World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Extensive review of quantum computing and network security

Isaiah Awende Otieno *

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

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(02), 770–807

Publication history: Received on 05 July 2024; revised on 12 August 2024; accepted on 15 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.2.0337

Abstract

This research addresses the critical challenge of maintaining network security and privacy in the face of emerging quantum computing technologies. While classical cryptographic methods have long been the cornerstone of network security, the advent of quantum computing threatens to render many of these techniques obsolete. While previously proposed solutions, such as post-quantum cryptography and quantum key distribution, are useful in some aspects of maintaining the security of communications between individuals or organizations, they are often insufficient to protect against the full range of security implications that arise from quantum computing, especially in open shared quantum computing environments. Research in this area is largely challenged by the immaturity of the quantum hardware, quantum error correction, and how to best design secure quantum-safe network architectures in the long term, lack of frameworks for cryptography, and we have very little idea about the best way to use quantum computers to perform certain types of cryptographic attacks for periods well into the future, known as 'collect now, break later' attacks. This paper uses qualitative methodology which is based on systematic literature reviews, using case studies and a document analysis, with the purpose of providing an unabridged and precise assessment on the impact of quantum computing on network security. The study synthesizes the findings from several academic databases regarding the use of quantum technologies in real-world security applications. The findings highlight that quantum computing brings about breakthrough levels of computational power, as well as allowing for super-secure data transmission with quantum key distribution. But there are also new risks, such as crosstalk attacks, qubit sensing attacks and challenges from quantum decoherence and scalability. The paper identifies possible mitigation measures, including new techniques for quantum error correction, quantum-safe cryptography and novel approaches for quantum resources sharing. The findings are of significance for the economy and society as a whole, as they outline the urgency to shift security approaches for networks by developing quantum-safe algorithms and protocols, the importance of interdisciplinary collaboration to this end, and the need to develop policies to prepare for a post-quantum cryptographic era. This range of analysis offers to the researchers, policy-makers and industry professionals a roadmap and concrete guiding principles for future innovation and development of quantum-enhanced network security, concluding that although quantum computing poses as a profound security threat, it could, at the same time, offer revolutionary pathways for secure communications and data-protection when used properly.

Keywords: Quantum computing; Quantum networks; Qubit; Superposition; Entanglement; Quantum gates; Quantum algorithms; Security issues; Decoherence; Cryptography

1. Introduction

Quantum computing is a revolutionary field that leverages the principles of quantum mechanics to process information in fundamentally different ways compared to classical computing [1]. Classical computers use bits as the smallest unit of data, which can be either 0 or 1. In contrast, quantum computers use quantum bits or qubits, which can exist in a state of 0, 1, or both simultaneously due to the phenomenon known as superposition [2], [3]. Additionally, qubits can be entangled, meaning the state of one qubit can be directly related to the state of another, no matter the distance between

* Corresponding author: Isaiah Awende Otieno

them. These properties allow quantum computers to perform complex calculations at exponentially faster rates than their classical counterparts for specific tasks. The potential applications of quantum computing are vast and transformative. In cryptography, quantum computers could break widely used encryption methods, necessitating the development of new cryptographic protocols [4]-[7]. In materials science, they could simulate molecular and atomic interactions with unprecedented accuracy, accelerating the discovery of new materials and drugs [8]. Quantum computing also holds promise for optimizing complex systems, such as supply chains and financial models [9]. Figure 1 shows the architecture of a typical quantum computer. However, despite significant advancements, practical and scalable quantum computers are still in development, facing challenges like qubit stability and error correction [10]. As research progresses, quantum computing is poised to revolutionize numerous fields, offering computational power that could solve problems previously deemed intractable**.**

Quantum computing is poised to revolutionize computer networks through the development of quantum communication and quantum cryptography [11], [12].

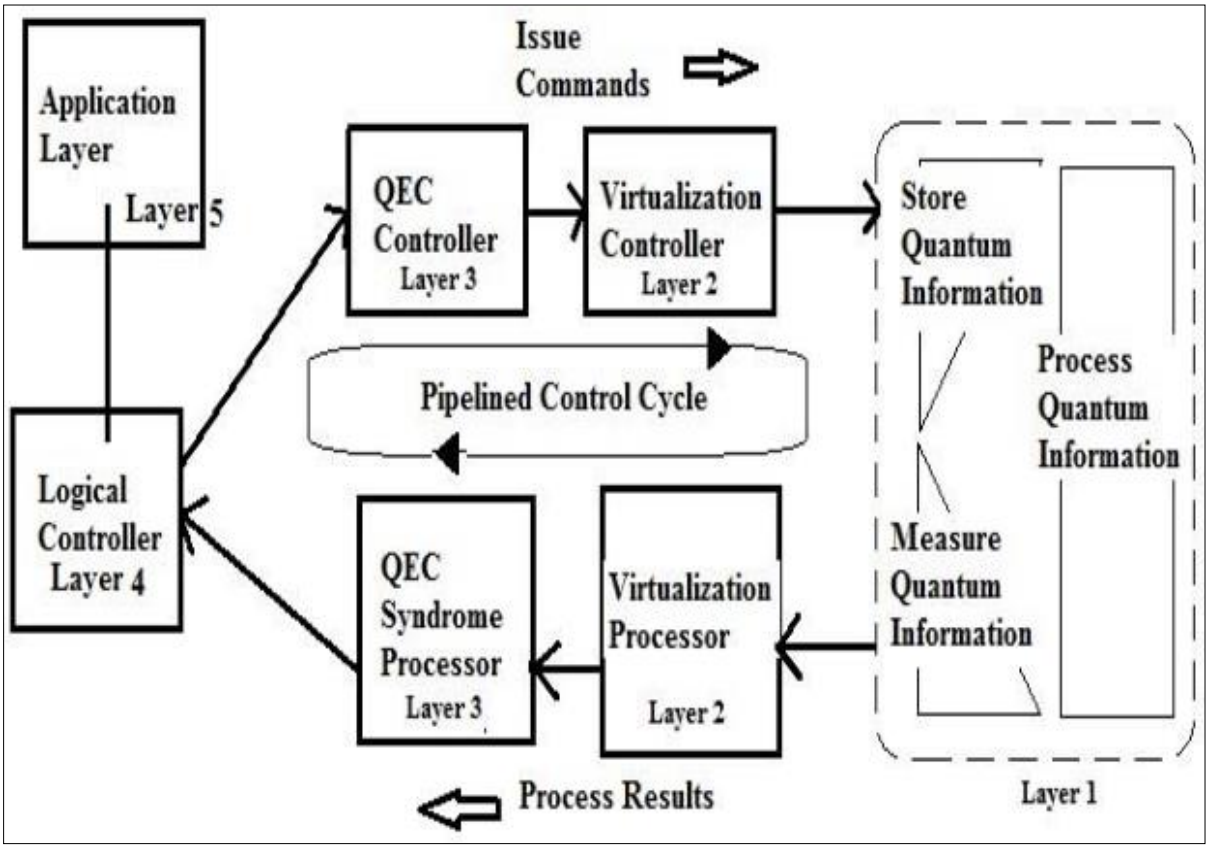

Figure 1 Quantum computer architecture

Quantum communication utilizes principles like entanglement and superposition to enable ultra-secure data transmission. Quantum key distribution (QKD), for instance, allows two parties to generate a shared, secret cryptographic key [13] using the properties of quantum mechanics. Any attempt to eavesdrop on the key exchange disturbs the quantum states involved, alerting the communicating parties to the presence of an intruder. This makes QKD exceptionally secure and has already been demonstrated in various experimental and real-world settings, heralding a new era of secure communications in computer networks [14]-[17]. Figure 2 gives a comparison between quantum and classical computers.

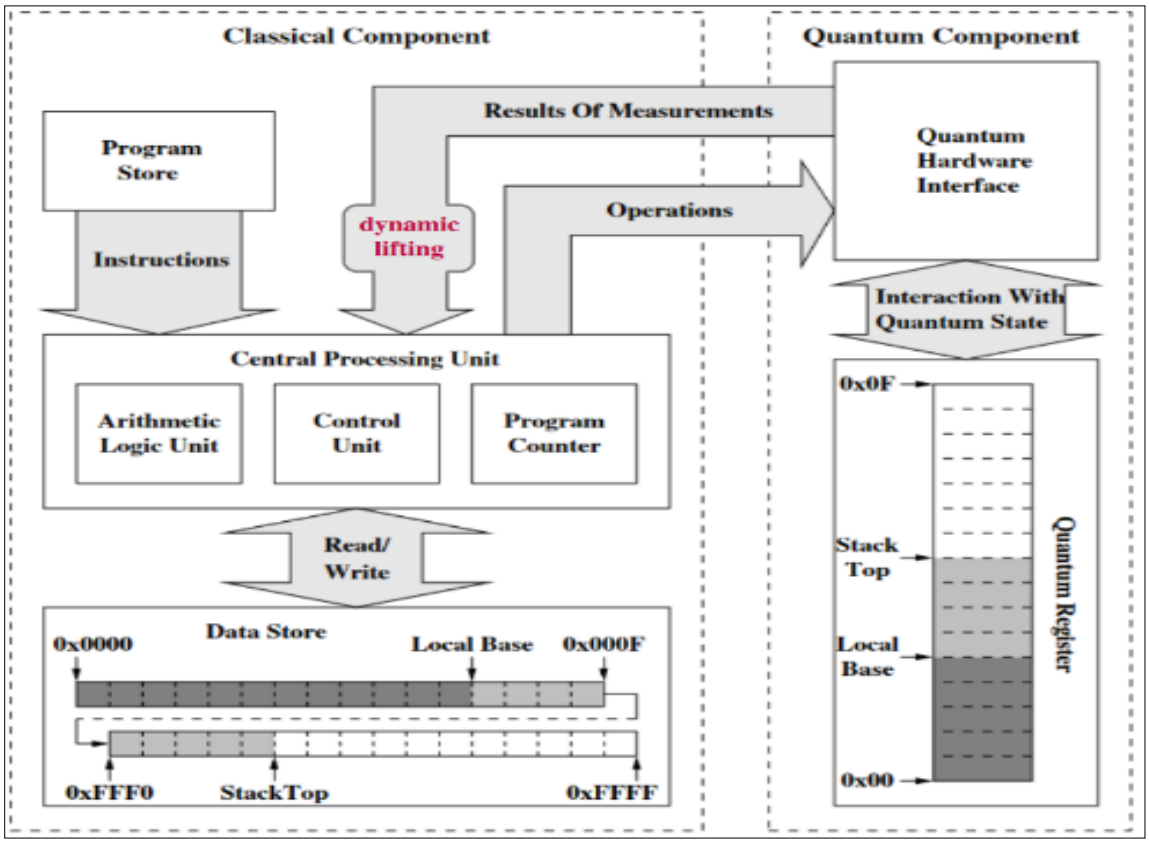

Figure 2 Comparison between classical and quantum computers

Moreover, quantum computing can optimize network operations and enhance performance. Quantum algorithms have the potential to solve complex optimization problems that are central to network design and management more efficiently than classical algorithms [18]. For instance, quantum computing could improve routing algorithms, leading to more efficient data packet delivery and reduced latency [19] in networks. Additionally, quantum-enhanced machine learning could analyze vast amounts of network data to predict and mitigate issues such as congestion and failures [20]-[24]. While practical quantum computing technology for widespread network integration is still under development, its future contributions promise significant advancements in the security, efficiency [25], and reliability of computer networks.

2. The basics of quantum computing

Quantum computing is based on the principles of quantum mechanics, a fundamental theory in physics that describes the behavior of particles at the atomic and subatomic levels [26]. Unlike classical computers, which use bits as the basic unit of information, quantum computers use quantum bits or qubits. Qubits can represent both 0 and 1 simultaneously, thanks to a property called superposition. This allows quantum computers to process a vast amount of information concurrently, offering the potential for exponential speedups in certain computational tasks [27]-[29].

Another key feature of quantum computing is entanglement, a phenomenon where qubits become interconnected in such a way that the state of one qubit directly influences the state of another, regardless of the distance between them [30]. Entanglement enables quantum computers to perform complex calculations and solve problems that are intractable for classical computers. Quantum gates, analogous to classical logic gates, manipulate qubits through operations that can exploit superposition and entanglement to perform quantum computations. Despite the immense potential, building practical and scalable quantum computers faces significant challenges, including maintaining qubit coherence and developing error-correction methods [31] to mitigate the effects of quantum decoherence and noise.

Quantum computing relies on several fundamental elements that distinguish it from classical computing. The primary elements are qubits, superposition, entanglement, quantum gates, and quantum circuits.

