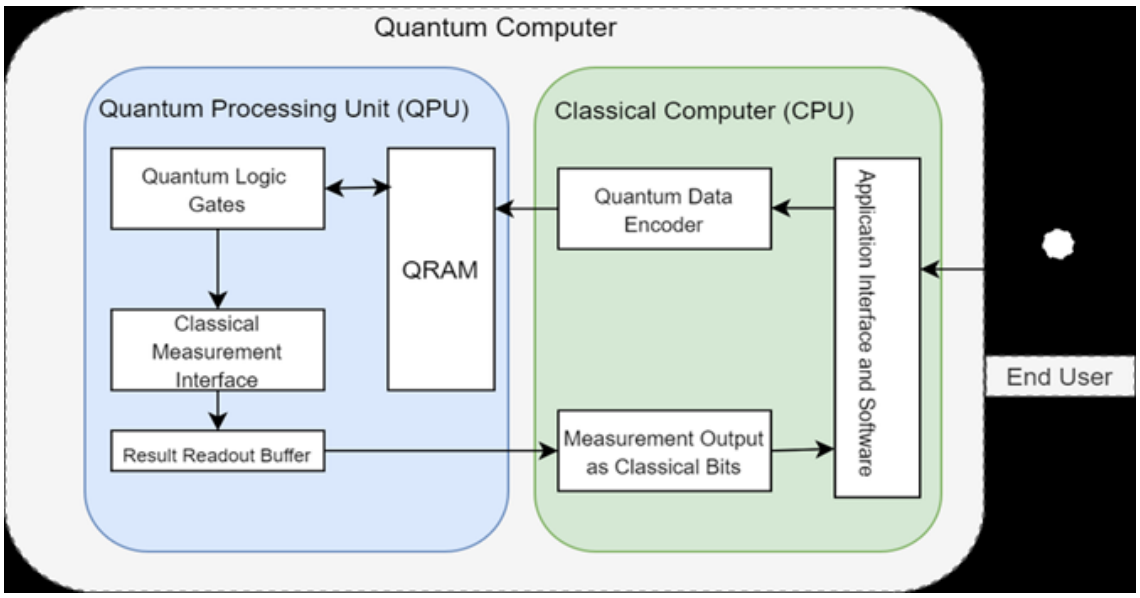

Figure 1 Quantum vs. classical computer

Moreover, the paper will review the state-of-the-art research on the application of quantum computing in enhancing or undermining wireless network security. By analyzing current approaches, challenges, and future directions, this survey aims to provide a solid foundation for researchers and practitioners seeking to understand and address the security implications of quantum computing in wireless networks. The goal is to foster a deeper understanding of the critical need for quantum-safe security measures in the ever-evolving landscape of wireless communication.

1.1. Problem statement

The impending reality of quantum computing poses a significant threat to the security of wireless networks, which are currently safeguarded by cryptographic algorithms considered secure against classical computational attacks. As quantum computers advance, they have the potential to break these classical encryption methods [9], thereby jeopardizing the confidentiality, integrity, and availability of wireless communications. This vulnerability stems from the ability of quantum algorithms, such as Shor's algorithm [10], to efficiently solve mathematical problems that are computationally infeasible for classical computers, such as integer factorization and discrete logarithms. Wireless networks, which are ubiquitous in both personal and professional environments, rely heavily on public-key cryptography for secure key exchange and encryption [11], [12]. The security of widely used cryptographic schemes like RSA and ECC, which underpin secure communication protocols such as Wi-Fi, LTE, and 5G, is based on the assumption that certain mathematical problems are hard to solve with classical computing resources. However, quantum computers threaten to dismantle this assumption, rendering these cryptographic schemes vulnerable to attack.

The primary problem addressed in this survey is the lack of quantum-resistant security measures within current wireless networks [13], [14]. As the quantum computing era approaches, there is an urgent need to develop, evaluate, and implement cryptographic solutions that can resist quantum attacks. This includes not only post-quantum cryptography [15], which aims to create algorithms that remain secure in a quantum world, but also quantum key distribution (QKD) technologies that utilize the principles of quantum mechanics to achieve theoretically unbreakable encryption [16], [17]. The challenge is compounded by the widespread deployment of wireless networks across various domains, from consumer electronics to critical infrastructure, making the transition to quantum-safe security a complex and resource-intensive task. Furthermore, the lack of consensus and standardization in quantum-resistant cryptography presents additional obstacles to ensuring a seamless and secure transition. Therefore, this survey addresses the imminent threat quantum computing poses to the security of wireless networks and the urgent need for quantum-resistant cryptographic solutions.

1.2. Motivation

The accelerating development of quantum computing technology is set to disrupt numerous industries, with profound implications for cybersecurity, particularly in the context of wireless networks. Wireless networks are the backbone of modern communication [18], enabling everything from personal device connectivity to the operation of critical infrastructure. The security of these networks relies heavily on classical cryptographic algorithms, which are designed to be computationally infeasible to break with current technologies. However, the advent of quantum computing threatens to undermine this security paradigm. Quantum computers, leveraging the principles of quantum mechanics [19], are capable of performing calculations that would be practically impossible for classical computers. Algorithms like Shor's and Grover's can, in theory, break the encryption schemes that protect wireless communications, rendering current security measures obsolete [20]. This presents a clear and present danger to the integrity, confidentiality, and availability of wireless networks, which are integral to both personal privacy and national security.

The motivation for this survey paper stems from the urgent need to address the vulnerabilities that quantum computing introduces into wireless network security. As quantum computing moves from theory to practice, the risk of widespread disruption increases. There is a pressing need for the research community to explore and develop quantum-resistant cryptographic methods [21] that can withstand the computational power of quantum computers. Additionally, understanding how quantum computing can be leveraged to enhance wireless network security is crucial for staying ahead of potential threats. This survey aims to consolidate existing research on the intersection of quantum computing and wireless network security, providing a comprehensive resource for researchers, practitioners, and policymakers. By highlighting the challenges and opportunities in this emerging field, this paper seeks to contribute to the development of robust, future-proof security solutions that can protect wireless networks in the quantum era. The ultimate goal is to ensure that the transition to a quantum-powered world does not compromise the security and reliability of the wireless networks that are so critical to modern society.

2. Basics of quantum computing

Quantum computing represents a radical departure from classical computing, leveraging the principles of quantum mechanics to process information in fundamentally different ways. Figure 2 shows some of the key elements in quantum computers. Understanding these key concepts of quantum computing is essential for grasping its potential and implications, particularly in fields like cryptography and network security. The sub-sections below discuss some of the most critical concepts in quantum computing.

2.1. Qubits (Quantum Bits)

The qubit is the fundamental unit of quantum information, analogous to the classical bit [22]. However, unlike classical bits, which can be either 0 or 1, qubits can exist in a superposition of both states simultaneously, as shown in Figure 3. Basically, a qubit can represent a 0, a 1, or any quantum superposition of these states, allowing quantum computers to process a vast amount of information at once. Superposition is what gives quantum computers their incredible parallelism, enabling them to solve certain complex problems much faster than classical computers.

Another key feature of qubits is entanglement, a quantum phenomenon where the state of one qubit becomes intrinsically linked to the state of another, regardless of the distance between them. When qubits are entangled, the measurement of one qubit instantly determines the state of its entangled partner. This property is crucial for quantum computing, as it allows for the creation of highly correlated qubit states, leading to more efficient information processing and error correction methods. Entanglement is also a foundational aspect of quantum algorithms, such as Shor's algorithm for factoring large numbers and Grover's algorithm for searching unsorted databases, which showcase the potential for quantum computers to outperform classical systems.

However, qubits are highly susceptible to decoherence and noise, which can disrupt their delicate quantum states and lead to errors in computation. Maintaining qubits in a stable state long enough to perform meaningful computations is one of the biggest challenges in quantum computing today. Researchers are exploring various physical implementations of qubits, including superconducting circuits, trapped ions, and topological qubits, each with its own advantages and challenges in terms of coherence time, scalability, and error rates. As the field of quantum computing advances, improving the stability and reliability of qubits will be key to unlocking the full potential of this revolutionary technology.

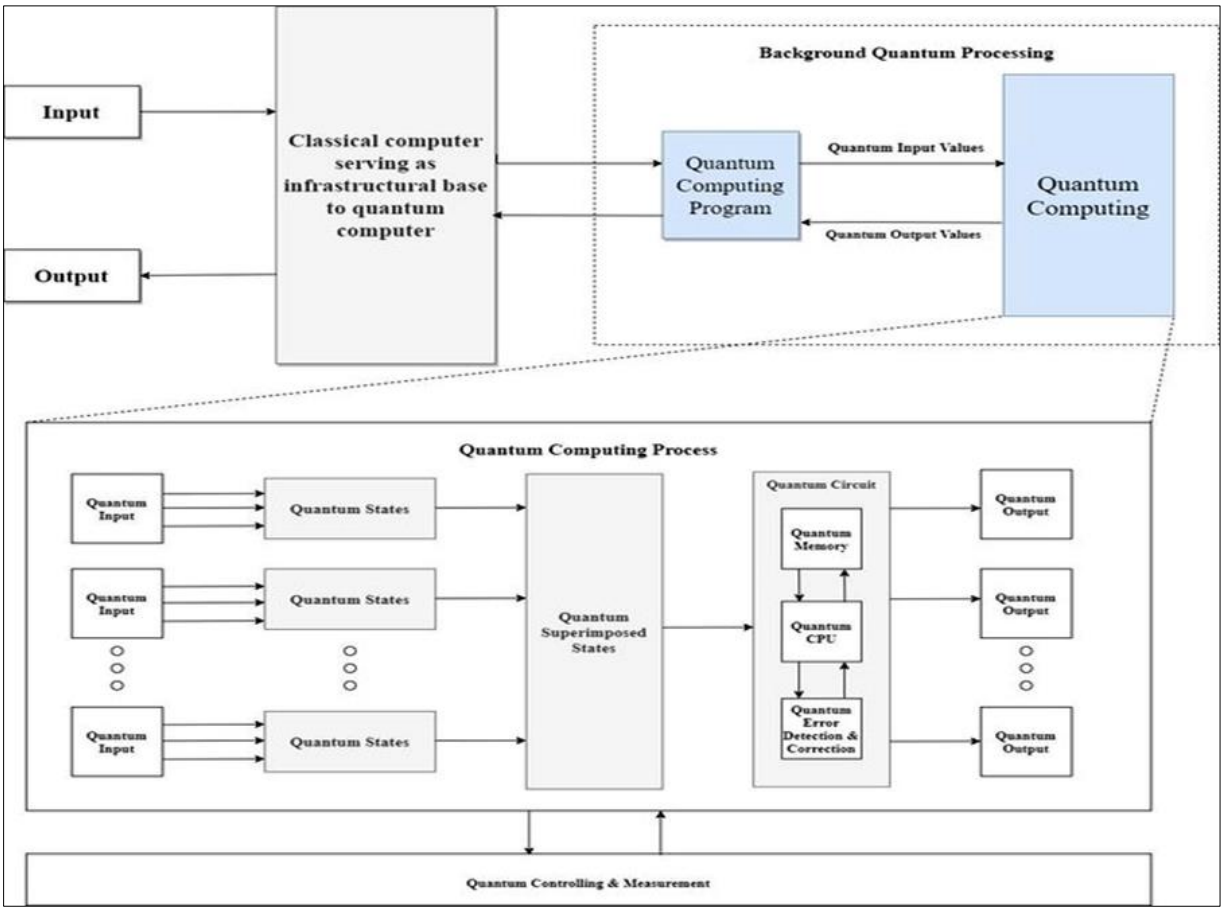

Figure 2 Quantum computer elements

Unlike a classical bit that can be either 0 or 1, a qubit can exist in a superposition of both states simultaneously, thanks to quantum superposition [23]. This allows qubits to perform multiple calculations at once. Additionally, qubits can be entangled with one another, meaning the state of one qubit can be directly related to the state of another, no matter the distance between them. This entanglement, along with superposition, enables quantum computers to solve complex problems more efficiently than classical computers.

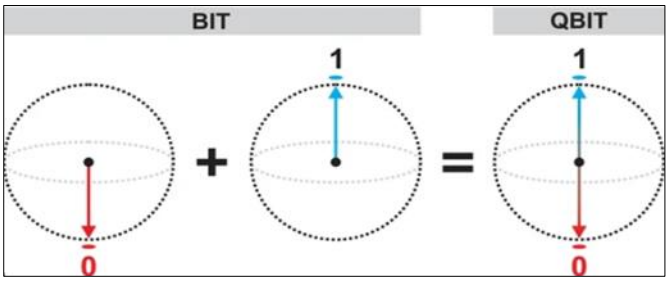

Figure 3 Qubit

The quantum principle of superposition enables quantum computers to perform many calculations in parallel, vastly increasing computational power [24]. Qubits can be realized using various physical systems, including trapped ions, superconducting circuits, and photons.

2.2. Superposition

Superposition is a fundamental principle of quantum mechanics where a quantum system can be in multiple states at once [25], as shown in Figure 4. For a qubit, this means it can be in a combination of the $|0\rangle$ and $|1\rangle$ states [26].

Superposition allows quantum computers to explore multiple possible solutions simultaneously, offering exponential speedup for certain types of computations, such as factoring large numbers.

2.3. Entanglement

Entanglement is a quantum phenomenon where the states of two or more qubits become interconnected such that the state of one qubit directly influences the state of the other(s), regardless of the distance separating them [27], [28].

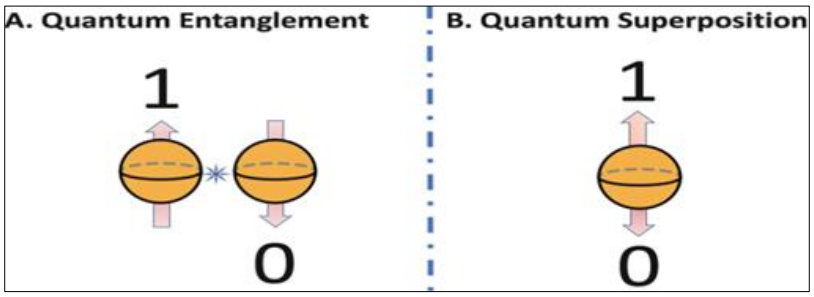

Figure 4 Quantum entanglement and superposition

Entangled qubits remain correlated even when separated by large distances. This property is central to many quantum algorithms and protocols, including quantum teleportation and quantum key distribution [29]. Entanglement is a key resource in quantum computing, enabling tasks like quantum error correction and creating highly secure communication channels.

2.4. Quantum Gates

Quantum gates are the basic operations that manipulate qubits, similar to logic gates in classical computing [30]. These gates perform operations on qubits by changing their states based on the principles of quantum mechanics. The common quantum gates include the Pauli-X, Pauli-Y, Pauli-Z, Hadamard, and CNOT gates [31], as shown in Figure 5. These gates can create superpositions, entangle qubits, and perform rotations in the quantum state space. Quantum gates are combined to form quantum circuits, which are used to implement quantum algorithms.

Quantum gates are the building blocks of quantum circuits, functioning similarly to classical logic gates but operating on qubits instead of bits. The rationale behind quantum gates lies in their ability to manipulate the state of qubits, utilizing principles like superposition and entanglement to perform complex computations.

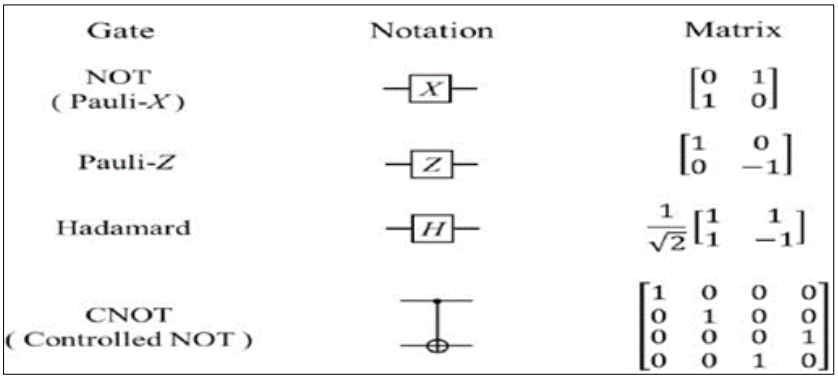

Figure 5 Quantum gates

Unlike classical gates that work on definite binary states, quantum gates operate on the probabilities of qubit states, enabling transformations that can explore multiple computation pathways simultaneously. This capability is crucial for quantum algorithms, as it allows quantum computers to perform tasks like factoring large numbers, searching databases, and simulating quantum systems exponentially faster than classical computers.

2.5. Quantum Algorithms

Quantum algorithms are sets of instructions executed on a quantum computer to solve specific problems more efficiently [32] than classical algorithms. Examples of quantum algorithms include the following:

Shor's Algorithm: An algorithm for factoring large integers in polynomial time [33], which poses a threat to classical cryptographic systems like RSA.

Grover's Algorithm: An algorithm that provides a quadratic speedup for unstructured search problems [34], reducing the number of steps needed to find a solution.

2.6. Quantum Decoherence

Quantum decoherence is the process by which a quantum system loses its quantum properties, such as superposition and entanglement [35], due to interactions with its environment. Decoherence is a major challenge in quantum computing because it causes qubits to lose information, leading to errors in computation [36],[37]. Protecting quantum systems from decoherence is a key focus of quantum error correction research.

2.7. Quantum Speedup

Quantum speedup refers to the advantage quantum algorithms have over their classical counterparts, solving problems in significantly less time [38]. While not all problems can be solved faster on a quantum computer, certain classes of problems (e.g., factoring, database searching) benefit from exponential or quadratic speedup.

2.8. Quantum Key Distribution (QKD)

QKD is a secure communication method [39] that uses quantum mechanics to exchange encryption keys. It ensures security based on the principles of quantum mechanics rather than computational complexity [40]. One of the most famous QKD protocols is BB84, which uses the properties of quantum superposition and entanglement to detect eavesdropping.

2.9. Quantum Supremacy

Quantum supremacy is the point at which a quantum computer can perform a task that is beyond the capability of classical computers within a reasonable time frame [41], [42]. Achieving quantum supremacy is a major milestone, demonstrating the practical power of quantum computing, although it does not necessarily mean quantum computers are ready to solve all practical problems.

2.10. Quantum Error Correction

Quantum error correction involves techniques to protect quantum information from errors due to decoherence and other quantum noise [43], [44], as shown in Figure 6. Quantum error correction codes, such as the surface code, are designed to detect and correct errors without directly measuring the quantum state, thereby preserving the information.

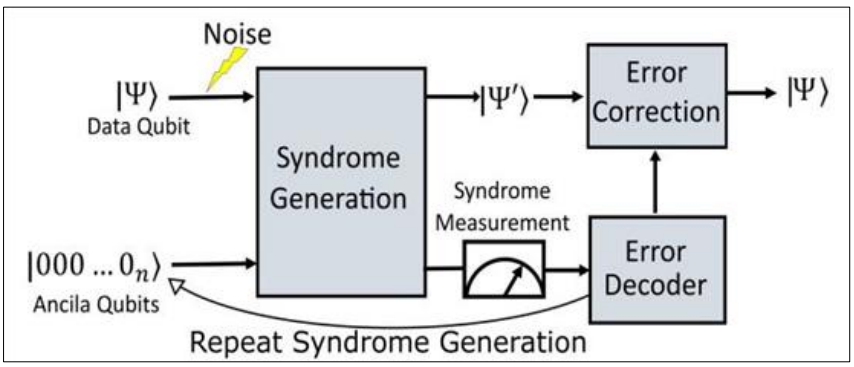

Figure 6 Quantum error correction

Quantum error correction is essential for maintaining the integrity of quantum computations, which are highly susceptible to errors due to the fragile nature of qubits. Unlike classical bits, qubits can be easily disrupted by external

noise, decoherence, or operational imperfections, leading to incorrect results. The rationale for quantum error correction lies in its ability to detect and correct these errors without directly measuring the qubits, which would collapse their quantum states. By encoding quantum information across multiple qubits and using specific quantum codes, errors can be identified and corrected, ensuring the reliability and stability of quantum computations. This is critical for the development of large-scale, fault-tolerant quantum computers capable of solving complex problems that are infeasible for classical computers.

3. Contributions towards wireless networks security

Quantum computing has the potential to significantly enhance wireless network security through several innovative techniques and paradigms. These enhancements can address the vulnerabilities of current classical cryptographic methods and introduce new ways of securing communication channels [45], making wireless networks more robust in the face of evolving cyber threats. Below, we discuss the key ways in which quantum computing can enhance wireless network security:

3.1. Quantum Key Distribution (QKD)

QKD is a method for securely distributing encryption keys using the principles of quantum mechanics [46], as shown in Figure 7. Unlike classical key distribution methods, which rely on the computational difficulty of certain mathematical problems, QKD's security is based on the laws of physics [47]. The most well-known QKD protocol is BB84, introduced by Bennett and Brassard in 1984. QKD allows two parties (typically referred to as Alice and Bob) to share a secret key with provable security. The key is transmitted as quantum bits (qubits) through a quantum channel. These qubits are typically encoded in the polarization states of photons [48], [49]. If an eavesdropper (Eve) attempts to intercept the key, the quantum state of the qubits will be disturbed due to the no-cloning theorem and Heisenberg's uncertainty principle [50], which states that the act of measurement disturbs the quantum system.

This disturbance can be detected by Alice and Bob, who can then abort the key exchange and try again, ensuring that only they share the final key. QKD applications in wireless networks include the following:

- *Secure key management:* QKD can be integrated into wireless networks to securely manage cryptographic keys [51], especially in environments where sensitive data is transmitted, such as military communications or financial transactions.

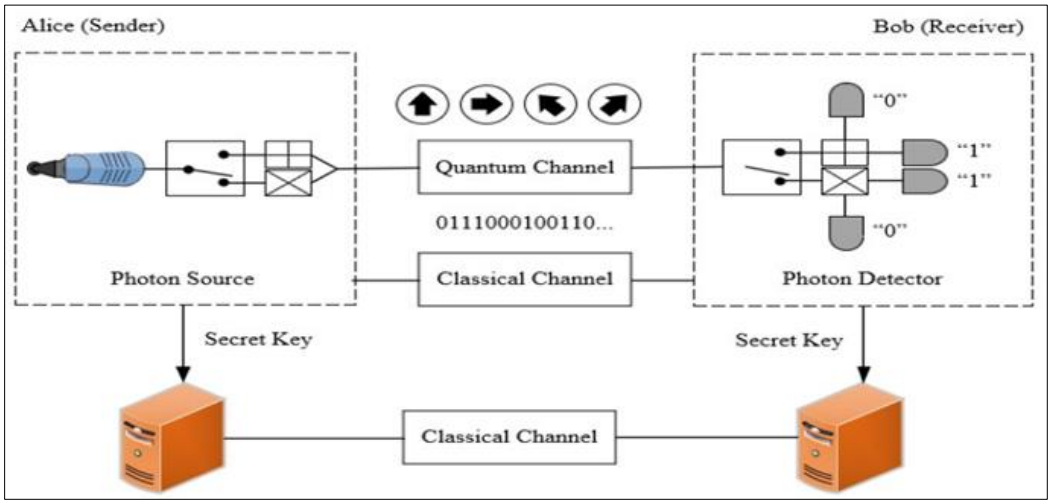

Figure 7 Quantum Key Distribution

- Mobile networks: Implementing QKD in mobile networks (e.g., 5G, future 6G) could protect against threats from both classical and quantum adversaries [52]-[55]. This is particularly relevant for safeguarding communications between base stations, mobile devices, and core networks.
- IoT security: As the Internet of Things (IoT) continues to grow, the need for secure communication between devices becomes critical [56], [57]. QKD can be used to protect the massive amount of data transmitted between IoT devices in smart cities, healthcare, and industrial automation.

3.2. Quantum-resistant cryptography

While QKD offers a new paradigm for key exchange, quantum-resistant cryptography (also known as post-quantum cryptography) focuses on developing cryptographic algorithms that can withstand attacks from quantum computers [58], [59]. These algorithms are based on mathematical problems that are believed to be hard for both classical and quantum computers. Some of the quantum-resistant algorithms include the following:

- Lattice-based cryptography: Relies on the hardness of lattice problems, such as the Learning With Errors (LWE) problem, which is resistant to both classical and quantum attacks [60], [61].
- Code-based cryptography: Based on the difficulty of decoding randomly generated linear codes [62]. An example is the McEliece cryptosystem.
- Multivariate Cryptography: Involves solving systems of multivariate polynomial equations [63], which are difficult to solve even with quantum computers.
- Hash-based cryptography: Utilizes the security of cryptographic hash functions [64], which are also considered secure against quantum attacks when appropriately designed.

Some of the applications of quantum-resistant cryptography in wireless networks include:

- End-to-end encryption: Quantum-resistant algorithms can be used to secure end-to-end communication in wireless networks, ensuring that even if a quantum computer is available to an adversary, the encryption cannot be easily broken [65]-[69].
- Authentication protocols: Quantum-resistant cryptographic methods can secure authentication protocols [70] in wireless networks, preventing unauthorized access and ensuring the integrity of transmitted data.
- Future-proof security: By adopting quantum-resistant cryptography now, wireless networks can be protected against future quantum threats [71], ensuring long-term security and compliance with emerging standards.

3.3. Quantum Random Number Generation (QRNG)

Quantum random number generators use quantum processes to produce truly random numbers [72] as evidenced in Figure 8. Unlike classical random number generators, which are deterministic and can be predicted with enough information, QRNGs leverage quantum phenomena such as photon emission or quantum noise to generate non-deterministic random numbers [73], [74]. QRNG applicability in wireless networks include:

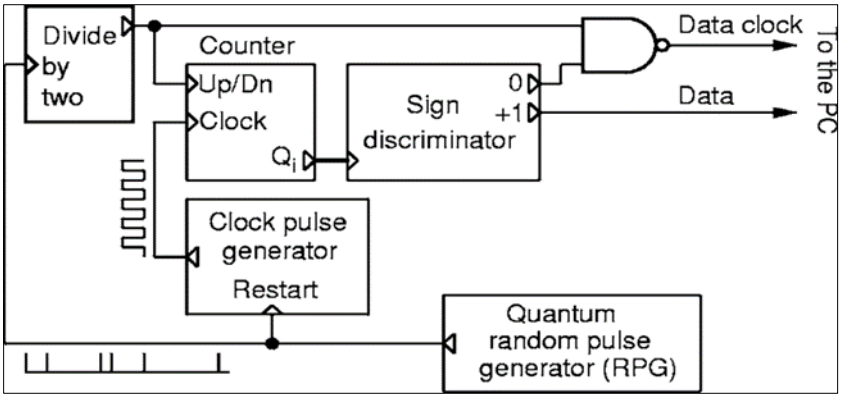

Figure 8 Quantum random number generator

QRNGs typically exploit phenomena such as quantum superposition or the random decay of particles, which are fundamentally indeterminate according to quantum mechanics [75]. This makes the numbers produced by QRNGs truly random, offering higher security and reliability in applications like cryptography, secure communications [76], and complex simulations where unpredictability is crucial. Their use is growing as the demand for stronger encryption and more secure data handling increases

- *Key generation*: Secure cryptographic systems rely on the generation of truly random keys [77]-[82]. QRNGs can be used in wireless networks to produce high-quality random keys, ensuring that encryption keys are not susceptible to prediction or compromise.
- *Session initialization*: QRNGs can be used to generate random session keys for each communication session in wireless networks, making it harder for attackers to perform replay attacks or brute-force attacks [83]-[87].

- *Enhancing protocol security*: The unpredictability of QRNGs can strengthen the security of various protocols in wireless networks, such as secure boot, challenge-response authentication, and anti-jamming techniques [89], [90].