- Qubits: The basic unit of information in quantum computing is the quantum bit, or qubit. Unlike classical bits, which can be either 0 or 1, qubits can exist in a state of 0, 1, or both simultaneously, thanks to superposition [32]-[34]. Physical implementations of qubits include trapped ions, superconducting circuits, and quantum dots, among others. Qubits can be manipulated and measured to perform computations and retrieve results.
- Superposition: This principle allows qubits to exist in multiple states at once. In superposition, a qubit can represent a combination of 0 and 1 simultaneously, which enables quantum computers to process a vast amount of information in parallel [35], [36]. Superposition is harnessed through quantum gates to perform complex calculations more efficiently than classical computers.
- Entanglement: Entanglement is a quantum phenomenon where pairs or groups of qubits become interconnected such that the state of one qubit directly influences the state of another, no matter the distance between them [37]. Entangled qubits share information instantaneously, which can be leveraged for highly efficient information processing and secure communication protocols [38], such as quantum key distribution (QKD).
- Quantum Gates: Quantum gates are the building blocks of quantum circuits, analogous to classical logic gates in conventional computing [39]. They manipulate the state of qubits through various operations, such as the Pauli-X, Hadamard, and CNOT gates [40], [41]. These gates enable the creation of complex quantum algorithms by applying specific transformations to qubits, utilizing superposition and entanglement.
- Quantum Circuits: Quantum circuits are composed of sequences of quantum gates arranged to perform specific computations [42]. These circuits are designed to exploit the unique properties of qubits to solve complex problems [43], [44]. A quantum algorithm is implemented as a series of operations on a set of qubits using a well-defined quantum circuit.
- These basic elements form the foundation of quantum computing, enabling it to perform certain types of computations much more efficiently than classical computers. Researchers continue to explore and refine these elements to build practical, scalable quantum computers capable of solving real-world problems.

3. Methodology

This research uses qualitative research methods to gather data from secondary sources and analyze it in an attempt to understand the phenomenon of quantum computing in enhancing network security. This study employs a systematic literature review by focusing on online published articles to gather comprehensive insights on the role of quantum computing in enhancing network security. This research utilizes several relevant academic databases such as google scholar, IEEE Xplore, PubMed among others with the aim of shedding more light on the contagious issue of enhancing network security using quantum computing. During the research, a detailed and specific keyword as well as different search methods were employed to help filter out articles that are more relevant to the topic of study. As such, to ensure quality of the selected articles or publications, the research include a strict inclusion and exclusion criteria which a focus on peer-reviewed articles and books that were published not more than ten years ago. This ensures relevance and latest report is used as a reference point in this study.

The process of synthesizing the findings involved both the descriptive integration and critical integration as a way of summarizing the major findings and yet as a way of also highlighting the strength and the limitations of the studies done. Based on these results, we identified the impact of these results to the discipline of network protection especially on how quantum computing can improve security features. Further, the recommendations on integration of QC into network security were provided based on strengths, weaknesses, opportunities, and threats analyses of current literature, as well as the scope and the limitation of the current study This paper also highlighted the recommendations for the future research on the integration of quantum computing into network security.

4. Role of quantum computing in computer security

Quantum computing offers several promising advantages in the realm of computer security, enhancing both the strength and efficiency of cryptographic protocols [45] and enabling new approaches to secure communication. Here are the key roles quantum computing can play in improving computer security:

4.1. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is one of the most significant contributions of quantum computing to computer security [46]. QKD leverages the principles of quantum mechanics to enable two parties to securely share a secret key [47], [48]. The most well-known QKD protocol is BB84, proposed by Charles Bennett and Gilles Brassard in 1984. Here's how QKD enhances security:

- Eavesdropping Detection: In QKD, any attempt by an eavesdropper to intercept the key will inevitably disturb the quantum states of the particles being transmitted, due to the no-cloning theorem and the principle of measurement in quantum mechanics [49], [50]. This disturbance alerts the communicating parties to the presence of an intruder.
- Unconditional Security: QKD offers security based on the laws of physics rather than computational assumptions. This means that even with unlimited computational resources [51], an attacker cannot gain information about the key without being detected [52].

4.2. Post-Quantum Cryptography

While quantum computers pose a threat to classical cryptographic schemes, they also inspire the development of post-quantum cryptography (PQC) [53]. PQC algorithms are designed to be secure against quantum attacks [54], ensuring long-term security for sensitive data. Some examples include:

- Lattice-Based Cryptography: These algorithms rely on the hardness of lattice problems, which are believed to be resistant to quantum attacks [55], [56]. Lattice-based schemes support advanced functionalities such as fully homomorphic encryption and efficient digital signatures.
- Code-Based Cryptography: McEliece and Niederreiter cryptosystems, based on error-correcting codes, are other candidates for post-quantum security [57].
- Multivariate Quadratic Equations: Cryptographic schemes based on the difficulty of solving systems of multivariate quadratic equations also show promise against quantum adversaries [58], [59].

4.3. Enhanced Random Number Generation

True randomness is critical for cryptographic applications. Quantum Random Number Generators (QRNGs) use quantum processes to generate truly random numbers, offering a higher level of unpredictability than classical methods [60]-[63]. This enhances the security of cryptographic keys and protocols [64], as the randomness used is fundamentally unpredictable.

4.4. Quantum-Safe Network Architectures

Quantum computing enables the design of new network architectures that enhance security. For example:

- Quantum Secure Direct Communication (QSDC): This approach allows the direct transmission of information without first establishing a key [65], [66]. The security is based on the quantum states used in the communication process.
- Quantum Repeaters: For long-distance quantum communication, quantum repeaters can be used to extend the range without compromising security, addressing the problem of decoherence and loss in quantum channels [67], [68].

4.5. Quantum Algorithms for Security Analysis

Quantum computing can also improve the analysis and enhancement of classical security systems:

- Quantum Algorithms for Cryptanalysis: While Shor's algorithm poses a threat to classical encryption, it also provides a tool for analyzing and understanding the strength of cryptographic systems [69]. This dual-use can help in designing more robust [70] encryption methods.
- Quantum Machine Learning (QML): QML algorithms can be applied to anomaly detection and threat prediction, improving the ability to detect and respond to security incidents in real-time [71], [72].

4.6. Blockchain and Distributed Ledger Technologies

Quantum computing can bolster the security and efficiency of blockchain and distributed ledger technologies (DLTs):

- Quantum-Resistant Consensus Mechanisms: By integrating quantum-safe cryptographic techniques, blockchains can be made resistant to future quantum attacks, ensuring the integrity and longevity of data stored on the blockchain [73]-[75].
- Enhanced Security Protocols: Quantum cryptographic techniques can enhance the security protocols [76] used in DLTs, providing stronger guarantees of data integrity and authenticity.

4.7. Secure Multi-Party Computation

Quantum computing can enhance Secure Multi-Party Computation (SMPC), where multiple parties compute a function over their inputs while keeping those inputs private [77]-[81]. Quantum SMPC protocols can leverage quantum entanglement and superposition to provide stronger security guarantees and more efficient computations.

4.8. Biometric Security

Quantum computing can improve biometric security systems [82] by enabling more accurate and secure processing of biometric data. Quantum algorithms can efficiently analyze and match biometric patterns, reducing false positives and negatives, and enhancing the overall security of biometric authentication systems [83]-[87].

In a nutshell, quantum computing holds transformative potential for computer security, offering new methods for secure communication [88], cryptographic resilience, and advanced security analysis. While practical, large-scale quantum computers are still in development, ongoing research in quantum-safe cryptography and the implementation of quantum-enhanced security protocols is essential to prepare for the quantum era. By leveraging the unique properties of quantum mechanics, quantum computing promises to significantly bolster the security of digital information and communication systems.

5. Role of quantum computing in network privacy

Quantum computing offers transformative potential in enhancing network privacy through its unique properties of superposition, entanglement, and quantum cryptographic techniques. This section explores the key roles quantum computing plays in bolstering network privacy:

5.1. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a groundbreaking application of quantum mechanics that ensures secure communication by enabling two parties to generate and share a secret cryptographic key with a high degree of security [89].

- *Eavesdropping Detection*: In QKD, any attempt to intercept the key introduces detectable anomalies due to the no-cloning theorem and the fundamental principles of quantum measurement [90]-[93]. This ensures that any eavesdropping [94] efforts are immediately apparent, alerting the communicating parties to potential breaches.
- *Unconditional Security*: Unlike classical key distribution methods, whose security depends on computational difficulty, QKD's security is based on the laws of quantum physics [95]. This offers unconditional security, making it invulnerable to the computational advancements, including those brought by quantum computers [96], [97].

5.2. Quantum Secure Communication

Quantum computing enables various methods of secure communication that directly protect network privacy:

- *Quantum Secure Direct Communication (QSDC)*: This method allows for the secure transmission of information without first establishing a key [98]. Information is encoded in quantum states and transmitted directly, ensuring that any attempt to eavesdrop will disturb the quantum states and be detected [99].
- *Quantum Teleportation*: This technique allows the transmission of quantum information (qubits) between two distant parties without actually moving the physical particles that hold the information [100]. It utilizes entanglement and classical communication to ensure that the information remains secure during transit.

5.3. Enhanced Random Number Generation

Quantum Random Number Generators (QRNGs) leverage quantum mechanical processes to produce truly random numbers [101], which are crucial for cryptographic applications:

- *Unpredictability*: Unlike classical random number generators, which rely on algorithms and can be potentially predictable, QRNGs provide genuine randomness based on quantum phenomena [102]- [106]. This unpredictability is essential for creating secure cryptographic keys that protect network privacy [107].
- *Stronger Encryption*: QRNGs enhance the security of encryption algorithms by providing high-quality random keys [108] that are immune to the predictability issues associated with classical methods.

5.4. Post-Quantum Cryptography

As quantum computers have the potential to break many classical cryptographic schemes, the development of post-quantum cryptography (PQC) is essential to maintaining network privacy:

- *Lattice-Based Cryptography*: This cryptographic approach relies on mathematical problems that are believed to be hard for quantum computers to solve, ensuring the security of encrypted communications even in a post-quantum world [109].
- *Hash-Based Cryptography*: Another promising area of PQC, hash-based cryptography, uses hash functions to create secure digital signatures resistant to quantum attacks [110], [111].
- *Code-Based Cryptography*: Utilizing error-correcting codes, code-based cryptography [112] offers another layer of protection against the potential threats posed by quantum computing.

5.5. Quantum Privacy Amplification

Quantum privacy amplification techniques help improve the security of shared keys in quantum communication protocols:

- *Error Correction*: By identifying and correcting errors introduced by noise and potential eavesdropping [113], quantum privacy amplification ensures that the final key shared between parties remains secure and private [114].
- *Key Distillation*: This process involves generating a highly secure final key from a partially secure one by applying quantum operations that amplify privacy and security [115], [116].

5.6. Secure Multi-Party Computation (SMPC)

Quantum computing enhances Secure Multi-Party Computation (SMPC), allowing multiple parties to jointly compute a function over their inputs while keeping those inputs private:

- *Quantum SMPC Protocols*: Utilizing quantum entanglement and superposition, quantum SMPC protocols can provide stronger privacy guarantees and more efficient computations compared to classical methods [117], [118].
- *Enhanced Privacy*: Quantum SMPC can ensure that sensitive data [119] used in joint computations remains private, even from other parties involved in the computation.

5.7. Quantum-Enhanced Blockchain Technology

Blockchain technology can significantly benefit from quantum enhancements, ensuring greater privacy and security:

- *Quantum-Resistant Blockchains*: Developing quantum-resistant cryptographic algorithms for blockchain systems ensures that the privacy and integrity of transactions are maintained even in the presence of quantum computers [120], [121].
- *Secure Consensus Mechanisms*: Quantum computing can enhance the security of consensus mechanisms used in blockchain technology, protecting against potential attacks and ensuring the privacy of the transaction data [122], [123].

5.8. Privacy-Preserving Quantum Machine Learning (QML)

Quantum machine learning (QML) can offer privacy-preserving solutions for analyzing and processing sensitive data:

- *Federated Learning*: QML can enable privacy-preserving federated learning, where multiple parties collaboratively train a model without sharing their private data [124], [125]. This ensures data privacy while benefiting from shared knowledge.
- *Anomaly Detection*: QML algorithms can enhance the detection of privacy breaches and anomalous activities in networks by analyzing large datasets more efficiently and accurately, ensuring timely responses to potential threats [126]-[128].

5.9. Biometric Data Privacy

Quantum computing can enhance the security and privacy of biometric data:

- *Secure Biometric Matching*: Quantum algorithms can improve the accuracy and security of biometric matching processes, reducing the risk of false positives and negatives while ensuring the privacy of biometric information [129], [130].
- *Encrypted Storage and Transmission*: Quantum encryption techniques can be used to securely store and transmit biometric data, protecting it from unauthorized access [131] and ensuring that personal information remains private.