3.4. Quantum-assisted secure communication protocols

Quantum computing can be used to develop new secure communication protocols that enhance the confidentiality and integrity of data transmitted over wireless networks [91], [92] as shown in Figure 9. Quantum-assisted secure communication protocols leverage the principles of quantum mechanics to enhance the security of information exchange. These protocols, such as QKD, utilize quantum states (like the polarization of photons) to generate and share cryptographic keys between parties. Any attempt to intercept or measure the quantum states alters them due to the no-cloning theorem [93], making eavesdropping detectable. This ensures that the communication remains secure, as the keys can be verified and discarded if compromised. Quantum-assisted protocols represent a significant advancement in cryptography [94], offering theoretically unbreakable security against both classical and quantum computing threats. These protocols may combine classical and quantum techniques to offer stronger security guarantees. Some of the examples include:

- *Quantum teleportation for secure data transmission*: Quantum teleportation is a process by which the state of a qubit can be transmitted from one location to another without physically sending the qubit itself [95]-[98]. This technique can be used to transmit encryption keys or sensitive data securely across wireless networks, leveraging entanglement and classical communication.

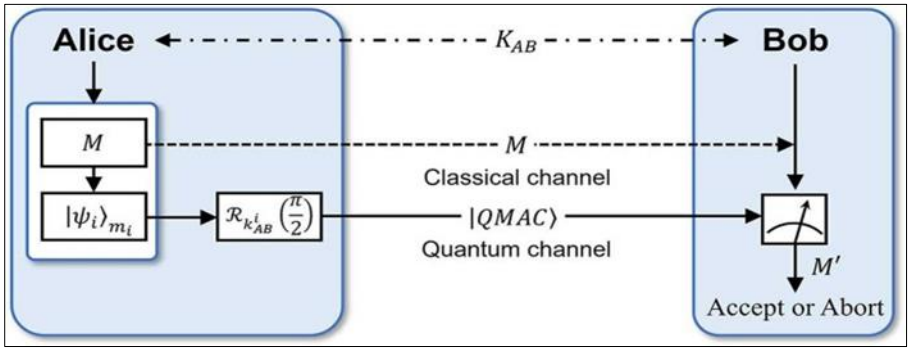

Figure 9 Quantum-assisted secure communication

- Quantum authentication: Quantum authentication protocols use quantum states to verify the identity of users and devices in a wireless network [99[. These protocols can be designed to detect any attempt at tampering or impersonation by an adversary [100], ensuring that only legitimate parties can access the network.

The applications of these quantum-assisted secure communication protocols in computer networks include:

- Device authentication: Quantum-assisted protocols can be used to authenticate devices in a wireless network, ensuring that only authorized devices can communicate, which is crucial for secure IoT deployments [101]-[106].
- Data integrity: By using quantum-assisted methods, wireless networks can ensure the integrity of transmitted data, preventing unauthorized modifications during transmission [107], [108].
- Secure routing: Quantum-enhanced secure routing protocols can be developed to protect the routing of data in wireless networks, particularly in ad-hoc or mesh networks where nodes may be vulnerable to attacks [109]-[112].

3.5. Quantum cryptography for wireless mesh and ad-hoc networks

Wireless mesh and ad-hoc networks are characterized by their decentralized nature and dynamic topologies [113], [114]. These networks are particularly challenging to secure due to the absence of a fixed infrastructure and the reliance on peer-to-peer communication. Entanglement-based QKD can be used in mesh and ad-hoc networks to establish secure communication channels between nodes [115], [116] as demonstrated in Figure 10. This can ensure that even if some nodes are compromised, the overall network security remains intact. Quantum Secure Multi-Party Computation (SMPC) techniques [117] allow multiple parties in a network to jointly compute a function over their inputs while keeping those inputs private.

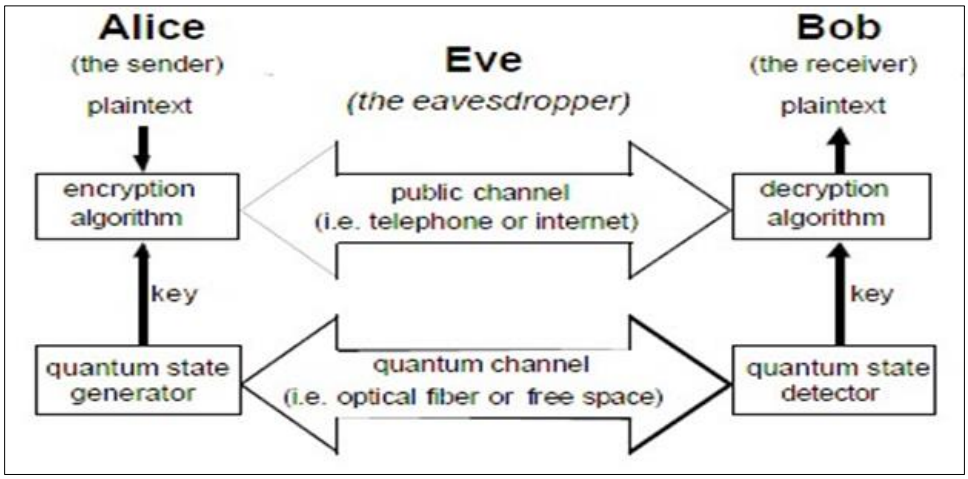

Figure 10 Quantum cryptographic communication system

Quantum computing can enhance SMPC protocols, making them more efficient [118] and secure against both classical and quantum attacks.

Quantum cryptography plays a crucial role in enhancing security in wireless mesh and ad-hoc networks, which are inherently vulnerable to eavesdropping and attacks due to their decentralized and dynamic nature. By leveraging principles like quantum key distribution (QKD), quantum cryptography ensures that cryptographic keys are exchanged in a manner that is theoretically immune to interception. In QKD, any attempt to eavesdrop on the key exchange process causes detectable disturbances in the quantum states, alerting the network to potential security breaches. This provides a level of security that is unattainable with classical cryptographic methods, making quantum cryptography an essential tool for securing communications in wireless mesh and ad-hoc networks, where traditional security measures may fall short. The applications include the following:

- *Secure communication in tactical networks*: Military and emergency response operations often rely on ad-hoc wireless networks [119]. Quantum-enhanced security can protect these networks from interception and disruption, ensuring reliable communication in critical situations [120], [121].
- *Collaborative IoT systems*: In collaborative IoT environments, where devices need to share information securely [122], quantum-enhanced security can protect data privacy and ensure that collaborative computations are performed securely [123].

3.6. Quantum machine learning for anomaly detection

Quantum machine learning (QML) combines quantum computing with machine learning techniques [124] to process and analyze large datasets more efficiently than classical methods, as demonstrated in Figure 11. This anomaly detection harnesses the power of quantum computing to identify unusual patterns or outliers in data more efficiently than classical methods. By leveraging quantum algorithms like quantum support vector machines or quantum neural networks, QML can process and analyze large datasets at much faster rates, exploring high-dimensional spaces more effectively [125]-[129]. This enhanced computational capability enables the detection of subtle anomalies that might be missed by traditional techniques, making QML particularly valuable in fields like cybersecurity, fraud detection, and complex system monitoring, where identifying rare or unexpected events [130] is crucial for maintaining security and stability. In the context of wireless network security, QML can be used to detect anomalies and potential security breaches. Applications of quantum machine learning-based anomaly detection include the following:

- *Intrusion detection*: QML can be used to develop advanced intrusion detection systems (IDS) that can identify unusual patterns of behavior in network traffic [131], which may indicate a security breach.
- *Fraud detection*: In financial or e-commerce transactions conducted over wireless networks, QML can be applied to detect fraudulent activities in real-time, reducing the risk of financial loss [132].

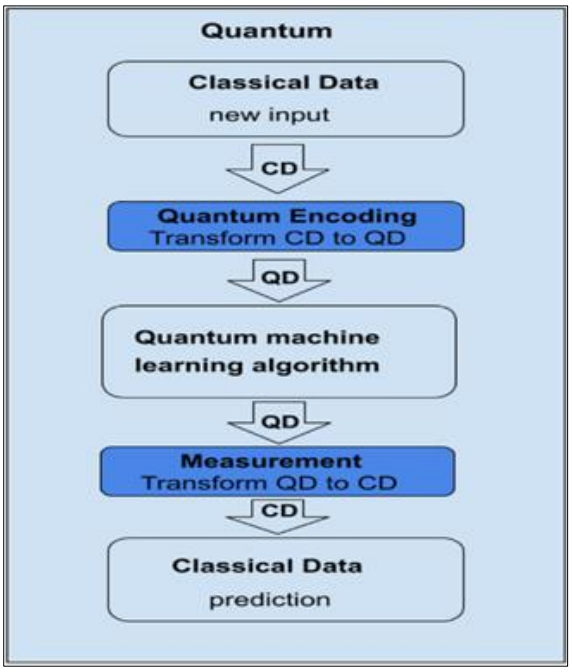

Figure 11 Quantum machine learning

- *Adaptive security mechanisms*: QML algorithms can adapt to new types of attacks by learning from past incidents [133], providing wireless networks with the ability to evolve their security measures in response to emerging threats.

3.7. Quantum secure routing protocols

Routing in wireless networks, especially in mobile ad-hoc networks (MANETs), is a critical aspect of network performance and security [134]. Quantum computing can be leveraged to develop secure routing protocols that are resistant to quantum-based attacks [135]. The various approaches in this perspective include:

- *Quantum cryptography-based routing*: Routing protocols can be enhanced using quantum cryptographic techniques, ensuring that routing information is transmitted securely [136] and cannot be tampered with by malicious nodes.
- *Quantum entanglement in routing decisions*: Quantum entanglement can be used to establish secure, verifiable connections between nodes in a network [137], ensuring that data is routed through trusted paths.

The applications of quantum secure routing protocols include the following domains.

- Secure communications in MANETs: Quantum-secure routing can be critical in military and emergency communications [138], where the integrity and confidentiality of routing information are paramount.
- Resilient IoT networks: In IoT networks with dynamic topologies, quantum-secure routing can ensure that data is transmitted securely, even as network configurations change [139].

3.8. Quantum-enhanced jamming resistance

Wireless networks are susceptible to jamming attacks, where an adversary deliberately interferes with the communication channels to disrupt network operations [140]-[142]. Quantum-enhanced techniques can be employed to improve the resistance of wireless networks to such attacks. Its various approaches include:

- *Quantum signal processing*: Quantum signal processing techniques can be used to detect and mitigate jamming signals more effectively than classical methods, ensuring the continuity of communication in hostile environments.
- *Quantum cryptographic techniques*: These can be used to secure the control channels of wireless networks [143], making it difficult for adversaries to target specific frequencies for jamming.

Quantum-enhanced jamming resistance applications include the following:

- Military and defense communications: Quantum-enhanced jamming resistance is particularly valuable in military applications [144], where secure and reliable communication is essential.
- Critical infrastructure protection: Protecting the communication channels of critical infrastructure (e.g., power grids, transportation systems) from jamming is crucial [145], and quantum techniques can offer robust solutions.

Quantum computing offers a range of powerful tools and techniques that can significantly enhance the security of wireless networks [146]. From quantum key distribution and quantum-resistant cryptography to quantum-enhanced anomaly detection and secure routing, these advancements provide a foundation for building more secure and resilient wireless communication systems [147], [148]. As quantum technologies continue to mature, their integration into wireless networks will become increasingly critical to safeguarding against both current and future threats, ensuring the continued reliability and security of these essential communication infrastructures.

4. Dangers posed by quantum computing in wireless network security

Quantum computing, while promising groundbreaking advancements across various fields, poses significant dangers to the security of wireless networks. These dangers stem primarily from the quantum computer's ability to solve complex mathematical problems [149] that underlie the security mechanisms of current cryptographic systems. As quantum computing matures, the integrity, confidentiality, and availability of wireless networks may be severely compromised [150]-[155]. The sub-sections below explore these dangers in detail, outlining the potential threats and their implications for wireless network security.

4.1. Breaking classical cryptographic algorithms

Public-key cryptographic systems, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on the difficulty of solving specific mathematical problems [155], like factoring large integers and computing discrete logarithms. These problems are computationally infeasible to solve with classical computers within a reasonable timeframe, forming the basis of the security for many wireless communication protocols.

- *Shor's algorithm*: Quantum computing poses a direct threat to these cryptographic systems through Shor's algorithm, which efficiently factors large integers and solves discrete logarithms in polynomial time [156]-[159]. A sufficiently powerful quantum computer could, therefore, break RSA and ECC, rendering them insecure.

The Implications for wireless networks security are as follows.

- *Encryption compromise*: Wireless networks widely use RSA and ECC for key exchange [160], digital signatures, and encryption. If these algorithms are broken by quantum computers, adversaries could decrypt intercepted wireless communications, leading to massive breaches of confidentiality [161].
- *Authentication breach*: Digital signatures, which rely on public-key cryptography, are used to authenticate users and devices in wireless networks [162]-[164]. A quantum attack could forge signatures, enabling unauthorized access to the network and potentially leading to widespread impersonation and data breaches [165].
- *Data integrity attacks*: Integrity checks in wireless networks are often secured using cryptographic hashes and digital signatures [166], [167]. Quantum computers could tamper with these, altering data without detection, which could be catastrophic in scenarios like financial transactions or command-and-control systems.

4.2. Quantum attacks on symmetric cryptography

Grover's algorithm is a quantum algorithm that provides a quadratic speedup for searching unsorted databases [168]. Applied to symmetric key cryptography, it can reduce the effective key length of encryption algorithms by half. For example, a 128-bit key used in AES (Advanced Encryption Standard) encryption, considered secure under classical assumptions, could be reduced to an effective security level of 64 bits under a quantum attack, making it susceptible to brute-force attacks by a quantum computer [169]-[171]. The implications for wireless networks security are as follows:

- *Weakened encryption*: Symmetric encryption is commonly used in wireless networks for securing data in transit [172], such as in WPA2 and WPA3 protocols for Wi-Fi. A quantum attack reducing the effective key length could make these protocols vulnerable to decryption [173], exposing sensitive data to interception and misuse.

- *Exacerbated security vulnerabilities*: Many legacy systems and IoT devices use outdated encryption standards with already minimal key lengths [174]-[177]. Quantum attacks could easily exploit these weaknesses, leading to widespread security vulnerabilities in wireless ecosystems.

4.3. Threats to Quantum Key Distribution (QKD) systems

While QKD promises theoretically unbreakable encryption based on the principles of quantum mechanics, practical implementations face challenges, such as imperfect photon sources, detector inefficiencies [178], and transmission losses, which could be exploited by sophisticated quantum attacks. Even if the quantum aspect of QKD is secure, the classical components (e.g., the transmission of classical data over a conventional channel) remain vulnerable to side-channel attacks [179], where an adversary could extract sensitive information by observing these channels. The implications for wireless networks security includes the following:

- *Overconfidence in QKD*: As organizations start deploying QKD in wireless networks, particularly in sensitive applications like military or financial communications [180], over-reliance on its perceived invulnerability could lead to neglect of potential side-channel vulnerabilities [181], creating openings for quantum-enhanced adversaries to exploit.
- *Complexity and interoperability issues*: The integration of QKD into existing wireless infrastructures can be complex [182], leading to potential mis-configurations and interoperability issues that could introduce new security risks.

4.4. Quantum-assisted eavesdropping

Quantum computers can process multiple possibilities simultaneously due to superposition, which could enhance an adversary's ability to eavesdrop on wireless communications more effectively than classical methods [183]. Figure 12 demonstrates how this attack can be executed. In addition, quantum signal processing techniques could allow adversaries to extract useful information from noisy or encrypted wireless signals [184] that classical techniques cannot decipher. The consequences of this include:

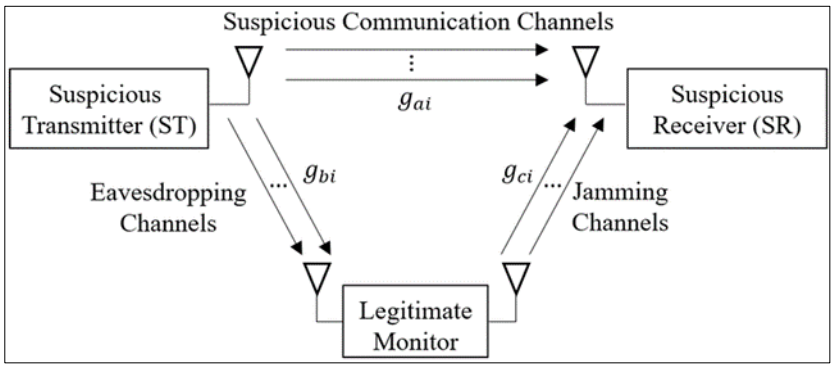

Figure 12 Quantum-assisted eavesdropping

Basically, quantum-assisted eavesdropping involves the use of quantum technologies to intercept and decode information from secure quantum communication channels [185], [186]. In theory, quantum eavesdropping could exploit the vulnerabilities of quantum systems, such as errors in the implementation of quantum key distribution (QKD) protocols [188], [189]. However, due to the principles of quantum mechanics, specifically the no-cloning theorem and the fact that measurement of quantum states disturbs them, any attempt to eavesdrop typically alters the quantum states involved, making detection of the intrusion likely. Thus, while quantum-assisted eavesdropping [190] presents potential risks, the inherent properties of quantum communication also offer robust defenses against such threats.

- *Interception of sensitive communications*: Quantum-assisted eavesdropping could allow adversaries to intercept and decode sensitive communications in wireless networks [191], including voice, video, and data transmissions, compromising privacy and leading to the unauthorized disclosure of confidential information.
- *Targeted attacks*: In military or critical infrastructure contexts, quantum-assisted eavesdropping could be used to gather intelligence on strategic communications [192], leading to targeted attacks and potentially devastating consequences.

4.5. Quantum-powered Denial of Service (DoS) attacks

Quantum computing could be used to launch more sophisticated and powerful DoS attacks by rapidly generating traffic patterns that exhaust the resources of wireless networks, such as bandwidth, processing power, and memory [193], [194]. Quantum algorithms could optimize the amplification of attack vectors, making it more difficult for wireless networks to detect and mitigate DoS attacks in real time [195]. The implications for wireless networks are as follows:

- *Network disruption*: Quantum-powered DoS attacks [196] could cripple wireless networks, leading to significant service outages. In critical applications like healthcare (e.g., wireless medical devices) or emergency services (e.g., communication networks used by first responders), this could have life-threatening consequences [197].
- *Economic impact*: In commercial settings, prolonged or frequent DoS attacks on wireless networks could result in substantial financial losses due to disrupted operations, loss of customer trust, and the costs associated with restoring service and strengthening defenses [198].

4.6. Quantum-enhanced cryptanalysis

Beyond Shor's and Grover's algorithms, quantum computing may facilitate the development of new algorithms specifically designed for cryptanalysis [199]. These algorithms could be used to discover weaknesses in existing cryptographic protocols or even to develop new, more efficient attack methods [200]. In addition, even protocols that are not directly broken by quantum computers might become vulnerable if quantum-enhanced cryptanalysis finds new weaknesses in the mathematical structures underlying them. The implications include the following:

- *Legacy systems at risk*: Many wireless networks, especially those supporting legacy systems, use older encryption protocols that may already have vulnerabilities [201], [202]. Quantum-enhanced cryptanalysis could quickly uncover and exploit these weaknesses, leading to widespread breaches.
- *Undermining of emerging standards*: Newer wireless security standards, such as WPA3, could also be at risk if quantum-enhanced cryptanalysis techniques discover weaknesses that were not anticipated during their design [203], undermining the security of networks that adopt these standards.

4.7. Long-term data security threats

Adversaries might begin harvesting encrypted data transmitted over wireless networks today, with the intention of decrypting it once quantum computers become powerful enough [204], [205]. Sensitive data, such as financial records, personal communications, or government secrets, that is intercepted today could be decrypted in the future [206], leading to breaches of confidentiality even years after the data was originally transmitted. The repercussion for wireless networks security are as follows:

- *Sensitive data exposure*: Wireless networks that transmit long-term sensitive data, such as government communications, intellectual property, or personal health information, are particularly at risk from this type of attack [207], [208]. Once quantum computers are capable of breaking the encryption, previously secure data could be exposed, leading to severe privacy and security breaches.
- *Regulatory and compliance issues*: Organizations may face regulatory and compliance challenges if it becomes known that their past communications are now vulnerable due to quantum attacks [209], potentially resulting in legal and financial repercussions.

4.8. Threats to emerging wireless technologies

As 5G networks are deployed, they introduce new security features and complexities [210]. However, these networks also rely on public-key cryptography for securing communications, which quantum computing could compromise [211], [212]. Future wireless technologies, such as 6G, are expected to integrate even more advanced features, such as AI-driven network management and IoT ecosystems [213]. The potential quantum threats to the cryptographic algorithms used in these networks could undermine their security foundations before they are fully realized. The implications are as follows:

- *Undermining network integrity*: Quantum computing could threaten the integrity of the security protocols [214] that are critical to the functioning of 5G and future networks, potentially leading to vulnerabilities that adversaries could exploit to disrupt services or compromise data.

- *Increased attack surface*: The advanced capabilities of 5G and beyond, such as network slicing and massive IoT connectivity, also increase the attack surface [215], [216]. Quantum threats could exploit these new attack vectors, leading to more sophisticated and damaging attacks on wireless networks.

4.9. Economic and strategic risks

As organizations and governments attempt to mitigate quantum threats, the costs of upgrading infrastructure, implementing quantum-resistant cryptography [217], and developing new security protocols could be substantial. Nations or companies that fail to adapt to the quantum threat landscape may face significant competitive disadvantages, both economically and in terms of national security. The strategic implications include the following:

- National security risks: Quantum computing poses a strategic risk to national security if adversaries gain the ability to break encryption protecting military communications [218], government secrets, and critical infrastructure.
- Global power shifts: Nations that achieve quantum supremacy (the ability to solve problems no classical computer can) [219] may gain a significant strategic advantage, potentially leading to shifts in global power dynamics and increased geopolitical tensions.

It is evident that the advent of quantum computing represents a double-edged sword for wireless network security. While it holds the potential to revolutionize secure communications through quantum-enhanced protocols, it also poses significant dangers that could undermine the very foundations of wireless network security as we know it. Breaking classical cryptographic algorithms [220], enhancing eavesdropping capabilities, and enabling new forms of attacks are just some of the risks posed by quantum computing. To mitigate these threats, it is crucial for the wireless network security community to invest in the development of quantum-resistant cryptographic algorithms [221], enhance the security of emerging wireless technologies, and remain vigilant about the evolving quantum threat landscape. Failure to do so could lead to a future where the confidentiality, integrity, and availability of wireless communications are severely compromised, with far-reaching consequences for both individuals and organizations.

5. Probable solutions

As quantum computing continues to advance, it is crucial to develop and implement strategies to mitigate the security risks it poses to wireless networks. These solutions involve a combination of new cryptographic approaches, enhancements to existing protocols, and forward-thinking strategies that anticipate the evolution of quantum technology. The sub-sections below discuss these solutions extensively, covering both immediate actions and long-term strategies to secure wireless networks against the quantum threat.

5.1. Quantum-resistant cryptography

Post-quantum cryptography refers to cryptographic algorithms designed to be secure against both classical and quantum computers [222]. The goal is to develop algorithms that can replace current public-key cryptosystems (e.g., RSA, ECC) that are vulnerable to quantum attacks [223]. Key approaches include lattice-based cryptography, hash-based cryptography, code-based cryptography, multivariate polynomial cryptography, and isogeny-based cryptography [224], [225]. These algorithms rely on mathematical problems that are believed to be resistant to quantum attacks. The implementations include the following:

- *Upgrading encryption protocols*: Wireless networks need to transition from classical cryptographic algorithms to Post-Quantum Cryptography (PQC) algorithms [226]. This includes updating protocols like WPA3 and TLS (Transport Layer Security) to incorporate quantum-resistant encryption methods.
- *Standards development*: Organizations such as the National Institute of Standards and Technology (NIST) are working on standardizing PQC algorithms. Wireless network security protocols [227] should be updated to comply with these emerging standards as they become available.

Some of the challenges and considerations include:

- *Performance impact*: PQC algorithms often have larger key sizes and higher computational requirements than classical algorithms [228], [229]. Wireless networks, particularly in resource-constrained environments like IoT, need to balance security with performance.
- *Interoperability*: Transitioning to PQC may introduce interoperability issues with legacy systems that still rely on classical cryptography [230]. Ensuring smooth integration during the transition period is critical.

5.2. Hybrid cryptographic systems

A practical approach during the transition to PQC is to use hybrid encryption schemes that combine classical and quantum-resistant algorithms [231]. This dual-layer security approach provides immediate protection against classical attacks while preparing for future quantum threats. Hybrid systems allow wireless networks to gradually transition to PQC without disrupting existing infrastructure [232]. As PQC standards mature, the reliance on classical cryptography can be reduced or eliminated. The applications in wireless networks include the following:

- *Secure key exchange*: In hybrid systems, key exchange protocols [233] could use both classical and PQC algorithms to ensure that even if one algorithm is compromised, the other provides a fallback layer of security.
- *Digital signatures*: Hybrid digital signature schemes can be implemented where messages are signed with both classical and quantum-resistant signatures [234], ensuring authenticity even if one method is broken by quantum computing.

However, the following considerations need to be taken:

- Complexity: Hybrid cryptographic systems are more complex to design and implement [235], requiring careful consideration of how different algorithms interact and how to manage key distribution and verification processes.
- Performance overheads: The use of two cryptographic methods in tandem may lead to performance overheads [236], particularly in wireless networks with limited bandwidth or processing power.

5.3. Quantum Key Distribution (QKD) integration

Quantum key distribution leverages the principles of quantum mechanics to enable two parties to share a secret key securely [237]. Any attempt to eavesdrop on the key exchange process disturbs the quantum states of the particles, alerting the communicating parties to the presence of an interceptor [238]. The most well-known QKD protocol is BB84, but there are several others, including E91, B92, and continuous-variable QKD. These protocols differ in how they encode and transmit quantum information. The probable applications in wireless networks are as follows:

- *Secure channel establishment*: QKD can be used to establish secure communication channels [239] in wireless networks, particularly in high-security environments such as military communications, financial transactions, and critical infrastructure control systems.
- *Authentication and integrity*: In addition to key distribution, QKD can be integrated with classical cryptographic techniques to enhance the authentication and integrity of data transmitted over wireless networks [240].

Some of the challenges and considerations include:

- *Infrastructure requirements*: QKD requires specialized quantum communication infrastructure, such as quantum repeaters and entangled photon sources [241], which may be challenging to deploy in existing wireless networks.
- *Distance and mobility limitations*: Current QKD implementations are limited in terms of distance and mobility [242], making them more suitable for fixed infrastructure networks than for highly mobile or geographically dispersed wireless networks.

5.4. Enhanced key management strategies

Regularly rotating cryptographic keys can reduce the risk of long-term data exposure [243], [244]. If an encryption key is compromised by a quantum attack, only the data protected by that specific key would be at risk. Frequent key rotation minimizes the impact. In addition, forward secrecy can ensure that even if a long-term key is compromised, past communication sessions remain secure [245]. This is particularly important for wireless networks where sensitive data is often transmitted in real-time. The applications in wireless networks include:

- *Dynamic key management:* Wireless networks, especially those with mobile or IoT devices, should implement dynamic key management systems [246] that can adapt to changing network conditions and threats.
- *Secure key distribution*: Implementing secure, quantum-resistant key distribution mechanisms is essential for maintaining the security of wireless communications [247], [248]. This includes the use of PQC algorithms for key exchange and the integration of QKD where feasible.

However, the following issues need to be put into considerations:

- *Scalability:* Effective key management in large-scale wireless networks requires scalable solutions that can handle the complexity of key distribution, rotation, and renewal across numerous devices and nodes [249].
- *Resource constraints:* Many wireless devices, particularly IoT devices, have limited processing power and memory, which can make advanced key management strategies challenging to implement [250, [251].