It is clear that quantum computing holds immense promise for enhancing network privacy through its advanced cryptographic capabilities, secure communication methods, and privacy-preserving algorithms. By leveraging the unique properties of quantum mechanics, quantum computing can provide robust security solutions that protect sensitive information, detect potential breaches, and ensure the privacy of communications. As the technology continues to evolve, it will play an increasingly critical role in safeguarding network privacy in an increasingly interconnected world.

6. Threats posed by quantum computing to network security

Quantum computing, while offering transformative benefits, also poses significant threats to network security [132]. The potential of quantum computers to solve certain mathematical problems exponentially faster than classical computers could undermine many of the cryptographic systems that secure modern networks. Figure 3 shows a typical attack on the quantum channel.

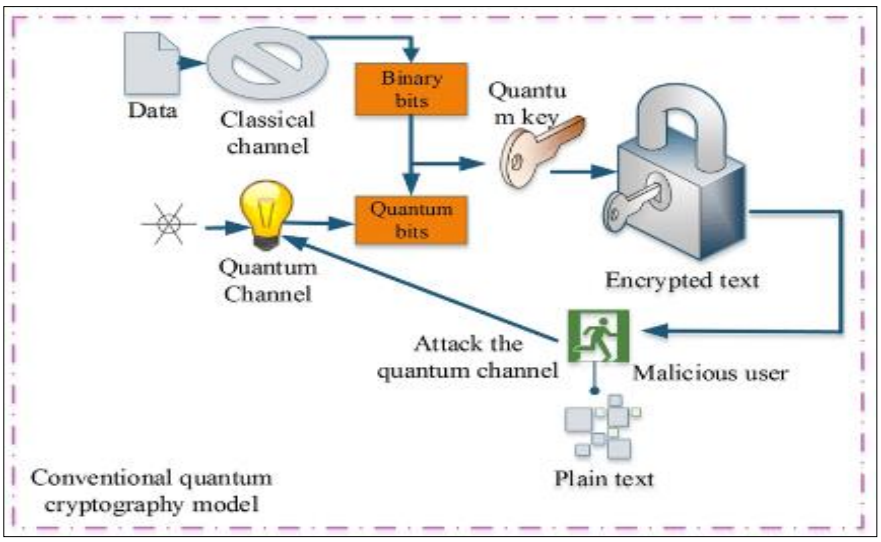

Figure 3 Quantum channel attack

The following are the major threats posed by quantum computing to network security:

6.1. Breaking Classical Cryptographic Algorithms

One of the most prominent threats quantum computing poses is its ability to break widely used classical cryptographic algorithms:

- *Public-Key Cryptography*: Shor's algorithm can efficiently factor large integers and compute discrete logarithms, which are the mathematical foundations of many public-key cryptosystems such as RSA, DSA, and Diffie-Hellman [134]-[136]. Figure 4 illustrates the operation of public cryptosystem.

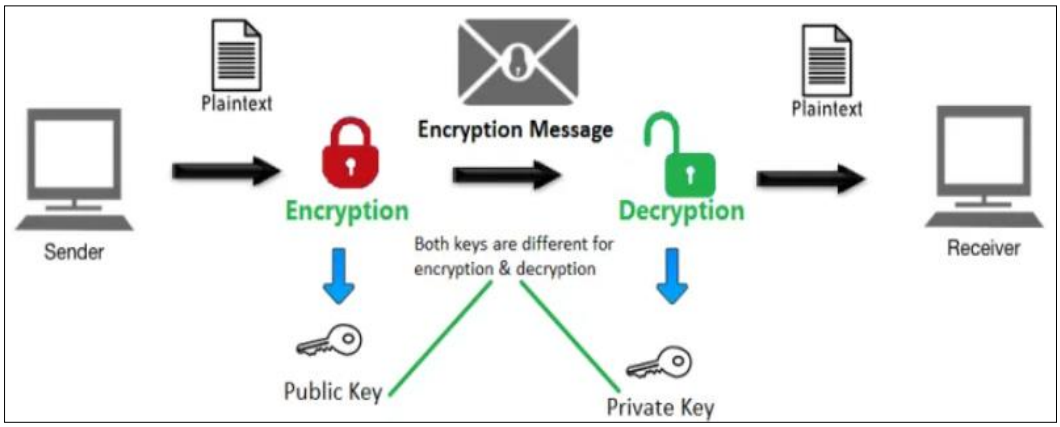

Figure 4 Operation of public-key cryptography

Once a practical quantum computer is available, it could decrypt data encrypted with these methods, compromising the security of confidential communications, financial transactions, and sensitive data stored or transmitted over networks [137].

- *Impact on Digital Signatures*: Many digital signature schemes rely on the same mathematical principles as public-key encryption [138]-[140]. Quantum computers could forge digital signatures, undermining the integrity and authenticity of digital documents and communications.
- *Symmetric-Key Cryptography*: Grover's algorithm provides a quadratic speedup for searching unsorted databases and solving problems like brute-forcing cryptographic keys [141], [142]. For symmetric-key cryptosystems [143], this means that the effective security of the key length is halved. For instance, AES-256 would provide the equivalent security of AES-128 against a quantum adversary, necessitating the use of longer key lengths to maintain security.

6.2. Vulnerability of Encrypted Data

Quantum computing threatens the long-term confidentiality of data encrypted with current standards:

- *Harvest Now, Decrypt Later*: As shown in Figure 5, adversaries might harvest encrypted data today, anticipating the future capability to decrypt it once quantum computers become powerful enough [144], [145]. This is particularly concerning for data that needs to remain confidential for long periods, such as government secrets, intellectual property, and personal information. I It refers to the strategy where adversaries collect and store encrypted data today, anticipating that future advancements in quantum computing will enable them to decrypt this data. Quantum computers, leveraging principles of quantum mechanics, have the potential to solve complex mathematical problems much faster than classical computers. This includes breaking widely used cryptographic algorithms, such as RSA and ECC, which rely on the difficulty of factoring large numbers and solving discrete logarithms. The HNDL threat underscores the urgency for developing and adopting quantum-resistant cryptographic methods to secure sensitive information against future quantum attacks. This is a significant cybersecurity threat model emerging from the potential capabilities of quantum computing. The concept revolves around the idea that adversaries, recognizing the impending power of quantum computers, are actively harvesting and storing vast amounts of encrypted data with the expectation that these future quantum systems will eventually enable them to decrypt this data. The current encryption methods, primarily based on RSA and ECC, rely on the computational difficulty of factoring large numbers and solving discrete logarithms. Quantum computers, with their ability to perform complex calculations at unprecedented speeds using algorithms like Shor's algorithm, pose a real threat to these cryptographic schemes. This means that data encrypted today, presumed secure under classical computation assumptions, could be at risk of exposure once quantum computing reaches a certain level of maturity.

The implications of HNDL are profound, as it suggests that sensitive information, including financial records, state secrets, and personal data, is vulnerable to future quantum attacks.

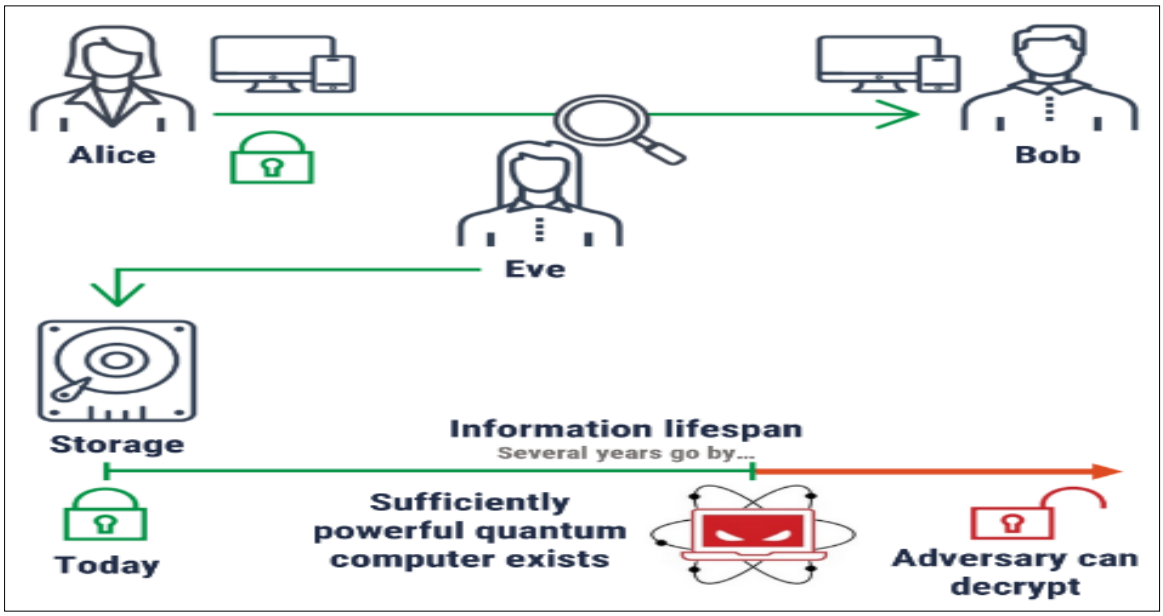

Figure 5 Illustration of harvest now, decrypt later

This looming threat has spurred a global effort to develop and implement quantum-resistant cryptographic algorithms, which are believed to be secure against quantum attacks. Organizations and governments are increasingly prioritizing the transition to post-quantum cryptography (PQC) to safeguard data against this future risk. The National Institute of Standards and Technology (NIST) has been actively working on standardizing PQC algorithms to provide robust security solutions. The HNDL scenario highlights the need for proactive measures in cybersecurity, emphasizing that the protection of today's data must account for the technological advancements of tomorrow.

6.3. Compromising Blockchain and Cryptocurrency Security

Quantum computing poses a specific threat to the security of blockchain technologies and cryptocurrencies:

- *Breaking Blockchain Hash Functions*: Many blockchain systems rely on cryptographic hash functions for security [146]-[148]. Quantum computers could potentially find collisions (two different inputs producing the same hash) much faster, threatening the integrity of blockchain records.
- *Compromising Wallet Security*: Public-key cryptography [149] secures cryptocurrency wallets. Quantum computers could derive private keys from public keys, enabling unauthorized access and transfer of digital assets.

6.4. Threats to Network Authentication Protocols

Quantum computing can undermine network authentication mechanisms:

- *Compromised Authentication*: Many network authentication protocols, such as those used in VPNs, SSL/TLS, and Wi-Fi security (e.g., WPA2), rely on public-key cryptography [150]-[152]. Quantum computers could potentially break these protocols, leading to unauthorized access to network resources and man-in-the-middle attacks.
- *Security Certificates*: The security of SSL/TLS certificates, which are used to establish secure connections between clients and servers, could be compromised by quantum computers [153], [154]. This could lead to the forging of certificates and the undermining of the entire PKI (Public Key Infrastructure) system.

6.5. Impacts on Internet of Things (IoT) Security

Quantum computing threatens the security of IoT devices, which often rely on lightweight cryptographic protocols [155]:

- *Weak Cryptography*: Many IoT devices use simplified cryptographic algorithms due to limited computational resources [156]-[161]. These simplified algorithms are more susceptible to quantum attacks, potentially compromising entire IoT ecosystems.

- *Network Vulnerabilities*: Quantum computing could enable new types of attacks on IoT networks, such as unauthorized device access, data interception, and control over IoT devices [162].

6.6. Compromising Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) protocols, used for privacy-preserving computations among multiple parties, could be at risk:

- *Breakdown of Security Guarantees*: Quantum computers could potentially break the cryptographic guarantees that underpin SMPC protocols [163], leading to the exposure of sensitive data during collaborative computations.

6.7. Threats to Privacy-Preserving Technologies

Quantum computing could undermine various privacy-preserving technologies, including:

- *Homomorphic Encryption*: While homomorphic encryption allows computations on encrypted data without revealing the data itself [164], quantum attacks could potentially compromise the underlying cryptographic assumptions. As shown in Figure 6, homomorphic encryption is a form of encryption that allows computations to be performed directly on encrypted data without needing to decrypt it first.