5.5. Quantum-resistant protocol design

Wireless networks will need new communication protocols specifically designed to be quantum-resistant [252]. This involves rethinking how data is encrypted, transmitted, and authenticated in a quantum computing environment. Figure 13 gives an illustration of the quantum-resistant transport layer security. Existing protocols should be hardened against quantum attacks [253]. This could involve increasing key sizes, adopting PQC algorithms, and incorporating quantum-safe primitives into protocol designs.

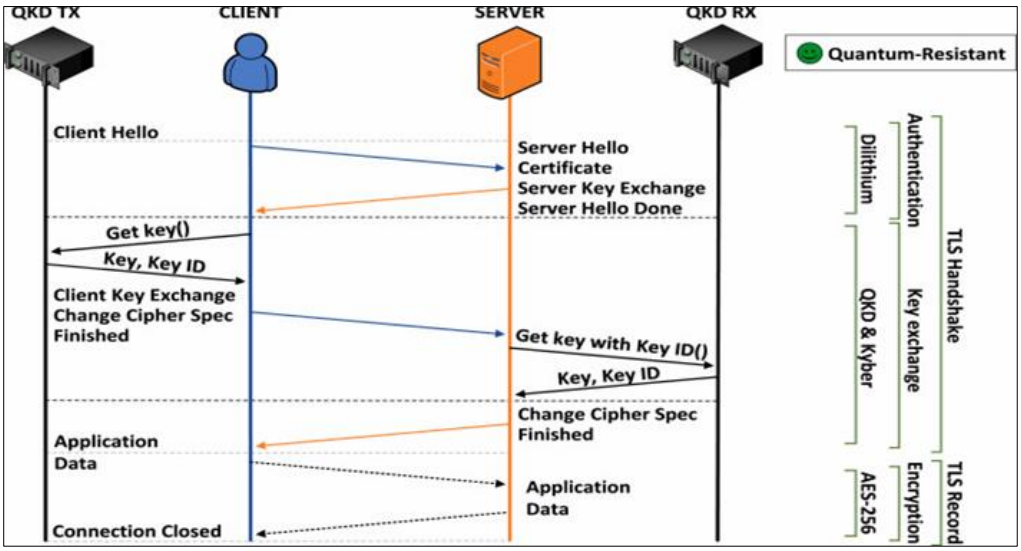

Figure 13 Quantum-resistant transport layer security

Quantum-resistant Transport Layer Security (TLS) is an adaptation of the standard TLS protocol designed to secure communications against potential threats posed by quantum computers [254]. Traditional TLS relies on cryptographic algorithms that could be compromised by quantum computing advancements, such as RSA and ECC, which are vulnerable to Shor's algorithm [255], [256]. Quantum-resistant TLS incorporates post-quantum cryptographic algorithms, like lattice-based or hash-based schemes, to provide encryption and authentication mechanisms that are believed to be secure against quantum attacks. By integrating these quantum-resistant algorithms, TLS aims to future-proof secure data transmission [257], ensuring that sensitive information remains protected even as quantum computing technology evolves.

The applications in wireless networks security include:

- *WPA3 enhancements*: While WPA3 is currently the standard for securing Wi-Fi networks [258], future versions should incorporate quantum-resistant elements, such as PQC-based key exchange and digital signatures.
- *IoT protocols*: Protocols like MQTT (Message Queuing Telemetry Transport) [259] and CoAP (Constrained Application Protocol) [260], used in IoT environments, should be updated to include quantum-resistant security features to protect the vast number of connected devices.

However, the following issues need to be considered:

- *Backward compatibility:* Ensuring that quantum-resistant protocols remain compatible with existing devices and systems is crucial for a smooth transition [261], [262]. This may involve supporting both classical and quantum-resistant modes of operation during the transition period.
- *Standardization:* The development of quantum-resistant protocols should align with emerging standards to ensure widespread adoption and interoperability across different wireless network environments [263].

5.6. Quantum-resistant anomaly detection

Wireless networks should incorporate quantum-resistant algorithms into their anomaly detection systems to detect and mitigate threats that might exploit quantum computing capabilities. In addition, machine learning algorithms [264] that can analyze large volumes of data in real-time, looking for patterns indicative of quantum-enhanced attacks, should be integrated into network monitoring tools. The applications in wireless networks are as follows:

- *Intrusion Detection Systems (IDS):* IDS in wireless networks should be updated to detect the unique signatures of quantum-assisted attacks [265], such as those that might target cryptographic weaknesses or exploit newly discovered vulnerabilities.
- *Real-time monitoring:* Continuous, real-time monitoring of wireless network traffic using quantum-resistant anomaly detection algorithms can help identify and respond to threats more effectively [266].

This requires special emphasis on the following issues:

- *False positives:* Advanced anomaly detection systems must be carefully tuned to avoid generating false positives [267], which can lead to unnecessary disruptions and increased operational costs.
- *Integration with existing tools:* Quantum-resistant anomaly detection systems should be integrated with existing security tools and protocols to provide a comprehensive defense strategy [268].

5.7. Secure software and firmware updates

Wireless devices should implement secure boot processes that verify the integrity and authenticity of the firmware using quantum-resistant cryptographic methods [269]. In addition, software and firmware updates should be signed using PQC-based digital signatures to ensure they have not been tampered with during transmission or installation. Figure 14 gives an illustration of the secure firmware update process. The rationale behind secure software and firmware updates is to protect systems from vulnerabilities and potential cyber threats that could arise from outdated or compromised code.

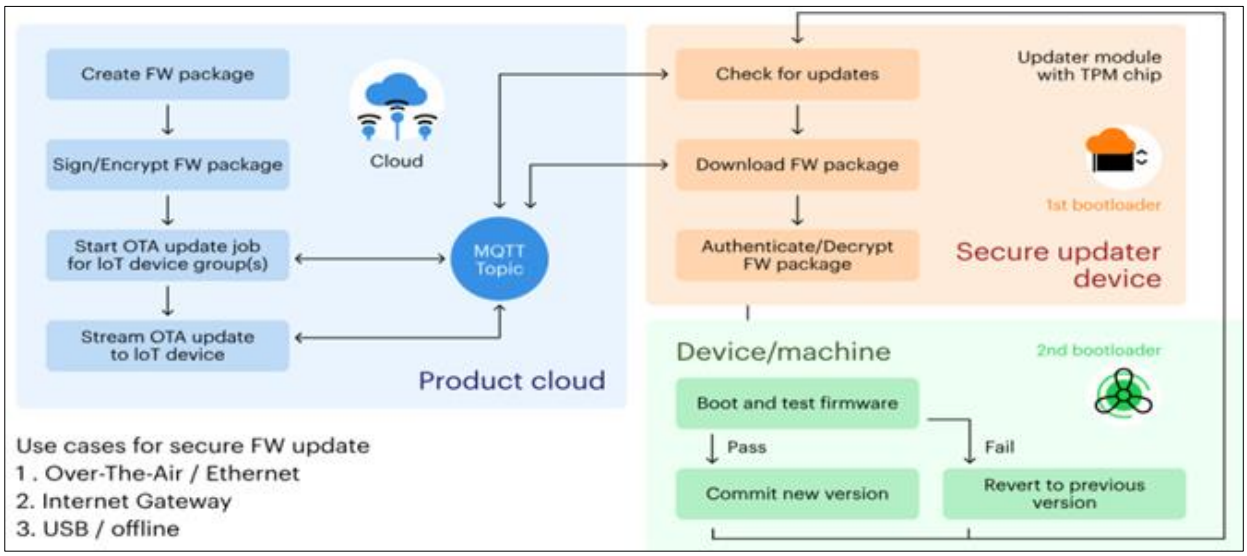

Figure 14 Secure firmware update process

As software and firmware are critical components of devices and systems, they must be kept up-to-date to address security flaws, enhance functionality, and improve performance. However, the update process itself can be a target for attacks, such as man-in-the-middle attacks, where malicious actors could inject harmful code. Secure update mechanisms ensure that updates are authenticated and transmitted safely, often using encryption and digital signatures, to verify the integrity and authenticity of the update source. This prevents unauthorized modifications and ensures that only trusted updates are installed, thereby safeguarding the system from potential breaches and maintaining the overall security posture.

The probable applications include the following:

- *IoT device security*: Many IoT devices are deployed in wireless networks with limited security measures [270]. Ensuring that these devices can receive and verify quantum-safe updates is critical for maintaining network security.
- *Router and access point security*: Wireless routers and access points should support quantum-resistant firmware updates to protect against quantum-assisted attacks that could compromise network infrastructure [271], [272].

However, the considerations must be made:

- *Legacy device support:* Ensuring that legacy devices can receive quantum-safe updates may require developing specialized update mechanisms [273] or gradually phasing out support for older, less secure devices.
- *Update distribution:* Efficiently distributing updates across large wireless networks, particularly in environments with many low-power or intermittent-connectivity devices [274], is a logistical challenge that must be addressed.

The dangers posed by quantum computing to wireless network security are significant, but they can be mitigated through a combination of quantum-resistant cryptographic techniques [275], enhanced security protocols [276], and proactive key management strategies. By investing in research, adopting emerging standards, and educating stakeholders, we can build wireless networks that are resilient to quantum threats, ensuring the continued security and reliability of wireless communications in the quantum era [277], [278]. The transition to quantum-resistant security will be a complex and ongoing process, requiring collaboration across multiple sectors and disciplines. However, by taking proactive steps now, we can protect wireless networks from the potentially devastating impacts of quantum computing, safeguarding critical data and communications for the future.

6. Conclusions

The rapid advancements in quantum computing present both unprecedented opportunities and significant challenges for wireless network security. As quantum technology matures, it has the potential to fundamentally transform the landscape of secure communications. On one hand, quantum computing can enhance security through innovations like Quantum Key Distribution (QKD) and quantum-resistant cryptography, promising stronger protections against future threats. On the other hand, the same technology threatens to render many of today's widely-used cryptographic methods obsolete, posing a serious risk to the confidentiality, integrity, and availability of wireless networks. This survey has explored the dual nature of quantum computing's impact on wireless network security, examining both the potential benefits and the grave dangers it introduces. We've discussed how current wireless security protocols are vulnerable to quantum attacks, particularly those based on public-key cryptography, and the urgent need to develop quantum-resistant solutions. Furthermore, we have explored a range of strategies and technologies that can be adopted to mitigate these risks, including the development of post-quantum cryptography, hybrid cryptographic systems, quantum key distribution, and enhanced key management protocols. The transition to quantum-resistant wireless networks is a complex and long-term process that requires a coordinated effort from researchers, industry leaders, and policymakers. While the challenges are significant, the development of quantum-safe technologies and protocols is critical to maintaining secure wireless communications in the quantum era. As we move forward, it is essential to continue investing in research, developing robust standards, and fostering collaboration across the global community to ensure that wireless networks remain secure against the evolving quantum threat landscape. Evidently, while quantum computing poses substantial risks to wireless network security, it also offers the tools to build a more secure future. By proactively addressing these challenges and embracing the opportunities presented by quantum technologies, we can safeguard the integrity of wireless communications and protect critical information from the quantum threats of tomorrow.

References

[1] Althobaiti OS, Dohler M. Cybersecurity challenges associated with the internet of things in a post-quantum world. Ieee Access. 2020 Aug 25; 8:157356-81.

[2] Akbar MA, Khan AA, Hyrynsalmi S. Role of quantum computing in shaping the future of 6 G technology. Information and Software Technology. 2024 Jun 1; 170:107454.

[3] Sharma S, Ramkumar KR, Kaur A, Hasija T, Mittal S, Singh B. Post-quantum cryptography: A solution to the challenges of classical encryption algorithms. Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021. 2023 Feb 19:23-38.

[4] Burg A, Chattopadhyay A, Lam KY. Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. Proceedings of the IEEE. 2017 Dec 20;106(1):38-60.

[5] Zhang J, Duong TQ, Woods R, Marshall A. Securing wireless communications of the internet of things from the physical layer, an overview. Entropy. 2017 Aug 18;19(8):420.

[6] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[7] Abidin S, Swami A, Ramirez-Asís E, Alvarado-Tolentino J, Maurya RK, Hussain N. Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC). Materials Today: Proceedings. 2022 Jan 1;51:508-14.

[8] Abuarqoub A, Abuarqoub S, Alzu'bi A, Muthanna A. The impact of quantum computing on security in emerging technologies. InProceedings of the 5th International Conference on Future Networks and Distributed Systems 2021 Dec 15 (pp. 171-176).

[9] Sharma M, Choudhary V, Bhatia RS, Malik S, Raina A, Khandelwal H. Leveraging the power of quantum computing for breaking RSA encryption. Cyber-Physical Systems. 2021 Apr 3;7(2):73-92.

[10] Kumar M, Mondal B. Study on Implementation of Shor's Factorization Algorithm on Quantum Computer. SN Computer Science. 2024 Apr 8;5(4):413.

[11] Tang Q, Teague V. Public-Key Cryptography–PKC 2024. InProceedings of the 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia 2024 Apr 15 (pp. 15-17).

[12] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[13] Baseri Y, Chouhan V, Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Computers & Security. 2024 May 1:103883.

[14] Alhakami H. Enhancing IoT Security: Quantum-Level Resilience against Threats. Computers, Materials & Continua. 2024 Jan 1;78(1).

[15] Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, Leichenauer S, Hidary J, Venables P, Hansen R. Transitioning organizations to post-quantum cryptography. Nature. 2022 May 12;605(7909):237-43.

[16] Stanley M, Gui Y, Unnikrishnan D, Hall SR, Fatadin I. Recent progress in quantum key distribution network deployments and standards. InJournal of Physics: Conference Series 2022 Dec 1 (Vol. 2416, No. 1, p. 012001). IOP Publishing.

[17] Liu R, Rozenman GG, Kundu NK, Chandra D, De D. Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication. 2022 Sep;3(3):151-63.

[18] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[19] Perez N. Basic Quantum Mechanics. InMaterials Science: Theory and Engineering 2024 Aug 1 (pp. 101-138). Cham: Springer Nature Switzerland.