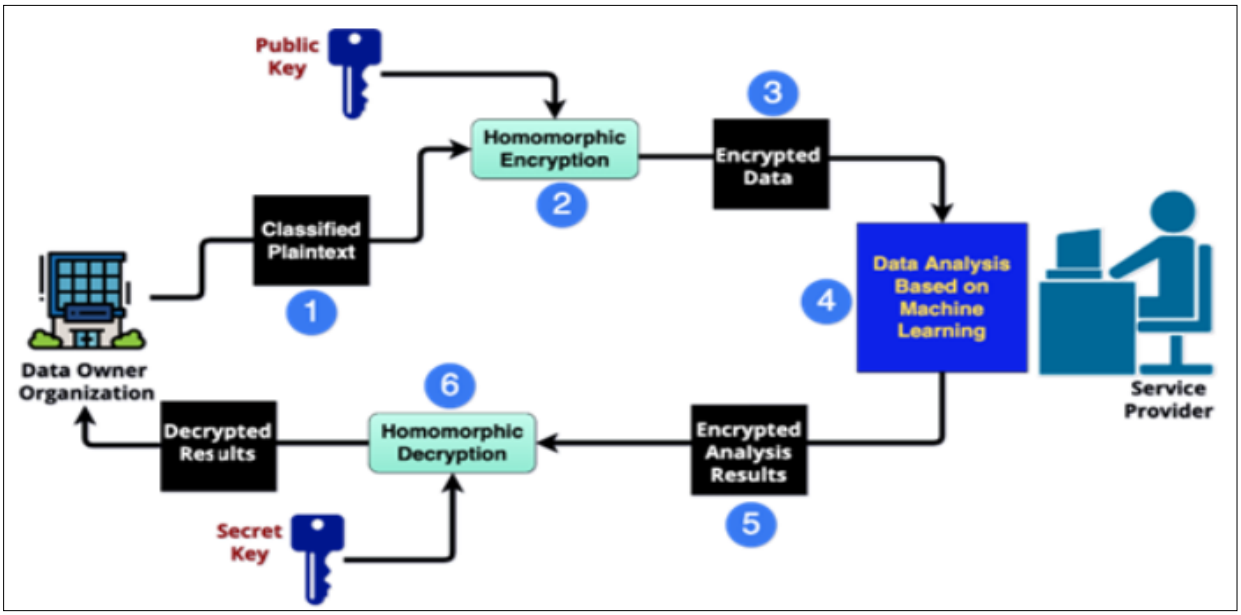

Figure 6 Homomorphic procedures

This means that mathematical operations carried out on the encrypted data produce an encrypted result which, when decrypted, matches the result of the same operations performed on the original plaintext. This technology has profound implications for data privacy and security, enabling secure data processing in various fields such as cloud computing, financial services, and healthcare. By allowing computations on encrypted data, homomorphic encryption ensures that sensitive information remains protected even while it is being processed, thereby enhancing the security and privacy of data handling practices.

- *Zero-Knowledge Proofs*: Quantum computers could break the cryptographic constructs used in zero-knowledge proofs [165], which are used to verify information without revealing the underlying data. As depicted in Figure 7, Zero-knowledge proofs (ZKPs) are cryptographic protocols that enable one party (the prover) to prove to another party (the verifier) that they know a specific piece of information or that a particular statement is true, without revealing the information itself or any additional details. This concept was first introduced by researchers Shafi Goldwasser, Silvio Micali, and Charles Rackoff in the 1980s. The main advantage of ZKPs is their ability to maintain privacy and security, ensuring that sensitive information is not disclosed during the verification process. ZKPs are particularly useful in scenarios where trust is essential but direct information sharing is undesirable, such as in authentication systems, secure voting, and confidential financial transactions.

One of the practical applications of zero-knowledge proofs is in blockchain technology, where ZKPs can enhance privacy and scalability. For example, zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are a type of ZKP that allows for efficient and compact proof verification without interaction between the prover and verifier.

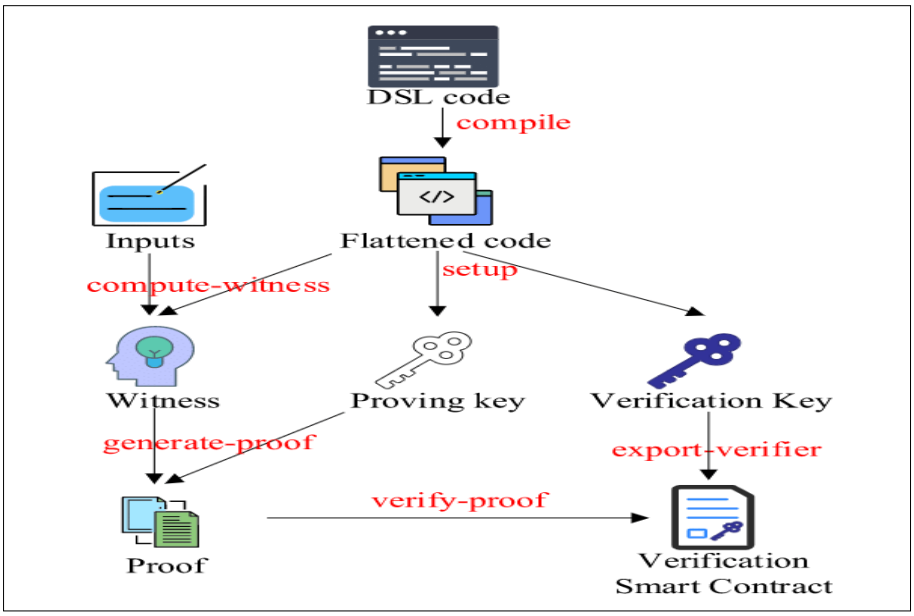

Figure 7 Zero-knowledge proofs process

This makes them ideal for use in cryptocurrencies like Zcash, where transaction details need to be kept private while still ensuring the validity and integrity of the transactions. Additionally, ZKPs can be employed in decentralized finance (DeFi) to provide secure and private smart contracts. By leveraging zero-knowledge proofs, systems can achieve a balance between transparency and privacy, offering robust security without compromising on confidentiality.

6.8. Risks to Financial Systems and Digital Economy

The financial sector, heavily reliant on cryptographic security, faces specific risks from quantum computing:

- *Transaction Security*: Quantum attacks could compromise the security of financial transactions, leading to fraud, theft, and market manipulation [166], [167].
- *Secure Communication*: Financial institutions rely on secure communication channels to protect sensitive information [168], [169]. Quantum computing could break these channels, exposing confidential data and undermining trust in financial systems.

7. Mitigation Strategies

Addressing the threats posed by quantum computing requires proactive measures, including:

- *Development of Post-Quantum Cryptography (PQC)*: Research and adoption of cryptographic algorithms resistant to quantum attacks are crucial [170], [171]. This includes lattice-based, hash-based, code-based, and multivariate quadratic equation-based cryptographic schemes.
- *Quantum-Safe Protocols*: Updating and designing network protocols to be quantum-safe, ensuring that authentication, encryption, and data integrity mechanisms remain secure against quantum adversaries [172], [173].
- *Hybrid Cryptographic Systems*: Implementing hybrid cryptographic systems that combine classical and quantum-resistant algorithms to provide security in the transition period before fully adopting quantum-resistant technologies [174], [175].
- *Quantum Key Distribution (QKD)*: Utilizing QKD to secure communication channels [176] with provable security based on the laws of quantum mechanics. As depicted in Figure 8, QKD is a secure communication protocol that uses the principles of quantum mechanics to generate and distribute cryptographic keys between two parties, typically referred to as Alice and Bob. The most well-known QKD protocol is BB84, proposed by Charles Bennett

and Gilles Brassard in 1984. QKD leverages the quantum properties of particles, such as photons, to ensure that any attempt to eavesdrop on the key transmission introduces detectable disturbances.

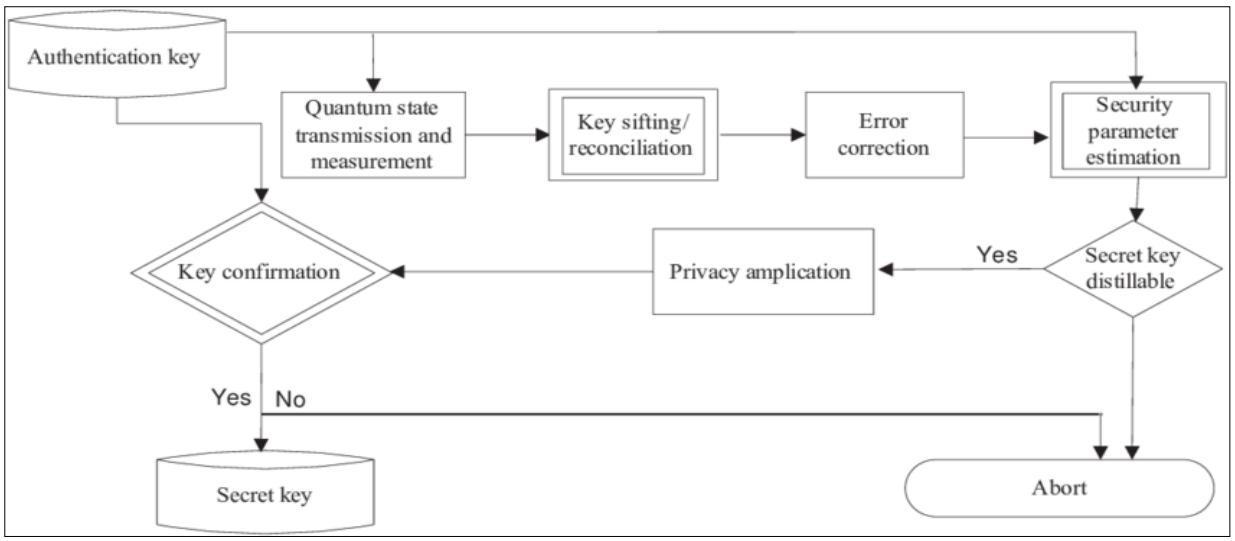

Figure 8 Quantum key distribution protocol

This allows Alice and Bob to detect the presence of an eavesdropper (Eve) and discard the compromised key, ensuring the security of the communication. By providing a method to establish a shared, secret key that is theoretically secure against any computational attack, including those from quantum computers, QKD represents a significant advancement in cryptographic security.

8. Privacy Issues in Quantum Computing Networks

As much as quantum computing is expected to be the best when it comes to network security and handling of vulnerabilities, it is still prone to some privacy issues [177]. Another serious threat is crosstalk noise, which is a type of interference where operations on one qubit end up affecting neighboring qubits (this can happen even when not one but multiple users access the same piece of quantum hardware day after day via cloud instances and share the qubits' usage) [178]. If that happens, crosstalk noise could leak private information [179] or lead to other breaches of security. In real-world scenarios, other users' computations can be disturbed by the interactions of your quantum programmed with a common piece of quantum hardware [180]. Just as a chat room with a loud participant can be annoyed by another loud participant, two different quantum programs computing simultaneously on the same quantum machine can get disturbed by one another's choice of computing recipe, thanks to the strange nature of the quantum machine. An attacker could use a particularly complex quantum programme to generate so much crosstalk noise that it would destroy the quantum algorithms of others [181]. This in turn requires the isolation of relevant hardware components to completely prevent unintentional and malicious interference.

Additionally, readout errors, especially in the measurement step of quantum computation, are another major source of leakage. Attacks that exploit readout errors usually occur as classical bit-flip errors [182]. In this scenario, letters in the victim's quantum computing programme are taken erroneously, which makes the readout inaccurate and the whole computation unreliable. In particular, readout errors are correlated across qubits and are state-dependent [183], [184]. An error in one qubit can lead to errors in the neighbouring qubits as well, and the leakage occurs even if the attacker has no direct access, especially when two users share the same hardware. Hence, sensitive information of the victim's quantum program can be leaked, implying the need for more effective error-mitigation measures, and better and more secure measurement protocols [185]. Some of these issues are as discussed below.

8.1. Crosstalk Attacks

Crosstalk noise is a type of interference that occurs in quantum computing the moment operations on qubit unintentionally influence neighboring qubits. This can cause faults in quantum computations; these are of particular concern, as states are fragile and operations require a great deal of accuracy [186]. In shared quantum computing environments, if many users share the same quantum hardware through cloud services, crosstalk noise may raise serious privacy and security concerns [187]. Shared quantum computing often takes place by running a quantum

program on the same physical quantum-processing unit simultaneously by several users. However, with this democratization of access to the cutting-edge quantum technology through a shared access model, certain trade-offs come. Users are effectively trying to run their computations in parallel on the same hardware, which means that the actions of one user can inadvertently or maliciously impact the computations of another user through mechanisms like crosstalk noise [188]. A crosstalk attack targets the facilitation of quantum computations by other users by use of the phenomenon called the crosstalk noise, in a disruptive or influential manner. In this regard, an attacker can create special quantum circuits that would generate excessive crosstalk noise and consequently propagate to the neighbouring qubits of other users. This type of intentional disruption will result in wrong computation results, hence effectively sabotaging the quantum algorithms corresponding to the other users [189]. These attacks exploit the physical closeness of qubits on the quantum processor, leaning on the hallmark features of hardware-intrinsic noise.