[20] Singh B, Ahateshaam M, Lahiri A, Sagar AK. Future of Cryptography in the Era of Quantum Computing. InInternational Conference on Electrical and Electronics Engineering 2023 Aug 19 (pp. 13-31). Singapore: Springer Nature Singapore.

[21] Bansod S, Ragha L. Secured and Quantum Resistant key Exchange Cryptography Methods–A Comparison. In2022 Interdisciplinary Research in Technology and Management (IRTM) 2022 Feb 24 (pp. 1-5). IEEE.

[22] Wetterich C. Quantum computing with classical bits. Nuclear Physics B. 2019 Nov 1;948:114776.

[23] Penchev V. Both classical & quantum information; both bit & qubit: transcendental time. Both physical & transcendental time. Both Physical & Transcendental Time (April 10, 2021). 2021 Apr 10.

[24] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[25] Doskoch IY, Man'ko MA. Superposition principle and Born's rule in the probability representation of quantum states. Quantum Reports. 2019 Sep 26;1(2):130-50.

[26] Kasirajan V. The Quantum Superposition Principle and Bloch Sphere Representation. InFundamentals of Quantum Computing: Theory and Practice 2021 Jun 22 (pp. 75-104). Cham: Springer International Publishing.

[27] Rahman AU, Javed M, Ji Z, Ullah A. Probing multipartite entanglement, coherence and quantum information preservation under classical Ornstein–Uhlenbeck noise. Journal of Physics A: Mathematical and Theoretical. 2021 Dec 22;55(2):025305.

[28] Cacciapuoti AS, Caleffi M, Van Meter R, Hanzo L. When entanglement meets classical communications: Quantum teleportation for the quantum internet. IEEE Transactions on Communications. 2020 Mar 4;68(6):3808-33.

[29] Wang Z, Wu W, Wang J. Steady-state entanglement and coherence of two coupled qubits in equilibrium and nonequilibrium environments. Physical Review A. 2019 Apr;99(4):042320.

[30] Saharia A, Maddila RK, Ali J, Yupapin P, Singh G. An elementary optical logic circuit for quantum computing: a review. Optical and Quantum Electronics. 2019 Jul;51(7):224.

[31] Mummaneni BC, Liu J, Lefkidis G, Hübner W. Laser-controlled implementation of controlled-NOT, hadamard, SWAP, and pauli gates as well as generation of bell states in a 3d–4f molecular magnet. The Journal of Physical Chemistry Letters. 2022 Mar 10;13(11):2479-85.

[32] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[33] Wong HY. Shor's Algorithm. InIntroduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps 2023 Jun 21 (pp. 289-298). Cham: Springer International Publishing.

[34] Qiu D, Luo L, Xiao L. Distributed Grover's algorithm. Theoretical Computer Science. 2024 Apr 27;993:114461.

[35] Deshmukh A. The Role of Quantum Decoherence in Quantum Computing Systems. Journal of Quantum Science and Technology. 2024 Jul 2;1(2):37-43.

[36] Khan MA, Ghafoor S, Zaidi SM, Khan H, Ahmad A. From Quantum Communication Fundamentals to Decoherence Mitigation Strategies: Addressing Global Quantum Network Challenges and Projected Applications. Heliyon. 2024 Jul 11.

[37] Sharifian M, Zarei M, Abdi M, Bartolo N, Matarrese S. Open quantum system approach to the gravitational decoherence of spin-1/2 particles. Physical Review D. 2024 Feb 15;109(4):043510.

[38] Liu Y, Arunachalam S, Temme K. A rigorous and robust quantum speed-up in supervised machine learning. Nature Physics. 2021 Sep;17(9):1013-7.

[39] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[40] Bäuml S, Pascual-García C, Wright V, Fawzi O, Acín A. Security of discrete-modulated continuous-variable quantum key distribution. Quantum. 2024 Jul 18;8:1418.

[41] AbuGhanem M, Eleuch H. NISQ computers: a path to quantum supremacy. IEEE Access. 2024 Jul 22.

[42] Grabowska A, Gunia A. On quantum computing for artificial superintelligence. European Journal for Philosophy of Science. 2024 Jun;14(2):25.

[43] Jayashankar A, Mandayam P. Quantum error correction: Noise-adapted techniques and applications. Journal of the Indian Institute of Science. 2023 Apr;103(2):497-512.

[44] Terhal BM. Quantum error correction for quantum memories. Reviews of Modern Physics. 2015 Apr 1;87(2):307-46.

[45] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[46] Zahidy M, Mikkelsen MT, Müller R, Da Lio B, Krehbiel M, Wang Y, Bart N, Wieck AD, Ludwig A, Galili M, Forchhammer S. Quantum key distribution using deterministic single-photon sources over a field-installed fibre link. npj Quantum Information. 2024 Jan 2;10(1):2.

[47] Zhang Y, Bian Y, Li Z, Yu S, Guo H. Continuous-variable quantum key distribution system: Past, present, and future. Applied Physics Reviews. 2024 Mar 1;11(1).

[48] Gallinad R. G24: A Novel Quantum Key Distribution Protocol for Enhanced Security in Telecommunication Networks. Available at SSRN 4752698. 2024 Feb 20.

[49] Abasifard M, Cholsuk C, Pousa RG, Kumar A, Zand A, Riel T, Oi DK, Vogl T. The ideal wavelength for daylight free-space quantum key distribution. APL Quantum. 2024 Mar 1;1(1).

[50] Michaud A. Critical Analysis of the Origins of Heisenberg's Uncertainty Principle. Journal of Modern Physics. 2024 May 17;15(6):765-95.

[51] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[52] Adnan MH, Ahmad Zukarnain Z, Harun NZ. Quantum key distribution for 5g networks: A review, state of art and future directions. Future Internet. 2022 Feb 25;14(3):73.

[53] Cao Y, Zhao Y, Wang Q, Zhang J, Ng SX, Hanzo L. The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials. 2022 Jan 18;24(2):839-94.

[54] Hoque S, Aydeger A, Zeydan E. Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. arXiv preprint arXiv:2404.10602. 2024 Apr 16.

[55] Stavdas A, Kosmatos E, Maple C, Hugues-Salas E, Epiphaniou G, Fowler DS, Razak SA, Matrakidis C, Yuan H, Lord A. Quantum Key Distribution for V2I communications with software-defined networking. IET Quantum Communication. 2024 Mar;5(1):38-45.

[56] Zikria YB, Ali R, Afzal MK, Kim SW. Next-generation internet of things (iot): Opportunities, challenges, and solutions. Sensors. 2021 Feb 7;21(4):1174.

[57] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[58] Widodo AM, Pappachan P, Sekti BA, Anwar N, Widayanti R, Rahaman M, Bansal R. Quantum-Resistant Cryptography. InInnovations in Modern Cryptography 2024 (pp. 100-130). IGI Global.

[59] Singamaneni KK, Muhammad G. A Novel Integrated Quantum-Resistant Cryptography for Secure Scientific Data Exchange in Ad Hoc Networks. Ad Hoc Networks. 2024 Jul 22:103607.

[60] Wang X, Xu G, Yu Y. Lattice-Based Cryptography: A Survey. Chinese Annals of Mathematics, Series B. 2023 Nov;44(6):945-60.

[61] Wang A, Xiao D, Yu Y. Lattice-based cryptosystems in standardisation processes: A survey. IET Information Security. 2023 Mar;17(2):227-43.

[62] Singh MK. Code-based cryptography: A comparative study of key sizes. InInternational Conference on Advanced Communication and Intelligent Systems 2022 Oct 21 (pp. 359-368). Cham: Springer Nature Switzerland.

[63] Dey J, Dutta R. Progress in multivariate cryptography: Systematic review, challenges, and research directions. ACM Computing Surveys. 2023 Mar 3;55(12):1-34.

[64] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[65] Lin S, Cui L, Ke N. End-to-End Encrypted Message Distribution System for the Internet of Things Based on Conditional Proxy Re-Encryption. Sensors. 2024 Jan 10;24(2).

[66] Jan MA, Zhang W, Usman M, Tan Z, Khan F, Luo E. SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications. 2019 Jul 1;137:1-0.

[67] Lamriji Y, El Makkaoui K, Maleh Y, Beni-Hssane A, Ouahbi I. A lightweight whatsapp end-to-end encryption. EDPACS. 2023 Jun 3;67(6):1-24.

[68] Khalid H, Hashim SJ, Hashim F, Al-Jawher WA, Chaudhary MA, Altarturi HH. RAVEN: Robust Anonymous Vehicular End-to-End Encryption and Efficient Mutual Authentication for Post-Quantum Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems. 2024 Jun 24.

[69] Scheffler S, Mayer J. Group Moderation Under End-to-End Encryption. InProceedings of the Symposium on Computer Science and Law 2024 Mar 12 (pp. 36-47).

[70] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[71] Chawla D, Mehra PS. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. Internet of Things. 2023 Sep 26:100950.

[72] Jacak MM, Jóźwiak P, Niemczuk J, Jacak JE. Quantum generators of random numbers. Scientific Reports. 2021 Aug 9;11(1):16108.

[73] Jóźwiak P, Jacak JE, Jacak WA. New concepts and construction of quantum random number generators. Quantum Information Processing. 2024 Mar 28;23(4):132.

[74] Mannalatha V, Mishra S, Pathak A. A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness. Quantum Information Processing. 2023 Dec 13;22(12):439.

[75] Iavich M. Post-quantum Scheme with the Novel Random Number Generator with the Corresponding Certification Method. InThe International Symposium on Computer Science, Digital Economy and Intelligent Systems 2022 Nov 11 (pp. 76-88). Cham: Springer Nature Switzerland.

[76] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[77] Turčaník M, Javurek M. The Use of Genetic Algorithms for Cryptographic Keys Generation. Digital Transformation, Cyber Security and Resilience of Modern Societies. 2021:315-24.

[78] Al Khaldy M, Aburub F, Al-Qerem A, Aldweesh A, Almomani A. Secure Key Generation and Management Using Generative Adversarial Networks. InInnovations in Modern Cryptography 2024 (pp. 165-189). IGI Global.

[79] Bordel B, Alcarria R, Robles T. Lightweight encryption for short-range wireless biometric authentication systems in Industry 4.0. Integrated Computer-Aided Engineering. 2022 Jan 1;29(2):153-73.

[80] Sathya K, Premalatha J, Rajasekar V. Investigation of strength and security of pseudo random number generators. InIOP Conference Series: materials Science and Engineering 2021 Feb 1 (Vol. 1055, No. 1, p. 012076). IOP Publishing.

[81] B Prajapati R, D Panchal S. Enhanced Approach To Generate One Time Password (OTP) Using Quantum True Random Number Generator (QTRNG). International Journal of Computing and Digital Systems. 2024 Jan 15;15(1):279-92.

[82] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[83] Soler D, Dafonte C, Fernández-Veiga M, Vilas AF, Nóvoa FJ. A privacy-preserving key transmission protocol to distribute QRNG keys using zk-SNARKs. Computer Networks. 2024 Apr 1;242:110259.

[84] Parameswarath RP, Wang C, Sikdar B. A Quantum Safe Mutual Authentication Protocol for Smart Meter Communications With Experimental Evaluation. IEEE Transactions on Network Science and Engineering. 2024 Jul 16.

[85] Li Y, Zhang P, Huang R. Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access. 2019 Jan 21;7:36285-93.

[86] Liu G, Han J, Zhou Y, Liu T, Chen J. QSLT: A Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks. Wireless Communications and Mobile Computing. 2022;2022(1):4809210.

[87] Shi Q, Yang Z, Cheng T, Wang C, Wu Z, Zhang X, Xu P. QKBAKA: A Quantum-Key-Based Authentication and Key Agreement Scheme for Internet of Vehicles. IEEE Internet of Things Journal. 2023 Nov 15.

[88] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[89] Saini A, Tsokanos A, Kirner R. Quantum randomness in cryptography—a survey of cryptosystems, RNG-based ciphers, and QRNGs. Information. 2022 Jul 27;13(8):358.

[90] Lin X, Wang S, Yin ZQ, Fan-Yuan GJ, Wang R, Chen W, He DY, Zhou Z, Guo GC, Han ZF. Security analysis and improvement of source independent quantum random number generators with imperfect devices. npj Quantum Information. 2020 Dec 10;6(1):100.

[91] Kalaivani V. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Personal and ubiquitous computing. 2023;27(3):875.

[92] Abd EL-Latif AA, Abd-El-Atty B, Venegas-Andraca SE, Mazurczyk W. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. Future generation computer systems. 2019 Nov 1;100:893-906.

[93] Kuzyk MG. Quantum no-cloning theorem and entanglement. American Journal of Physics. 2019 May 1;87(5):325-7.

[94] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[95] Hamdoun H, Sagheer A. Information security through controlled quantum teleportation networks. Digital Communications and Networks. 2020 Nov 1;6(4):463-70.

[96] Agarwal S, Somaddar A, Bala N. Revolutionizing Quantum Communication through Quantum Teleportation Techniques. In2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) 2024 May 9 (pp. 1-7). IEEE.

[97] Ahammed MF, Kadir MI. Entanglement and teleportation in quantum key distribution for secure wireless systems. IET Quantum Communication. 2024.

[98] Peng J, Maihemuti N, Aisan Y, Yang Z. Quantum teleportation of shared high-dimensional quantum secret. Physica Scripta. 2024 Jul 25;99(8):085125.

[99] Prajapat S, Kumar P, Kumar S. A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks. Cluster Computing. 2024 Apr 14:1-7.

[100] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[101] Javeed D, Saeed MS, Ahmad I, Adil M, Kumar P, Islam AN. Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. Future Generation Computer Systems. 2024 Jun 13.

[102] Prajapat S, Kumar P, Kumar S, Das AK, Shetty S, Hossain MS. Designing high-performance identity-based quantum signature protocol with strong security. IEEE Access. 2024 Jan 17.