8.2. Qubit Sensing Attack

One major flaw with these powerful quantum computers lies in readout errors. Such an error occurs in the final phases of quantum computation majorly in the measurement phase [190]. More specifically, readout errors can be understood as classical bit-flip errors, in which the qubit in state "1" might be read as "0" and vice versa. It is quite a nasty type of error since it contaminates the accuracy [191] and reliability of quantum computations. Two of the critical characteristics of readout errors in these devices are state dependence and correlation across qubits. State dependence refers to the fact that the two states do not have equal probabilities for readout errors; that is, one is not equally likely to flip from "1" to "0" as when flipping from "0" to "1". In particular, qubit correlations mean that the error probabilities are not insulated; an error on one qubit is able to interact with and affect the errors on neighbouring qubits, further complicating the picture [192], [193]. Consequently, this attack type adduces tangible risk of privacy as it may tentatively lead to sensitive processed information by the victim's quantum program leaked. The critical vulnerability in the current quantum computing systems is depicted by the action ability to infer outputs with high level of accuracy. This is more prone on shared environments where numerous users share the same hardware.

8.3. Quantum Decoherence

Quantum deceherence is one of the central aspects of quantum mechanics, and create a median opposition to quantum computing. Quantum decoherence is what happens to a quantum system that interacts with its environment [194]. It describes how a quantum system loses its intrinsic quantum behaviour, and goes from a coherent quantum state to an incoherent classical state. Losing quantum behaviour is a bad thing for quantum calculations [195]. Error accumulation sets in, and after a relatively short time, it is no longer possible to increase the number of steps taken before all is lost.

Quantum systems obey another rule, one that stipulates that a particle can be in a superposition of states. That's what a qubit, the quantum computing analogue of a bit, is all about; it can be both 0 and 1 at the same time, unlike a classical bit, which can be either 0 or 1, but not both. This super positional property is absolutely key to the power of the quantum computer, because it allows high-speed computations in a way that is practically impossible for classical computers. But quantum systems are also extremely susceptible to the environment [196], [197]. As soon as a quantum system connects with its surroundings, for example, with electromagnetic fields, or with thermal radiation or cosmic rays, those fine-grained superposition states collapse due to decoherence. They collapse into classical states and lose their quantum coherence, because they begin to interact with each other. The coherence time of the qubit is the duration the qubit can maintains its quantum state before decohering. Because a quantum computation is merely the ability to maintain quantum coherence, this limits the time window of a computation before quantum computations accumulate large amounts of errors.

Decoherence injects noise and errors into a quantum computation. Suppose one of your qubits decohers, meaning they no longer 'interfere' as you need them to in order to produce the correct result for the quantum algorithm. Now they're in the wrong superposition to give you the answer you were after! This hinders the trustworthiness of your computation.

8.4. Quantum Error Correction (QEC)

A key component of quantum computing that tackles the inherent fragility of quantum states is quantum error correction [198]. The development of QEC and its main obstacles are essential to the advancement of quantum computing. Quantum error correction is more involved than classical error correction [199] because of the peculiar properties of quantum information. One such peculiarity is the quantum no-cloning theorem, the idea that you can't make an object that is an exact copy of an arbitrary unknown quantum state. Classical error correction doesn't share this problem because you can duplicate the data and cross-check it against the original so as to be able to pinpoint and correct errors. Furthermore, qubit errors are more varied than classical bit errors [200]. While classical bits have only

the option to flip, going from 0 to 1, or 1 to 0. Qubits can suffer bit flips as well as phase flips, and/or some combination of the two. This variety in the kinds of errors possible demands more sophisticated error correction codes that can correct for several error types at once [201]. Beyond that, quantum errors are also more easily propagated because of qubit entanglement. When one qubit in an entangled pair experiences an error, this error gets copied into the other qubit and from there into the entire system, making the correction harder.

8.5. Scalability

Scalability concerns whether a quantum processor can continue to grow the number of quality qubits while minimising the impact of errors [202]. Major quantum information processing applications require many qubits to interact with each other in order to solve useful problems. In essence, collected qubits have to interact with one another, which can dramatically increase the rate of choice-indeterminacy errors [203]. As the number of qubits grows, keeping their quality and their interactions all intact is much harder to achieve. This is why scalability concerns whether a quantum processor can continue to grow the number of quality qubits while minimising the influence of errors. Quite simply, another obstacle to scalability is the extreme fragility of qubits. Qubits are extremely sensitive to their environment, and even the slightest perturbation can cause a process called decoherence error [204]. Adding more qubits also requires more physical space and control systems to manage their interactions, increasing the susceptibility [205] of the system as a whole to noise and operational errors, things that need to be corrected.

8.6. “Collect Now, Break Later" Attacks

Quantum computing also introduces the risk of "collect now, break later" attacks. In this scenario, attackers could intercept and store encrypted data now, with the intention of decrypting it in the future when quantum computers become powerful and accessible enough [206]. This is a significant concern for sensitive data with a long shelf life, such as government, defense, financial, and medical information. The potential for such attacks means that organizations need to start thinking about quantum-safe encryption methods today to protect data that will still be sensitive in the future [207]. Quantum computing is believed to undermine most classical cryptographic algorithms currently in use in the public and private sector [208], [209]. These include RSA (Rivest-Shamir-Adleman), for protecting the confidentiality and integrity of communication, DSA (Digital Signature Algorithm), for providing authentication and non-repudiation, and ECC (Elliptic Curve Cryptography) [210], [211]. These algorithms are protections used in daily communications, most encrypted emails and secure online transactions rely on these methods. Quantum computers have the capability of solving hard combinatorial problems that are currently intractable for classical computers. Two of these are factoring large integers and computing discrete logarithms which underly RSA and ECC, respectively. Data of long-term value is particularly susceptible in this type of attack. Information in the federal, military, financial and medical fields is often of long-term interest, providing an ideal target. One part of the ‘collect now, break later’ threat that seems currently underappreciated is the long useful life of sensitive data. Classified information in government and defence communications could have dire national security consequences, even years after the communications took place. Financial records and transactions can impact matters of personal or corporate integrity. Medical records contain data that can be used to identify theft, other privacy violations or embarrassment [212], [213]. Since the quantum computers that might finally break today’s encryption might not exist for 10 or more years, the data that organisations want to keep secret for the long term needs to be protected as though it will finally fall to the implications of quantum computers.

9. Discussion

It has been shown that quantum computing offers immense computational power and enhanced network security, but significant privacy and security challenges, such as crosstalk attacks, qubit sensing attacks, quantum decoherence, error correction, and scalability concerns need to be addressed. These concerns are described in the sub-sections below.

9.1. Security Issues in Quantum networks

Quantum decoherence hinders the implementation of quantum computations due to its impact on the quantum system's behaviour. This loss of quantum nature, due to qubits' sensitive properties to environmental disturbances, reduces the accuracy of computations and reduces the trustworthiness of qubits, making it crucial to overcome decoherence in quantum computing technologies [214]. As such, Quantum error correction is a crucial development in quantum computing, enabling stable and reliable quantum computations [215]. Quanta are sensitive to their environment, and the quantum no-cloning theorem prevents exact copies of unknown states. Qubit errors, such as bit flips or phase flips, are easy to spread due to their entangled nature. Stable quantum computers can compute robust error correction schemes, enabling more precise quantum computation applications like factoring large numbers or simulating complex quantum many-body systems. Also, scalability is a significant challenge in quantum processor design and construction

[216]. It requires increasing the number of quality qubits while minimizing error impact on computation. This increases the rate of errors and requires maintaining control of interactions. Scaling the processor also requires scaling the quantum control systems, which may become large and noisy as qubits interact.

With 'collect now, break later' attacks, attackers intercept and store encrypted communications traffic now for possible decryption later, when the quantum computers of the future become powerful enough to break conventional 'classical' cryptography [217]. That future might come sooner than expected, since the most secure cryptographic algorithms [218] available today use informational inefficiencies of their own to withstand attackers. Quantum computers could solve otherwise-intractable problems such as integer factorisation (for example, breaking RSA encryption) and computing discrete logarithms (for example, breaking ECC, used by many mobile devices). Currently held encrypted secrets, such as government, defence, financial and healthcare data with a long-term lifespan, would be vulnerable to such collect now break later attacks until we have developed quantum-safe encryption methods [219]. This means that organisations handling highly sensitive information should begin moving toward quantum-safe encryption of their most sensitive data today, while it is still in storage. While we may not know exactly when we will need to 'go quantum' in order to protect ourselves from future quantum decryption capabilities, preparing to do so now will ensure data security in the quantum age.

9.2. Solutions to the security and privacy issues in quantum computing

The mitigation of the security and privacy issues in quantum computing involves developing quantum-resistant cryptographic algorithms and leveraging advanced cryptographic techniques such as post-quantum cryptography (PQC) and quantum key distribution (QKD). PQC focuses on creating algorithms that are secure against both classical and quantum attacks, ensuring the long-term protection of sensitive data. QKD, on the other hand, uses the principles of quantum mechanics to securely distribute cryptographic keys, providing a robust method for secure communication. Additionally, the implementation of homomorphic encryption and zero-knowledge proofs can further enhance data security and privacy by allowing computations on encrypted data and verifying statements without revealing sensitive information. These combined efforts aim to safeguard data against the potential threats posed by the advent of powerful quantum computers. The sub-sections below gives a description of these techniques.

9.2.1. Mitigation against quantum error correction

Another type of attack to mitigate is 'quantum error correction (QEC) attacks'. These require protecting from interference or exploitation the processes and mechanisms that safeguard the robustness of quantum computations. A critical example is the secure implementation of QEC codes [220] which redundantly encode quantum information (a qubit being encoded into multiple qubits] so that errors can be detected and corrected without measuring the quantum state directly [221]. Verification of the integrity of the encoding and decoding processes can protect against remote interference or tampering with the correctness of the processes by attackers [222]. For example, authenticated encoding and authenticated decoding could be used to safeguard the integrity and authenticity of the QEC operations. Also, a very important issue to address is the secure use of error syndromes in QEC [223]. Error syndromes are information derived from measurements used to detect errors in quantum states. We need to be able to prove to each other that the syndromes have been recorded and not tampered with or 'injected' with fake signals. Cryptographic techniques [224] can be used to encrypt and authorize syndromes and error-correction data so that only the relevant parties can read or change it.

Equally important are physical security measures, which limit the possibility of direct assaults upon qubits and quantum hardware. The importance of security provisions, like unregistered facility access and authentication protocols to ensure that users are who they say they are. There are mutual-exclusion protocols [225], and tamper-resistant hardware that limit the risk of physical access to and tampering with quantum computing components. Further, these methods of forming quantum firewalls can cordon off modules for error correction within the quantum system such that unauthorised access to QEC operations cannot infect the larger operation of quantum computations. Continuous monitoring, such as intrusion detection systems [226], can help pinpoint the possibility of intrusions into a quantum computing environment, attempting to access information through improper means, or displaying unusual behaviour where it is not expected. Monitoring in real time can alert stakeholders to possible QEC attacks when they are in progress, and as soon as they occur. The computer-aided mitigation of the attack can be deployed as quickly as possible to minimize the damage to quantum information. Besides, quantum key distribution, or QKD, protocols can be used to improve security. These protocols encode messages in light particles and enable provable security of communication channels within the quantum system, which can be used to create unbreakable encryption keys [227[for sensitive data and communication, even during the error-correcting process.

9.2.2. Mitigation against quantum decoherence

Traditional light, which doesn't take advantage of quantum coherence, maximises the coding bandwidth for storing information and maximises the signal-to-noise ratio of detectors by avoiding quantum indeterminism. However, from recent findings in metrology, we know that quantum coherence is essential to achieve the best sensitivity of a high-precision force sensor based on laser interferometric force sensing [228], [229]. In particular, both gravitational-wave detection and optomechanics widely rely on the squeezing of quantum-correlated light. Light squeezed on the phase or amplitude quadrature generally enjoys better noise reduction than ordinary light, which supports the development of advanced experiments. However, quantum indeterminism does come with some downsides, such as quantum decoherence. The effects of squeezing the light within the cavity are thought to be able to without significantly distorting the measurement outcomes, beat down the detrimental quantum decoherence effects.

9.2.3. Mitigation to collect now break later attacks

Against 'collect now break later' attacks that are beginning to emerge, the only approach is for organisations to combine several mitigations in order to harden their cryptographic defenses, especially for the post-quantum world. The first step towards improving the security of any encryption is to minimize the risk of breach of encrypted data [230]. Operational measures to reduce the scope of a breach include 'micro-segmentation' of data. Meaning that data is broken up into smaller segments that are encrypted and independently controlled by separate access controls [231]. In this way, breaches of individual segments will have a much lower chance of compromising all data across an organisation. Another processing policy is to use different rotation schedules for encryption keys for data of different classification [232]; this means that if their control is breached, encryption keys for one type of data or transaction simply won't apply to others. Furthermore, the most obvious, it's essential to keep encryption software up to date with the latest security patches and improvements [233]. This mitigates 'chinks in the armour' that could be exploited in future, whether for years or decades to come. Moreover, organisations who store important data such as trade secrets or medical records are encouraged to use higher grades of encryption. This ensures that measures are in place to protect data against any future ability to decrypt it, which would otherwise be possible by exploiting new quantum computer capabilities [234].