[103] Sharma P, Choi K, Krejcar O, Blazek P, Bhatia V, Prakash S. Securing optical networks using quantum-secured blockchain: An overview. Sensors. 2023 Jan 20;23(3):1228.

[104] Hasan SR, Chowdhury MZ, Saiam M, Jang YM. Quantum communication systems: vision, protocols, applications, and challenges. IEEE Access. 2023 Feb 13;11:15855-77.

[105] Farouk A, Al-Kuwari S, Abulkasim H, Mumtaz S, Adil M, Song H. Quantum Computing: A Tool for Zero-trust Wireless Networks. IEEE Network. 2024 Jun 27.

[106] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[107] Al-Hraishawi H, Rehman JU, Razavi M, Chatzinotas S. Characterizing and utilizing the interplay between quantum technologies and non-terrestrial networks. IEEE Open Journal of the Communications Society. 2024 Mar 25.

[108] Ali MZ, Abohmra A, Usman M, Zahid A, Heidari H, Imran MA, Abbasi QH. Quantum for 6G communication: A perspective. IET Quantum Communication. 2023 Sep;4(3):112-24.

[109] Granelli F, Bassoli R, Nötzel J, Fitzek FH, Boche H, da Fonseca NL. A novel architecture for future classical-quantum communication networks. Wireless Communications and Mobile Computing. 2022;2022(1):3770994.

[110] Rozenman GG, Kundu NK, Liu R, Zhang L, Maslennikov A, Reches Y, Youm HY. The quantum internet: A synergy of quantum information technologies and 6G networks. IET Quantum Communication. 2023 Dec;4(4):147-66.

[111] Veera Jyothi B, Suresh Kumar L, Surya Samantha B. Security Issues in Vehicular Ad Hoc Networks and Quantum Computing. Evolution and Applications of Quantum Computing. 2023 May 29:249-64.

[112] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[113] Banerjee I, Warnier M, Brazier FM. Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices. Complex Adaptive Systems Modeling. 2020 Aug 24;8(1):7.

[114] Abid K, Lakhlef H, Bouabdallah A. A survey on recent contention-free MAC protocols for static and mobile wireless decentralized networks in IoT. Computer Networks. 2021 Dec 24;201:108583.

[115] Dutta H, Bhuyan AK. Quantum Communication: From Fundamentals to Recent Trends, Challenges and Open Problems. arXiv preprint arXiv:2406.04492. 2024 Jun 6.

[116] Kržič A, Sharma S, Spiess C, Chandrashekara U, Töpfer S, Sauer G, González-Martín del Campo LJ, Kopf T, Petscharnig S, Grafenauer T, Lieger R. Towards metropolitan free-space quantum networks. npj Quantum Information. 2023 Sep 27;9(1):95.

[117] Dou Z, Wang Y, Liu Z, Bi J, Chen X, Li L. Quantum secure multi-party computational geometry based on multi-party summation and multiplication. Quantum Science and Technology. 2024 Apr 2;9(2):025023.

[118] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[119] Yigit Y, Ferrag MA, Sarker IH, Maglaras LA, Chrysoulas C, Moradpoor N, Janicke H. Critical infrastructure protection: Generative ai, challenges, and opportunities. arXiv preprint arXiv:2405.04874. 2024 May 8.

[120] Rajawat AS, Goyal SB, Verma C, Singh J. Advancing network security paradigms integrating quantum computing models for enhanced protections. InApplied Data Science and Smart Systems 2025 (pp. 517-528). CRC Press.

[121] Landers VS. Quantum Technologies for Space and Aerial Vehicles. InSpace Governance: Challenges, Threats and Countermeasures 2024 Aug 1 (pp. 105-128). Cham: Springer Nature Switzerland.

[122] Li W, Tug S, Meng W, Wang Y. Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems. 2019 Jul 1;96:481-9.

[123] Devulapally Swetha DS. Quantum-Enhanced Security Advances for Cloud Computing Environments. Quantum. 2024;15(6).

[124] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[125] Tychola KA, Kalampokas T, Papakostas GA. Quantum machine learning—an overview. Electronics. 2023 May 24;12(11):2379.

[126] Gujju Y, Matsuo A, Raymond R. Quantum machine learning on near-term quantum devices: Current state of supervised and unsupervised techniques for real-world applications. Physical Review Applied. 2024 Jun 1;21(6):067001.

[127] Schetakis N, Aghamalyan D, Griffin P, Boguslavsky M. Review of some existing QML frameworks and novel hybrid classical–quantum neural networks realising binary classification for the noisy datasets. Scientific reports. 2022 Jul 13;12(1):11927.

[128] Ullah U, Garcia-Zapirain B. Quantum machine learning revolution in healthcare: a systematic review of emerging perspectives and applications. IEEE Access. 2024 Jan 12.

[129] Innan N, Khan MA, Panda B, Bennai M. Enhancing quantum support vector machines through variational kernel training. Quantum Information Processing. 2023 Oct 15;22(10):374.

[130] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[131] Faker O, Cagiltay NE. Quantum Machine Learning in Intrusion Detection Systems: A Systematic Mapping Study. InInternational conference on WorldS4 2023 Aug 21 (pp. 99-113). Singapore: Springer Nature Singapore.

[132] Innan N, Khan MA, Bennai M. Financial fraud detection: a comparative study of quantum machine learning models. International Journal of Quantum Information. 2024 Mar 16;22(02):2350044.

[133] Alluhaibi R. Quantum Machine Learning for Advanced Threat Detection in Cybersecurity. International Journal of Safety & Security Engineering. 2024 Jun 1;14(3).

[134] Srilakshmi U, Alghamdi SA, Vuyyuru VA, Veeraiah N, Alotaibi Y. A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access. 2022 Jan 19;10:14260-9.

[135] Cherbal S, Zier A, Hebal S, Louail L, Annane B. Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. The Journal of Supercomputing. 2024 Feb;80(3):3738-816.

[136] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[137] Patil A, Pant M, Englund D, Towsley D, Guha S. Entanglement generation in a quantum network at distance-independent rate. npj Quantum Information. 2022 May 6;8(1):51.

[138] Ralegankar VK, Bagul J, Thakkar B, Gupta R, Tanwar S, Sharma G, Davidson IE. Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study. IEEE Access. 2021 Dec 27;10:1475-92.

[139] Bajrić S. Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions. IEEE Access. 2023 Nov 14;11:128801-9.

[140] Savadatti S, Kuldeep Dhariwal S, Krishnamoorthy S, Delhibabu R. An Extensive Classification of 5G Network Jamming Attacks. Security and Communication Networks. 2024;2024(1):2883082.

[141] Adil M, Almaiah MA, Omar Alsayed A, Almomani O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors. 2020 Apr 18;20(8):2311.

[142] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[143] Vithalkar PN. Cryptographic Protocols Resilient to Quantum Attacks: Advancements in Post-Quantum Cryptography. Communications on Applied Nonlinear Analysis. 2024 Jun 23;31(3s):520-32.

[144] Krelina M. Quantum technology for military applications. EPJ Quantum Technology. 2021 Dec 1;8(1):24.

[145] Lehto M. Cyber-attacks against critical infrastructure. InCyber security: Critical infrastructure protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[146] Wang C, Rahman A. Quantum-enabled 6G wireless networks: Opportunities and challenges. IEEE Wireless Communications. 2022 Feb;29(1):58-69.

[147] Leka E, Lamani L, Hoxha E. Securing the Foundations of 6G: Innovative Intelligent Controls at the Physical Layer for Trustworthiness and Resilience. In2024 47th MIPRO ICT and Electronics Convention (MIPRO) 2024 May 20 (pp. 1526-1531). IEEE.

[148] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[149] Gill SS, Buyya R. Transforming research with quantum computing. Journal of Economy and Technology. 2024 Jul 18.

[150] Farouk A, AbuAli NA, Mumtaz S. Quantum-Computing-Based Channel and Signal Modeling for 6G Wireless Systems. IEEE Communications Magazine. 2024 Feb 19;62(2):64-70.

[151] Muthukrishnan H, Suresh P, Logeswaran K, Sentamilselvan K. Exploration of quantum blockchain techniques towards sustainable future cybersecurity. Quantum Blockchain: An Emerging Cryptographic Paradigm. 2022 Jul 15:317-40.

[152] Urgelles H, Maheshwari S, Nande SS, Bassoli R, Fitzek FH, Monserrat JF. In-Network Quantum Computing for Future 6G Networks. Advanced Quantum Technologies. 2024 Mar 10:2300334.

[153] Shamshad S, Riaz F, Riaz R, Rizvi SS, Abdulla S. An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. Sensors. 2022 Oct 25;22(21):8151.

[154] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[155] Yang W. ECC, RSA, and DSA analogies in applied mathematics. InInternational Conference on Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021) 2022 Apr 22 (Vol. 12163, pp. 699-706). SPIE.

[156] Tom JJ, Anebo NP, Onyekwelu BA, Wilfred A, Eyo RE. Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems. International Journal of Engineering and Advanced Technology. 2023;12(5):25-38.

[157] Ukwuoma HC, Arome G, Thompson A, Alese BK. Post-quantum cryptography-driven security framework for cloud computing. Open Computer Science. 2022 Mar 30;12(1):142-53.

[158] Joshi S, Bairwa AK, Pljonkin AP, Garg P, Agrawal K. From Pre-Quantum to Post-Quantum RSA. InProceedings of the 6th International Conference on Networking, Intelligent Systems & Security 2023 May 24 (pp. 1-8).

[159] Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. 2022 Sep 1;15:100242.

[160] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[161] Adesina D, Hsieh CC, Sagduyu YE, Qian L. Adversarial machine learning in wireless communications using RF data: A review. IEEE Communications Surveys & Tutorials. 2022 Sep 12;25(1):77-100.

[162] Naeem S. Network security and cryptography challenges and trends on recent technologies. Journal of Applied and Emerging Sciences. 2023 Jun 30;13(1):01-8.

[163] Rao PM, Deebak BD. A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks. 2023 Jul 1;146:103159.

[164] Lalem F, Laouid A, Kara M, Al-Khalidi M, Eleyan A. A novel digital signature scheme for advanced asymmetric encryption techniques. Applied Sciences. 2023 Apr 21;13(8):5172.

[165] Iqbal S, Sujatha BR. Secure authentication and key management based on hierarchical enhanced identity based digital signature in heterogeneous wireless sensor network. Wireless Networks. 2024 May 6:1-21.

[166] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[167] Banerjee K, Saha S. Blockchain Signatures to Ensure Information Integrity and Non-Repudiation in the Digital Era: A comprehensive study. International Journal of Computing and Digital Systems. 2024 Mar 23;16(1):1-2.

[168] Shrivastava P, Soni KK, Rasool A. Evolution of Quantum Computing Based on Grover's Search Algorithm. In2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019 Jul 6 (pp. 1-6). IEEE.

[169] Wu H, Feng X, Zhang J. Quantum Implementation of the SAND Algorithm and Its Quantum Resource Estimation for Brute-Force Attack. Entropy. 2024 Feb 29;26(3):216.

[170] Szatmáry S. Quantum Computers—Security Threats and Solutions. InIFIP International Conference on Human Choice and Computers 2022 Sep 8 (pp. 431-441). Cham: Springer Nature Switzerland.

[171] Tiwari A, Chauhan R, Joshi N, Devliyal S, Aluvala S, Kumar A. The Quantum Threat: Implications for Data Security and the Rise of Post-Quantum Cryptography. In2024 IEEE 9th International Conference for Convergence in Technology (I2CT) 2024 Apr 5 (pp. 1-7). IEEE.

[172] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[173] Kearney JJ, Perez-Delgado CA. Vulnerability of blockchain technologies to quantum attacks. Array. 2021 Jul 1;10:100065.

[174] Alrawi O, Lever C, Antonakakis M, Monrose F. Sok: Security evaluation of home-based iot deployments. In2019 IEEE symposium on security and privacy (sp) 2019 May 19 (pp. 1362-1380). IEEE.

[175] Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y. Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. IEEE Access. 2020 Mar 24;8:60539-51.

[176] Zandberg K, Schleiser K, Acosta F, Tschofenig H, Baccelli E. Secure firmware updates for constrained iot devices using open standards: A reality check. IEEE access. 2019 May 29;7:71907-20.

[177] Rasori M, La Manna M, Perazzo P, Dini G. A survey on attribute-based encryption schemes suitable for the internet of things. IEEE Internet of Things Journal. 2022 Feb 25;9(11):8269-90.

[178] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[179] Tosun T, Savas E. Zero-Value Filtering for Accelerating Non-Profiled Side-Channel Attack on Incomplete NTT based Implementations of Lattice-based Cryptography. IEEE Transactions on Information Forensics and Security. 2024 Jan 29.

[180] Cavaliere F, Prati E, Poti L, Muhammad I, Catuogno T. Secure quantum communication technologies and systems: From labs to markets. Quantum Reports. 2020 Jan 22;2(1):80-106.

[181] Xiao D, Wei X, Meng H, Zhao Q, Xu H, Xia F, Chen S, Li X, Jin B, Yu Z. Research and Application of Side Channel Attacks and Defenses on Embedded Systems. In2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) 2024 Feb 23 (pp. 1-5). IEEE.

[182] Manzalini A. Quantum communications in future networks and services. Quantum Reports. 2020 Mar 11;2(1):221-32.

[183] Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, Buyya R. Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience. 2022 Jan;52(1):66-114.

[184] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[185] Zawadzki P. Advances in quantum secure direct communication. IET Quantum Communication. 2021 Jun;2(2):54-62.

[186] Vasani V, Prateek K, Amin R, Maity S, Dwivedi AD. Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions. Journal of Industrial Information Integration. 2024 Mar 21:100594.

[187] Brazaola-Vicario A, Ruiz A, Lage O, Jacob E, Astorga J. Quantum key distribution: a survey on current vulnerability trends and potential implementation risks. Optics Continuum. 2024 Aug 6;3(8):1438-60.

[188] Sun S, Huang A. A review of security evaluation of practical quantum key distribution system. Entropy. 2022 Feb 10;24(2):260.

[189] Kong PY. A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Systems Journal. 2020 Oct 2;16(1):41-54.

[190] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[191] Biswas S, Goswami RS, Reddy KH. Advancing quantum steganography: a secure IoT communication with reversible decoding and customized encryption technique for smart cities. Cluster Computing. 2024 Apr 21:1-20.

[192] Nawaz SJ, Sharma SK, Wyne S, Patwary MN, Asaduzzaman M. Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. IEEE access. 2019 Apr 4;7:46317-50.

[193] Mangla C, Rani S, Qureshi NM, Singh A. Mitigating 5G security challenges for next-gen industry using quantum computing. Journal of King Saud University-Computer and Information Sciences. 2023 Jun 1;35(6):101334.

[194] Saritha A, Reddy BR, Babu AS. QEMDD: quantum inspired ensemble model to detect and mitigate DDoS attacks at various layers of SDN architecture. Wireless Personal Communications. 2022 Dec;127(3):2365-90.

[195] Szymanski TH. The “cyber security via determinism” paradigm for a quantum safe zero trust deterministic internet of things (IoT). IEEE Access. 2022 Apr 21;10:45893-930.

[196] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[197] Pervez F, Qadir J, Khalil M, Yaqoob T, Ashraf U, Younis S. Wireless technologies for emergency response: A comprehensive review and some guidelines. Ieee Access. 2018 Nov 23;6:71814-38.

[198] Eliyan LF, Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems. 2021 Sep 1;122:149-71.

[199] Cavaliere F, Mattsson J, Smeets B. The security implications of quantum cryptography and quantum computing. Network Security. 2020 Sep;2020(9):9-15.

[200] Hassija V, Chamola V, Goyal A, Kanhere SS, Guizani N. Forthcoming applications of quantum computing: peeking into the future. IET Quantum Communication. 2020 Dec;1(2):35-41.

[201] Gopalakrishnan K. Security vulnerabilities and issues of traditional wireless sensors networks in IoT. Principles of internet of things (IoT) ecosystem: Insight paradigm. 2020:519-49.

[202] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[203] Baseri Y, Chouhan V, Ghorbani A. Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. arXiv preprint arXiv:2404.10659. 2024 Apr 16.

[204] Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD. Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials. 2021 Aug 30;23(4):2384-428.

[205] Oliveira LB, Pereira FM, Misoczki R, Aranha DF, Borges F, Nogueira M, Wangham M, Wu M, Liu J. The computer for the 21st century: present security & privacy challenges. Journal of Internet Services and Applications. 2018 Dec;9:1-25.

[206] Manpearl E. Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate. U. Fla. JL & Pub. Pol'y. 2017;28:65.

[207] Layode O, Naiho HN, Adeleke GS, Udeh EO, Labake TT. Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information. International Journal of Applied Research in Social Sciences. 2024 Jun 13;6(6):1193-214.

[208] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[209] George AS. When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage. Partners Universal Multidisciplinary Research Journal. 2024 Jul 25;1(2):134-52.

[210] Sullivan S, Brighente A, Kumar SA, Conti M. 5G security challenges and solutions: a review by OSI layers. Ieee Access. 2021 Aug 16;9:116294-314.

[211] Yunakovsky SE, Kot M, Pozhar N, Nabokov D, Kudinov M, Guglya A, Kiktenko EO, Kolycheva E, Borisov A, Fedorov AK. Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technology. 2021 Dec 1;8(1):14.

[212] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access. 2020 Jan 23;8:21091-116.

[213] Bhat JR, Alqahtani SA. 6G ecosystem: Current status and future perspective. IEEE Access. 2021 Jan 26;9:43134-67.

[214] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[215] Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M. Security for 5G and beyond. IEEE Communications Surveys & Tutorials. 2019 May 10;21(4):3682-722.

[216] Mahmood A, Beltramelli L, Abedin SF, Zeb S, Mowla NI, Hassan SA, Sisinni E, Gidlund M. Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends. IEEE Transactions on Industrial Informatics. 2021 Sep 27;18(6):4122-37.

[217] Zhang S, Du X, Liu X. A novel and quantum-resistant handover authentication protocol in IoT environment. Wireless Networks. 2023 Aug;29(6):2873-90.

[218] Raghuvanshi D, Kumar S. Cyber and quantum threats to space systems–A study of the restructuring of a modern armed forces. Comparative Strategy. 2024 May 3;43(3):206-22.

[219] Yung MH. Quantum supremacy: some fundamental concepts. National Science Review. 2019 Jan 1;6(1):22-3.

[220] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[221] Surla G, Lakshmi R. Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks. Optical and Quantum Electronics. 2023 Dec;55(14):1252.

[222] Yousefipoor V, Eghlidos T. An Efficient Post-quantum Attribute-Based Encryption Scheme based on Rank Metric Codes for Cloud Computing. IEEE Access. 2023 Sep 7.

[223] Redkins B, Kuzminykh I, Ghita B. Security of Public-Key Schemes in the Quantum Computing Era–A Literature Review. IEEE Access. 2023 Jun:1-6.

[224] Ravi P, Howe J, Chattopadhyay A, Bhasin S. Lattice-based key-sharing schemes: A survey. ACM Computing Surveys (CSUR). 2021 Jan 2;54(1):1-39.

[225] Yalamuri G, Honnavalli P, Eswaran S. A review of the present cryptographic arsenal to deal with post-quantum threats. Procedia Computer Science. 2022 Jan 1;215:834-45.

[226] Zeydan E, Turk Y, Aksoy B, Ozturk SB. Recent advances in post-quantum cryptography for networks: A survey. In2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ) 2022 Feb 26 (pp. 1-8). IEEE.

[227] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[228] Kumar M, Pattnaik P. Post quantum cryptography (pqc)-an overview. In2020 IEEE High Performance Extreme Computing Conference (HPEC) 2020 Sep 22 (pp. 1-9). IEEE.

[229] Kan K, Une M. Recent trends on research and development of quantum computers and standardization of post-quantum cryptography.

[230] Paul S, Scheible P, Wiemer F. Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication 1. Journal of Computer Security. 2022 Jan 1;30(4):623-53.

[231] Campbell R. Transitioning to a hyperledger fabric quantum-resistant classical hybrid public key infrastructure. The Journal of The British Blockchain Association. 2019 Jul 31.

[232] Ricci S, Dobias P, Malina L, Hajny J, Jedlicka P. Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. IEEE Access. 2024 Feb 8.

[233] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[234] Bindel N, Herath U, McKague M, Stebila D. Transitioning to a quantum-resistant public key infrastructure. InPost-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8 2017 (pp. 384-405). Springer International Publishing.

[235] Nouma SE, Yavuz AA. Trustworthy and efficient digital twins in post-quantum era with hybrid hardware-assisted signatures. ACM Transactions on Multimedia Computing, Communications and Applications. 2024 Mar 8;20(6):1-30.

[236] Mehic M, Michalek L, Dervisevic E, Burdiak P, Plakalovic M, Rozhon J, Mahovac N, Richter F, Kaljic E, Lauterbach F, Njemcevic P. Quantum cryptography in 5G networks: a comprehensive overview. IEEE Communications Surveys & Tutorials. 2023 Aug 28.

[237] Raparthi M. Quantum Cryptography and Secure Health Data Transmission: Emphasizing Quantum Cryptography's Role in Ensuring Privacy and Confidentiality in Healthcare Systems. Blockchain Technology and Distributed Systems. 2022 Jul 5;2(2):1-0.

[238] Pillai SE, Polimetla K. Analyzing the Impact of Quantum Cryptography on Network Security. In2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) 2024 Feb 23 (pp. 1-6). IEEE.

[239] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[240] Alanezi A, Abd El-Latif AA, Kolivand H, Abd-El-Atty B. Quantum walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks. New Journal of Physics. 2023 Dec 22;25(12):123041.

[241] Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, Martin V, Schauer S, Poppe A, Pacher C, Voznak M. Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR). 2020 Sep 28;53(5):1-41.

[242] Sharma P, Agrawal A, Bhatia V, Prakash S, Mishra AK. Quantum key distribution secured optical networks: A survey. IEEE Open Journal of the Communications Society. 2021 Aug 23;2:2049-83.

[243] Myers S, Shull A. Practical revocation and key rotation. InTopics in Cryptology–CT-RSA 2018: The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings 2018 (pp. 157-178). Springer International Publishing.

[244] Everspaugh A, Paterson K, Ristenpart T, Scott S. Key rotation for authenticated encryption. InAdvances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part III 37 2017 (pp. 98-129). Springer International Publishing.

[245] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[246] Sreeravindra BB, Tabbassum A, Saraswathi PK, Najana M. Data Security and Storage Administration with Dynamic Encryption Key Management. International Journal of Global Innovations and Solutions (IJGIS). 2024 May 30.

[247] Khan MA, Puri D. Challenges and Opportunities in Implementing Quantum-Safe Key Distribution in IoT Devices. In2024 3rd International Conference for Innovation in Technology (INOCON) 2024 Mar 1 (pp. 1-7). IEEE.

[248] Ahn J, Kwon HY, Ahn B, Park K, Kim T, Lee MK, Kim J, Chung J. Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). Energies. 2022 Jan 19;15(3):714.

[249] De Ree M, Mantas G, Radwan A, Mumtaz S, Rodriguez J, Otung IE. Key management for beyond 5G mobile small cells: A survey. IEEE Access. 2019 May 1;7:59200-36.

[250] Singh S, Sharma PK, Moon SY, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. 2024 Feb:1-8.

[251] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[252] Allende M, León DL, Cerón S, Pareja A, Pacheco E, Leal A, Da Silva M, Pardo A, Jones D, Worrall DJ, Merriman B. Quantum-resistance in blockchain networks. Scientific Reports. 2023 Apr 6;13(1):5664.

[253] Allgyer W, White T, Youssef TA. Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms. SoutheastCon 2024. 2024 Mar 15:1282-7.

[254] Garcia CR, Rommel S, Takarabt S, Olmos JJ, Guilley S, Nguyen P, Monroy IT. Quantum-resistant Transport Layer Security. Computer Communications. 2024 Jan 1;213:345-58.

[255] Khan MU, Ashraf M, Rehman T, Javaid MA, Khalid MA. Exploration of PQC-Based Digital Signature Schemes in TLS Certificates. The Asian Bulletin of Big Data Management. 2024 Aug 1;4(3):Science-4.

[256] Gharavi H, Granjal J, Monteiro E. Post-quantum blockchain security for the Internet of Things: Survey and research directions. IEEE Communications Surveys & Tutorials. 2024 Jan 17.

[257] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[258] Lamers E, Dijksman R, van der Vegt A, Sarode M, de Laat C. Securing home Wi-Fi with WPA3 personal. In2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) 2021 Jan 9 (pp. 1-8). IEEE.

[259] Sanjuan EB, Cardiel IA, Cerrada JA, Cerrada C. Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach. IEEE Access. 2020 Jun 22;8:115051-62.

[260] Gamess E, Hester G. An Empirical Evaluation of the Constrained Application Protocol in ARM-Based Platforms. InSoutheastCon 2024 2024 Mar 15 (pp. 1-9). IEEE.

[261] Fernández-Caramés TM. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal. 2019 Dec 13;7(7):6457-80.

[262] Kong I, Janssen M, Bharosa N. Challenges in the Transition towards a Quantum-safe Government. InDG. O 2022: The 23rd Annual International Conference on Digital Government Research 2022 Jun 15 (pp. 282-292).

[263] Petrenko K, Mashatan A, Shirazi F. Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications. 2019 Jun 1;46:151-63.

[264] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[265] Rivero-Angeles ME. Quantum-based wireless sensor networks: A review and open questions. International Journal of Distributed Sensor Networks. 2021 Oct;17(10):15501477211052210.

[266] Jenefa A, Ebenezer V, Isaac AJ, Marshell J, Pradeepa P, Naveen V. Adversarial Attacks on Generative AI Anomaly Detection in the Quantum Era. In2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA) 2023 Nov 22 (pp. 1833-1840). IEEE.

[267] Ruff L, Kauffmann JR, Vandermeulen RA, Montavon G, Samek W, Kloft M, Dietterich TG, Müller KR. A unifying review of deep and shallow anomaly detection. Proceedings of the IEEE. 2021 Feb 4;109(5):756-95.

[268] Singh S, Kumar D. Enhancing cyber security using quantum computing and Artificial Intelligence: A Review. algorithms. 2024 Jun;4(3).

[269] Catuogno L, Galdi C. Secure Firmware Update: Challenges and Solutions. Cryptography. 2023 Jun 1;7(2):30.

[270] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[271] Yang Z, Zolanvari M, Jain R. A survey of important issues in quantum computing and communications. IEEE Communications Surveys & Tutorials. 2023 Mar 8;25(2):1059-94.

[272] Tuli EA, Lee JM, Kim DS. Integration of Quantum Technologies into Metaverse: Applications, Potentials, and Challenges. IEEE Access. 2024 Feb 16; 12:29995-30019.

[273] Raheman F. Defining Quantum Advantage for Building a Sustainable MVP to Deliver Quantum Computing Services. Open Journal of Applied Sciences. 2024 Jun 7;14(6):1530-49.

[274] Sarros CA, Demiroglou V, Tsaoussidis V. Intermittently-connected IoT devices: Experiments with an NDN-DTN architecture. In2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) 2021 Jan 9 (pp. 1-9). IEEE.

[275] Althobaiti OS, Dohler M. Quantum-resistant cryptography for the internet of things based on location-based lattices. IEEE Access. 2021 Sep 23; 9:133185-203.

[276] Muslam MM. Enhancing security in vehicle-to-vehicle communication: a comprehensive review of protocols and techniques. Vehicles. 2024 Feb 27;6(1):450-67.

[277] Ziegler V, Schneider P, Viswanathan H, Montag M, Kanugovi S, Rezaki A. Security and Trust in the 6G Era. Ieee Access. 2021 Oct 14;9: 142314-27.

[278] Mayuri AV, Chauhan J, Gadgil A, Rajani O, Rajadhyaksha S. 6G Systems in Secure Data Transmission. Wireless Communication for Cybersecurity. 2023 Nov 8:217-38.