We also suggest a phased approach to transitioning cryptography. Rather than immediately ripping out legacy algorithms for post-quantum algorithms that, despite years of research, might still not have been proven yet, organizations could phase the new encryption in with their existing encryption. A mixed approach allows them to take advantage of the best of both worlds, minimize their risk exposure to potentially dangerous and bug-ridden new technologies, and also recognize that, given how immature some of this technology is, there's a good chance it's going to take a while to catch up. Finally, adopting crypto-agility [235] provides another crucial means for preparing for future change in cryptographic algorithms and standards. Being forward-looking can combat the risk of building brittle infrastructure and can ensure that there will be little delay in adopting security measures as new cryptographic algorithms and standards become necessary.

9.2.4. Mitigation to qubit sensing attack

Quantum computing is especially vulnerable to privacy issues via a class of assault vectors called error sensing attacks [236]. In such attacks, an adversary tries to infer information about a computation that was run on a user's behalf by analysing the error patterns in the output of the quantum computer. A general and powerful countermeasure to such a privacy problem is called randomised output flipping [237], [238]. The technique of randomising output error-flipping is used to obscure the error patterns that result from quantum computations while they are underway. The basic concept is, if you can flip an output bit with some probability, your adversary's ability to make inferences based on the error signature is likely to be misleading to them. It's a noisy output, which would lead them astray. The technique of randomised output flipping is rather simple to implement. At the end of a quantum computation, right after each output bit has been measured, the calculated result is flipped with a fixed probability. This probability needs to be determined carefully in order to strike the right balance in the trade-off between security and the quality of the computation, but randomizing the output hides the error patterns well enough to minimize penetration without significantly degrading the outcome of the computation. Randomized output flipping gives us a general and universal defence mechanism that can secure any quantum computation [239], protecting valuable information and guaranteeing the privacy of quantum networks.

9.2.5. Mitigation on quantum safe cryptography

A first line of defense against these threats is to ensure that the relevant cryptographic algorithms would still be secure in case a malicious quantum computer would be built. Any such algorithm should be quantum-safe [240], that is, be resilient against attacks from such a machine. Research on quantum-safe 'post-quantum' cryptography (PQC) is still underway. Such quantum-safe algorithms are based on certain hard mathematical problems that are not susceptible to

quantum attack. The three frontrunners are lattice-based cryptography, hash-based cryptography, and code-based cryptography [241]-[243]. A lesser-known but still plausible candidate is multivariate polynomial cryptography [244] . All these approaches rely on a different class of hard mathematical problems that are not believed to be easy to solve for near-term quantum algorithms, contrary to Shor's algorithm. The move to quantum-safe cryptographic standards will be complex and difficult. It means a vast migration of cryptographic infrastructure (software, hardware, protocols) [245] that has been built over decades, taking years to plan, implement and roll out. There will be decisions about which systems and data are a priority for transition, given the sensitivity of the data and the lifespan for which it will be kept. Additionally, there are considerations for the need to maintain interoperable functionality between classical and quantum-safe systems during the transition period. However, the move to quantum-safe cryptography hinges on co-ordination between governments, industry and academia. Standards and regulatory bodies within government need to set the rules; industry stakeholders have to shoulder the costs associated with innovation and engineering quantum-safe solutions for their products and services; and academic researchers need to further develop the theory behind quantum-safe algorithms [246], and prototypes of the practical implementations of these emerging algorithms.

10. The Challenges of current solutions

Implementing solutions to the security and privacy issues posed by quantum computing faces several significant challenges. Developing and standardizing post-quantum cryptographic algorithms is a complex and time-consuming process, requiring rigorous testing to ensure their robustness and efficiency against quantum attacks. QKD protocols, while theoretically secure, are expensive to deploy and require specialized hardware, limiting their practical scalability and integration into existing infrastructures. Additionally, technologies like homomorphic encryption and zero-knowledge proofs, although promising, often involve substantial computational overhead, making them less practical for real-time applications. Furthermore, transitioning current systems to quantum-resistant protocols involves significant logistical and financial efforts, necessitating widespread coordination and cooperation across various sectors to ensure a seamless and secure upgrade.

10.1. Quantum error correction gaps

QEC is necessary because quantum computations may be disrupted by quantum decoherence. Unlike classical error correction, which is widely understood and quite simple in most cases, QEC is far from trivial. There are two main and fundamental obstacles with QEC. First, quantum errors are far more tenacious than classical errors [247], and second, quantum mechanics places severe constraints on the procedure. Errors on conventional computers are exceedingly rare, things such as bit-flips occur less than once for every 108 operations. If quantum computers did suffer from errors only at this rate, classical error correction could be easily imported into the quantum realm. Unfortunately, quantum computers generate errors even more frequently [248], and at much higher complexity, they suffer from bit-flips, phase flips, or, even worse, combinations of bit and phase flips. One of the big problems in QEC is that you can't copy qubits the way you can copy classical bits. This is a fundamental restriction known as the no-cloning theorem [249], [250]. The reason we need techniques like quantum error correction is that any quantum information requires protecting against decoherence, noise and imperfections in its quantum nature. QEC techniques encode a single logical qubit into multiple physical qubits, the number depends on the particular hardware, algorithm and application, with more physical qubits required for faster error rates. There are many QEC codes but the basic idea is to encode quantum information in some way and hence need more physical qubits than to encode just one.

10.2. Scalability gaps

Scalability means increasing the number of qubits in a quantum system, so that you can solve more complex problems [251]. You have to start by getting errors in a qubit, which are very easy, because these systems are massively sensitive to little interferences. If you build large systems from those few qubits linked together as a circuit, the probability of errors rapidly grows. One potential solution is error correction, which forces redundancy [252] in the system so that it is able to recognize the probability that there is some glitch, and then correct it. However, both the redundancy and the techniques to correct it impose additional layers of complexity. The current record for the number of qubits in one quantum computer stands at 1180. Factoring a 2048-bit integer in eight hours requires around 20 million physical qubits. That would be enough to withstand the natural errors in superconducting circuits, using surface code error correction. IBM estimates the first 1 million-qubit quantum computer may be realised by 2030, while Google expects it to arrive in by 2029 [253]. The quantum-computing start-up PsiQuantum hopes to create a 1 million-qubit quantum computer with error correction that they plan to ship in 2025 using photonic qubits.

10.3. Trained personel

Building up a skilled workforce is a huge challenge for the quantum computing field as well. The pool of people who are properly educated and trained in quantum technologies is pretty small and geographically dispersed. The scarcity of skilled workers is a major bottleneck. Building a workforce of programmers, computer scientists, engineers and support staff capable of developing usable quantum [254] computers is a huge task, but this is exactly what has to happen if innovation in the field is going to accelerate. On the other hand, attracting more people to the field waiting for quantum computers to get practical.

10.4. High expense involved

One of the biggest challenges of quantum networking is its cost. This cost is partly due to the requirements of advanced technology and large investments into the infrastructural facilities and on-going research and development [255]. For instance, QKD systems need long-distance communication to establish the secure key, which involves the investment of fibre optical cables or satellite systems [256], both of which have high launch and operation costs. Additionally, building a world network for quantum communications demands that we have the best quality cables or satellite navigation systems. Such cables require costly installation and persevering maintenance. The operational and maintenance costs of quantum networking are also high, as quantum devices require extremely low temperatures and a great deal of isolation to operate [257]. These conditions are expensive to maintain, and the fast evolution of technology means frequent and costly upgrades of the equipment are necessary. Finally, high salaries for scientists and engineers in this new research field are expensive since other industries are now vying for their limited skills and knowledge. The high costs of quantum networking will have a significant impact on restricting access to the market for both consumers and enterprise customers who, in the face of higher prices, reduced availability and potential high costs for substitutes, may either wait or search for alternatives until the technology demonstrates that it represents real value. Reduced availability due to lack of competition among suppliers and the high costs of adoption mean that industries may lean towards alternative, cheaper and less complex but less secure options . Government funding for research and development, along with public-private partnerships, can also ease financial dependency in the initial stages and spread costs.

11. Negative Impacts on Privacy and Security

11.1. Breaking Traditional Cryptography

Quantum versions of Shor's Algorithm would allow a quantum computer to factorise large integers exponentially faster than the best-known algorithms for classical computers [258], making RSA and also the cryptosystems ECC [259] that are used to protect information between mobile devices, completely insecure to hack. The Grover's algorithm is a quadratically faster search algorithm for unsorted databases that threatens symmetric key cryptography (ie, AES, etc), reducing such a key's length in half, from say 256-bit to 128-bit length.

11.2. Data Harvesting

Adversaries could take the 'store now, decrypt later' option, in case they're able to decipher the ciphertext in the future [260], perhaps with a quantum computer that becomes available sometime in the distant present.

12. Research gaps

Despite significant progress in quantum computing and its potential applications for network security, several research gaps need to be addressed to ensure robust and practical implementations. Table 1 presents an illustration of the research gaps in quantum computing for network security.

Table 1 Research gaps

Gaps	Information
Scalability and Stability of Quantum Computers	*Scalability* *Large-Scale Qubit Integration*: Current quantum computers operate with a limited number of qubits [261]. Scaling up to hundreds or thousands of qubits while maintaining coherence and error rates is a significant challenge.

	Error Rates: As the number of qubits increases, so does the complexity of error correction. Developing scalable quantum error correction methods that can handle large-scale qubit systems is critical. *Stability* *Qubit Coherence Time*: Qubits are susceptible to decoherence, where they lose their quantum state due to interaction with the environment. Extending the coherence time of qubits is essential for reliable quantum computation. *Noise Reduction*: Reducing the noise in quantum systems, which affects the fidelity of quantum operations, is a major research focus. Noise-resilient qubit designs and error mitigation techniques are needed [262].
Post-Quantum Cryptography (PQC)	*Algorithm Development* *Efficient Algorithms*: While various post-quantum cryptographic algorithms have been proposed (e.g., lattice-based, code-based, hash-based), further research is needed to develop algorithms that are not only secure but also efficient and practical for widespread use. *Standardization*: The process of standardizing post-quantum cryptographic algorithms is ongoing. Contributions to international standardization efforts, such as those by NIST, are crucial for ensuring widespread adoption. *Performance and Usability* *Performance Optimization*: Many post-quantum algorithms have high computational overheads compared to classical cryptographic algorithms [263]. Optimizing these algorithms for performance without compromising security is a key challenge. *Integration with Existing Systems*: Research is needed on how to seamlessly integrate post-quantum cryptographic algorithms into existing systems and protocols, ensuring backward compatibility and ease of transition.
Quantum Key Distribution (QKD)	*Practical Implementation* *Long-Distance QKD*: Implementing QKD over long distances remains a challenge due to photon loss and decoherence in optical fibers [264]. Research into quantum repeaters and satellite-based QKD is essential to extend the range of secure quantum communication. *Deployment in Real-World Networks*: Practical deployment of QKD in existing network infrastructures requires overcoming challenges related to cost, complexity, and compatibility with current communication technologies. *Security and Reliability* *Security Proofs*: While QKD is theoretically secure [265], rigorous security proofs for practical implementations, considering real-world imperfections and attack vectors, are necessary. *Reliability and Robustness*: Ensuring the reliability and robustness of QKD systems in various environmental conditions and operational scenarios is a critical area of research.
Quantum-Resistant Network Protocols	*Protocol Design* *Hybrid Protocols*: Developing hybrid network protocols that combine classical and quantum-resistant cryptographic techniques can provide security during the transition period to fully quantum-resistant systems. *New Protocols*: Designing entirely new network protocols that leverage quantum-resistant cryptographic techniques from the ground up is also a significant research area. *Implementation and Testing* *Practical Testing*: Real-world testing and validation of quantum-resistant protocols in diverse network environments are necessary to ensure their effectiveness and reliability. *Performance Metrics*: Establishing performance metrics and benchmarks for quantum-resistant network protocols to compare their efficiency and security with classical counterparts.
Quantum Algorithms for Security Applications	*Quantum Cryptanalysis* *Understanding Quantum Threats*: Research into quantum algorithms that can break classical cryptographic schemes (e.g., Shor's algorithm, Grover's algorithm) is essential to understand the potential threats and develop countermeasures. *Algorithm Optimization*: Optimizing quantum cryptanalysis algorithms for practical use, including reducing resource requirements and improving execution speed, is an ongoing area of research.

	Quantum Machine Learning (QML) for Security *Anomaly Detection*: involves developing QML algorithms [266] for detecting network anomalies and intrusions with higher accuracy and efficiency than classical methods. *Privacy-Preserving Computation*: Researching QML techniques that ensure privacy-preserving [267] computations, protecting sensitive data while leveraging quantum machine learning capabilities.
Legal and Ethical Considerations	*Regulatory Frameworks* *Legal Standards*: Developing legal and regulatory frameworks for the deployment and use of quantum cryptographic technologies in various sectors, ensuring compliance with privacy and security laws. *Ethical Implications*: Addressing the ethical implications of quantum computing in network security, including issues related to surveillance, privacy, and the balance between security and civil liberties. *Policy Development* *Government Policies*: Formulating government policies that support research and development in quantum computing and network security, including funding, international collaboration, and public-private partnerships. *Standards and Guidelines*: Establishing standards and guidelines for the secure implementation and use of quantum computing technologies in network security.
Quantum-Safe Blockchain and Distributed Ledger Technologies	*Quantum-Resistant Consensus Mechanisms* *New Consensus Protocols*: Researching and developing new consensus mechanisms for blockchain and distributed ledger technologies that are resistant to quantum attacks [268]. *Implementation Challenges*: Addressing the practical challenges of implementing quantum-resistant consensus mechanisms, including scalability, efficiency, and interoperability with existing blockchain systems. *Security and Privacy Enhancements* *Quantum-Enhanced Privacy*: Exploring how quantum computing can enhance privacy in blockchain systems, such as through quantum-secure smart contracts and private transactions [269]. *Resistance to Quantum Attacks*: Ensuring that blockchain systems and digital assets remain secure against potential quantum attacks, including research into new cryptographic schemes for securing blockchain data.

Mitigating these research gaps is essential for leveraging the full potential of quantum computing in network security while mitigating its associated risks. By focusing on scalability, practical implementation, performance optimization, protocol design, legal and ethical considerations, and education, the research community can develop robust quantum-resistant solutions that ensure the security and privacy of future network systems.

13. Future research scope

In this section, several promising avenues for further research are explored. One key area is the advancement and optimization of post-quantum cryptographic algorithms, focusing on making them more efficient and easier to implement in real-world applications. Additionally, enhancing QKD protocols to be more cost-effective and scalable is crucial for broader adoption. Research is also likely to delve into integrating quantum-resistant cryptographic methods seamlessly with existing systems, ensuring minimal disruption during the transition. Another exciting frontier is developing practical applications of homomorphic encryption and zero-knowledge proofs, aimed at reducing computational overhead while maintaining security and privacy. Furthermore, exploring hybrid models that combine classical and quantum techniques to bolster security measures could offer a balanced approach to protecting data in the quantum era. These research efforts will be vital in addressing the evolving challenges posed by quantum computing and ensuring robust network security in the future. Other future research domains are discussed below.

13.1. Security and vulnerability analysis

Security work focuses on quantum-safe cryptographic algorithms and quantum attack resistance – vetted older algorithms designed to operate under the noisy realities of current devices, new algorithms, as well as side-channel attacks [270]. Asymmetric key protocols (such as RSA) will either need to be replaced or need to be made resistant to quantum attack. Developing resilient protocols for quantum networks to protect against attack, while dealing with the inevitable errors of quantum devices, is a new challenge as well.

13.2. Technological Development

Through longer qubit coherence times, reduced error rates and increased stability of devices, progress in quantum hardware is being made. Interoperability standards [271] are being considered for cross-manufacturer communication, and new manufacturing methods and system design approaches for reducing the cost of quantum networking hardware architecture and components are being researched to propel the necessary infrastructure forward.

13.3. Practical Applications and Deployment

Applied research is needed to study potential real-world applications, for example, fast and secure financial transactions, and the use of large datasets for improving government communications and services. Experimental pilot projects, case studies and benchmarking can be useful for illustrating real-world benefits. This includes investigation of use and enterprise adoption factors, economic analysis and business cases, as well as regulatory approaches to ensure safe implementation of quantum networks. In summary, future of quantum computing in network security presents a vast landscape of research opportunities. As quantum technology advances, addressing emerging challenges and harnessing new possibilities will be crucial. Table 2 gives detailed future research scopes in quantum computing for network security.

Table 2 Future research scopes

Scope	Information
Advanced Quantum Cryptographic Protocols	*Novel Quantum Key Distribution (QKD) Protocols* *Device-Independent QKD*: Developing protocols that ensure security without relying on the trustworthiness of the quantum devices used [272]. This addresses vulnerabilities due to device imperfections. *Measurement-Device-Independent QKD*: Enhancing security by making the system immune to all possible loopholes in the measurement devices, thereby reducing the risk of side-channel attacks. *Quantum Digital Signatures* *Secure Quantum Signing*: Researching methods for secure quantum digital signatures [273] that can replace classical digital signatures and are resistant to quantum attacks. *Scalable Protocols*: Developing scalable quantum digital signature schemes that can be efficiently [274] implemented in large-scale networks.
Quantum-Resistant Cryptographic Algorithms	*Lattice-Based Cryptography* *Performance Optimization*: Enhancing the efficiency of lattice-based cryptographic algorithms [275] to make them practical for widespread use in real-time applications. *Security Proofs*: Providing rigorous security proofs for lattice-based schemes under various attack models, including those that leverage quantum computing. *Code-Based Cryptography* *Efficient Implementation*: Improving the implementation of code-based cryptographic algorithms to reduce computational overhead and make them viable for everyday use. *Error-Correcting Codes*: Exploring new types of error-correcting codes that provide stronger security guarantees against quantum attacks. *Multivariate Quadratic Equations* *Algorithm Development*: Developing new cryptographic schemes based on the hardness of solving multivariate quadratic equations, which are believed to be secure against quantum attacks. *Practical Applications*: Identifying practical applications for these schemes in securing communications and transactions.
Quantum-Safe Network Architectures	*Quantum Internet* *Network Infrastructure*: Designing and building a quantum internet infrastructure [276] that supports quantum communication across global networks. *Protocol Standardization*: Establishing standardized protocols for quantum internet communications to ensure interoperability and security. *Quantum Routers and Switches*

	Device Development: Developing quantum routers and switches that can handle quantum data and route it securely through quantum networks. *Efficiency and Scalability*: Ensuring that these devices are efficient and scalable for large-scale deployment.
Quantum-Secure Blockchain and Distributed Ledger Technologies	*Quantum-Resistant Consensus Mechanisms* *New Consensus Algorithms*: Researching and developing new consensus algorithms for blockchain systems [277] that are resistant to quantum attacks. *Security and Performance*: Balancing security and performance in these new consensus mechanisms to ensure they are both secure and practical for use. *Quantum-Safe Smart Contracts* *Design and Implementation*: Designing smart contracts that use quantum-resistant cryptographic techniques [278] to ensure their security against quantum attacks. *Use Cases*: Exploring use cases for quantum-safe smart contracts in various industries, such as finance, healthcare, and supply chain management.
Quantum Machine Learning (QML) for Network Security	*Anomaly Detection* *Advanced Algorithms*: Developing QML algorithms that can detect network anomalies and intrusions with higher accuracy and efficiency than classical methods [279]. *Real-Time Monitoring*: Implementing these algorithms in real-time network monitoring systems to provide early detection and response to security threats. *Privacy-Preserving Computation* *Federated Learning*: Researching QML techniques that enable privacy-preserving [280] federated learning, where multiple parties collaboratively train models without sharing their data. *Secure Data Analysis*: Ensuring that sensitive data remains secure during the training and analysis processes.
Integration of Quantum and Classical Systems	*Hybrid Cryptographic Systems* *Transition Strategies*: Developing strategies for transitioning from classical to quantum-resistant cryptographic systems, including the use of hybrid systems that combine both. *Interoperability*: Ensuring that quantum and classical systems can work together seamlessly, maintaining security and performance [281]. *Quantum-Safe Protocols* *Protocol Design*: Designing network protocols that are secure against quantum attacks while being compatible with existing classical systems [282], [283]. *Testing and Validation*: Conducting extensive testing and validation of these protocols in real-world scenarios to ensure their effectiveness.
Quantum-Enhanced Privacy Technologies	*Homomorphic Encryption* *Quantum Homomorphic Encryption*: Researching quantum homomorphic encryption techniques that allow computations on encrypted data without decrypting it, enhancing data privacy [284], [285]. *Efficiency Improvements*: Improving the efficiency of these techniques to make them practical for use in various applications. *Zero-Knowledge Proofs* *Quantum Zero-Knowledge Proofs*: Developing quantum zero-knowledge proofs that allow one party to prove to another that they know a value without revealing the value itself [286]. *Applications*: Exploring applications of quantum zero-knowledge proofs in areas such as authentication [287], identity verification, and secure voting.
Quantum Hardware and Physical Layer Security	*Quantum Hardware Security* *Tamper-Resistant Qubits*: Developing tamper-resistant qubits and quantum hardware that prevent unauthorized access and manipulation [288]-[291]. *Physical Layer Security*: Researching physical layer security techniques that leverage quantum properties to protect data at the hardware level [292]. *Quantum-Safe IoT Devices*

	Secure IoT Architectures: Designing IoT architectures that incorporate quantum-resistant cryptographic techniques to ensure the security of IoT devices and networks. *Lightweight Cryptography*: Developing lightweight quantum-resistant cryptographic algorithms [293] suitable for resource-constrained IoT devices.

Evidently, future of quantum computing in network security is rich with research opportunities that span multiple disciplines and address critical challenges. By focusing on the development of advanced cryptographic protocols [294], quantum-resistant algorithms, quantum-safe network architectures [295], and ethical and legal frameworks, the research community can ensure that quantum computing enhances network security while mitigating its associated risks.

14. Conclusion

The findings imply that quantum computing is neither the solution to problems in network security nor a reason for pessimism. In fact, it is a revolutionary improvement in terms of computational power that may help enhance network security, and the vulnerabilities of quantum computers also have the potential to be an impetus for enhanced security measures. Beyond these operational concerns, a major vulnerability arises from the shared quantum computing environment itself. Such aggregate quantum systems lend themselves naturally to crosstalk attacks, in which interference by a malicious third party with physical proximity to honest qubits disrupts their computations. A second major vulnerability to shared-quantum computing environments involves attack vectors known as qubit sensing attacks. In these attacks, errors in readout affect successive computations on the same qubit, leading to flawed results and occasional breaches of sensitive information. Another vital issue is quantum decoherence, which interferes with the robustness of quantum states. Decoherence disrupts quantum coherence, thereby causing the wave function to 'collapse' into one or another classical states and introduce errors in the computations. This phenomenon severely constrains the time during which the quantum systems remain in their operational lifetime, marked by their computational accuracy, thereby diminishing the trustworthiness of the quantum operations. Quantum Error Correction [QEC] is indispensable for such tasks, yet current approaches are inadequate for coping with the broad range of errors inherent to quantum systems. The development of advanced QEC techniques will be essential for mitigating the myriad forms of errors that quantum hardware will encounter, thus paving the way for trusted quantum computation. Another major challenge is scalability. Practical quantum computing depends on amplifying the number of qubits in a quantum system. But the more qubits you add, the harder it is to maintain the quality of them, and the more difficult it is to correct for errors. So, while it is theoretically straightforward to create stable 100- or 1,000-qubit systems in principle, these systems would be extremely difficult to build. In other words, a lot of further innovation is necessary to overcome the practical technical challenges of scaling up quantum systems to a workable size. Second, for a lot of sensitive long-term information, decades from today is still too soon to risk cryptanalytic breach from an attack known only as 'collect now, break later'. For example, quantum computers are likely at some point to break today's encryption methods, including those widely used in the past. This, too, represents the need to start working now on quantum-safe encryption methods, to protect long-term data into the distant future, especially in government, defense, finance and health and other sensitive areas.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that he holds no conflict of interest.

References

[1] Hidary JD, Hidary JD. Quantum computing: an applied approach. Cham: Springer; 2019 Aug 29.

[2] Ahmadi A. Quantum Computing and Artificial Intelligence: The Synergy of Two Revolutionary Technologies. Asian Journal of Electrical Sciences. 2023 Nov 2;12(2):15-27.

[3] Hossain KA. The potential and challenges of quantum technology in modern era. Scientific Research Journal. 2023 Jun;11(6).

[4] Buchanan W, Woodward A. Will quantum computers be the end of public key encryption?. Journal of Cyber Security Technology. 2017 Jan 2;1(1):1-22.

[5] Mattsson JP, Smeets B, Thormarker E. Quantum-resistant cryptography. arXiv preprint arXiv:2112.00399. 2021 Dec 1.

[6] 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.

[7] 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.

[8] Hassanzadeh P. Towards the quantum-enabled technologies for development of drugs or delivery systems. Journal of Controlled Release. 2020 Aug 10;324:260-79.

[9] Bayerstadler A, Becquin G, Binder J, Botter T, Ehm H, Ehmer T, Erdmann M, Gaus N, Harbach P, Hess M, Klepsch J. Industry quantum computing applications. EPJ Quantum Technology. 2021 Dec 1;8(1):25.

[10] Córcoles AD, Kandala A, Javadi-Abhari A, McClure DT, Cross AW, Temme K, Nation PD, Steffen M, Gambetta JM. Challenges and opportunities of near-term quantum computing systems. Proceedings of the IEEE. 2019 Dec 19;108(8):1338-52.

[11] Singh SK, Azzaoui AE, Salim MM, Park JH. Quantum communication technology for future ICT-review. Journal of Information Processing Systems. 2020;16(6):1459-78.

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

[13] 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.

[14] Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. Reviews of modern physics. 2020 Apr 1;92(2):025002.

[15] 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.

[16] Aji A, Jain K, Krishnan P. A Survey of Quantum Key Distribution (QKD) network simulation platforms. In2021 2nd Global Conference for Advancement in Technology (GCAT) 2021 Oct 1 (pp. 1-8). IEEE.

[17] Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. npj Quantum Information. 2017 Aug 9;3(1):30.

[18] Ajagekar A, You F. Quantum computing for energy systems optimization: Challenges and opportunities. Energy. 2019 Jul 15;179:76-89.

[19] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[20] 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.

[21] Alshaer NA, Ismail TI. AI-Driven Quantum Technology for Enhanced 6G networks: Opportunities, Challenges, and Future Directions. Journal of Laser Science and Applications. 2024 Jul 1;1(1):21-30.

[22] Jawad AT, Maaloul R, Chaari L. A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges. Computer Networks. 2023 Nov 6:110085.

[23] Ansere JA, Tran DT, Dobre OA, Shin H, Karagiannidis GK, Duong TQ. Energy-efficient optimization for mobile edge computing with quantum machine learning. IEEE Wireless Communications Letters. 2023 Dec 5.

[24] Alqahtani H, Kumar G. Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems. Engineering Applications of Artificial Intelligence. 2024 Mar 1;129:107667.

[25] 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.

[26] Wong YK. Understanding the Fundamentals of Quantum Computing. International Journal of Computer Science Trends and Technology. 2022 Apr;10(2):xx-.

[27] Alexeev Y, Amsler M, Barroca MA, Bassini S, Battelle T, Camps D, Casanova D, Choi YJ, Chong FT, Chung C, Codella C. Quantum-centric supercomputing for materials science: A perspective on challenges and future directions. Future Generation Computer Systems. 2024 Nov 1;160:666-710.

[28] Mohanaprabhu D, Monish Kanna SP, Jayasuriya J, Lakshmanaprakash S, Abirami A, Tyagi AK. Quantum Computation, Quantum Information, and Quantum Key Distribution. Automated Secure Computing for Next-Generation Systems. 2024 May 3:345-66.

[29] Yuan G, Chen Y, Lu J, Wu S, Ye Z, Qian L, Chen G. Quantum Computing for Databases: Overview and Challenges. arXiv preprint arXiv:2405.12511. 2024 May 21.

[30] Gill SS, Buyya R. Transforming Research with Quantum Computing. Journal of Economy and Technology. 2024 Jul 18.

[31] 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).

[32] Dutta T, Jin A, Huihong CL, Latorre JI, Mukherjee M. Trainability of a quantum-classical machine in the NISQ era. arXiv preprint arXiv:2401.12089. 2024 Jan 22.

[33] Jahanbani S, Zhang ZH, Hua B, Godeneli K, Müllendorff B, Zhang X, Zhou H, Sipahigil A. A Nanomechanical Atomic Force Qubit. arXiv preprint arXiv:2407.15387. 2024 Jul 22.

[34] Tuokkola M, Sunada Y, Kivijärvi H, Grönberg L, Kaikkonen JP, Vesterinen V, Govenius J, Möttönen M. Methods to achieve near-millisecond energy relaxation and dephasing times for a superconducting transmon qubit. arXiv preprint arXiv:2407.18778. 2024 Jul 26.

[35] Gu X, Fernández-Pendás J, Vikstål P, Abad T, Warren C, Bengtsson A, Tancredi G, Shumeiko V, Bylander J, Johansson G, Kockum AF. Fast multiqubit gates through simultaneous two-qubit gates. PRX Quantum. 2021 Dec 1;2(4):040348.

[36] Zhang Y, Deng H, Li Q, Song H, Nie L. Optimizing quantum programs against decoherence: Delaying qubits into quantum superposition. In2019 International Symposium on Theoretical Aspects of Software Engineering (TASE) 2019 Jul 29 (pp. 184-191). IEEE.

[37] Li Z, Xue K, Li J, Chen L, Li R, Wang Z, Yu N, Wei DS, Sun Q, Lu J. Entanglement-assisted quantum networks: Mechanics, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials. 2023 Jul 11.

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

[39] Nedjah N, Raposo S, de Macedo Mourelle L. Dedicated hardware design for efficient quantum computations using classical logic gates. The Journal of Supercomputing. 2024 Mar;80(5):7028-70.

[40] Bhattacharjee J, Deyasi A. Quantum Logic Gate–Based Circuit Design for Computing Applications. InIntelligent Quantum Information Processing 2024 (pp. 157-188). CRC Press.

[41] Shafique MA, Munir A, Latif I. Quantum Computing: Circuits, Algorithms, and Applications. IEEE Access. 2024 Feb 6.

[42] Du Y, Huang T, You S, Hsieh MH, Tao D. Quantum circuit architecture search for variational quantum algorithms. npj Quantum Information. 2022 May 23;8(1):62.

[43] Daei O, Navi K, Zomorodi-Moghadam M. Optimized quantum circuit partitioning. International Journal of Theoretical Physics. 2020 Dec;59(12):3804-20.

[44] Iten R, Moyard R, Metger T, Sutter D, Woerner S. Exact and practical pattern matching for quantum circuit optimization. ACM Transactions on Quantum Computing. 2022 Jan 21;3(1):1-41.

[45] 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.

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

[47] 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.

[48] 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.

[49] Trizna A, Ozols A. An overview of quantum key distribution protocols. Inf. Technol. Manage. Sci. 2018 Dec 1;21:37-44.

[50] Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Quantum cryptography with realistic devices. arXiv preprint arXiv:1903.09051. 2019 Mar.

[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] Nurhadi AI, Syambas NR. Quantum key distribution (QKD) protocols: A survey. In2018 4th International Conference on Wireless and Telematics (ICWT) 2018 Jul 12 (pp. 1-5). IEEE.

[53] 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.

[54] 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.

[55] Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R. Post-quantum lattice-based cryptography implementations: A survey. ACM Computing Surveys (CSUR). 2019 Jan 28;51(6):1-41.

[56] Khalid A, McCarthy S, O'Neill M, Liu W. Lattice-based cryptography for IoT in a quantum world: Are we ready?. In2019 IEEE 8th international workshop on advances in sensors and interfaces (IWASI) 2019 Jun 13 (pp. 194-199). IEEE.

[57] Sendrier N. Code-based cryptography: State of the art and perspectives. IEEE Security & Privacy. 2017 Aug 17;15(4):44-50.

[58] 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.

[59] Bernstein DJ, Yang BY. Asymptotically faster quantum algorithms to solve multivariate quadratic equations. InInternational Conference on Post-Quantum Cryptography 2018 Apr 1 (pp. 487-506). Cham: Springer International Publishing.

[60] Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Reviews of Modern Physics. 2017 Jan 1;89(1):015004.

[61] Ma X, Yuan X, Cao Z, Qi B, Zhang Z. Quantum random number generation. npj Quantum Information. 2016 Jun 28;2(1):1-9.

[62] 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.

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

[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] Sheng YB, Zhou L, Long GL. One-step quantum secure direct communication. Science Bulletin. 2022 Feb 26;67(4):367-74.

[66] Qi Z, Li Y, Huang Y, Feng J, Zheng Y, Chen X. A 15-user quantum secure direct communication network. Light: Science & Applications. 2021 Sep 14;10(1):183.

[67] Munro WJ, Azuma K, Tamaki K, Nemoto K. Inside quantum repeaters. IEEE Journal of Selected Topics in Quantum Electronics. 2015 Jan 15;21(3):78-90.

[68] Ruihong Q, Ying M. Research progress of quantum repeaters. InJournal of Physics: Conference Series 2019 Jun 1 (Vol. 1237, No. 5, p. 052032). IOP Publishing.

[69] Suo J, Wang L, Yang S, Zheng W, Zhang J. Quantum algorithms for typical hard problems: a perspective of cryptanalysis. Quantum Information Processing. 2020 Jun;19:1-26.

[70] 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.

[71] Martín-Guerrero JD, Lamata L. Quantum machine learning: A tutorial. Neurocomputing. 2022 Jan 22;470:457-61.

[72] Dunjko V, Wittek P. A non-review of quantum machine learning: trends and explorations. Quantum Views. 2020 Mar 17;4:32.

[73] 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.

[74] Gomes J, Khan S, Svetinovic D. Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience. IEEE Access. 2023 Jul 18.

[75] Thanalakshmi P, Rishikhesh A, Marion Marceline J, Joshi GP, Cho W. A quantum-resistant blockchain system: a comparative analysis. Mathematics. 2023 Sep 17;11(18):3947.

[76] 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.

[77] Agarwal A, Bartusek J, Goyal V, Khurana D, Malavolta G. Post-quantum multi-party computation. InAdvances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I 40 2021 (pp. 435-464). Springer International Publishing.

[78] Dulek Y, Grilo AB, Jeffery S, Majenz C, Schaffner C. Secure multi-party quantum computation with a dishonest majority. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2020 May 1 (pp. 729-758). Cham: Springer International Publishing.

[79] Jiang Y, Zhou Y, Feng T. A Blockchain-Based Secure Multi-Party Computation Scheme with Multi-Key Fully Homomorphic Proxy Re-Encryption. Information. 2022 Oct 6;13(10):481.

[80] Dou Z, Xu G, Chen XB, Niu XX, Yang YX. Rational protocol of quantum secure multi-party computation. Quantum Information Processing. 2018 Aug;17:1-22.

[81] Büscher N, Demmler D, Karvelas NP, Katzenbeisser S, Krämer J, Rathee D, Schneider T, Struck P. Secure two-party computation in a quantum world. InApplied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part I 18 2020 (pp. 461-480). Springer International Publishing.

[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] Alrawili R, AlQahtani AA, Khan MK. Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering. 2024 Oct 1;119:109485.

[84] Joshi M, Mazumdar B, Dey S. A comprehensive security analysis of match-in-database fingerprint biometric system. Pattern Recognition Letters. 2020 Oct 1;138:247-66.

[85] Arman SM, Yang T, Shahed S, Al Mazroa A, Attiah A, Mohaisen L. A Comprehensive Survey for Privacy-Preserving Biometrics: Recent Approaches, Challenges, and Future Directions. CMC-COMPUTERS MATERIALS & CONTINUA. 2024 Jan 1;78(2):2087-110.

[86] Meden B, Rot P, Terhörst P, Damer N, Kuijper A, Scheirer WJ, Ross A, Peer P, Štruc V. Privacy–enhancing face biometrics: A comprehensive survey. IEEE Transactions on Information Forensics and Security. 2021 Jul 12;16:4147-83.

[87] Salem SH, Hassan AY, Moustafa MS, Hassan MN. Blockchain-based biometric identity management. Cluster Computing. 2024 Jun;27(3):3741-52.

[88] 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.

[89] 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.

[90] Grover S. Security and Efficiency of Quantum Key Distribution Protocols: A Comprehensive Review. Journal of Quantum Science and Technology. 2024 Jul 2;1(2):23-30.

[91] Lee C, Sohn I, Lee W. Eavesdropping detection in BB84 quantum key distribution protocols. IEEE Transactions on Network and Service Management. 2022 Apr 6;19(3):2689-701.

[92] Leuchs G, Marquardt C, Sánchez-Soto LL, Strekalov DV. R&D advances for quantum communication systems. InOptical Fiber Telecommunications VII 2020 Jan 1 (pp. 495-563). Academic Press.

[93] 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.

[94] 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.

[95] Al-Mohammed HA, Yaacoub E, Abualsaud K. QKD Protocol for Securing the Communication With Real-Life Application Scenarios. InQuantum Computing and Cryptography in Future Computers 2024 (pp. 208-228). IGI Global.

[96] Cvitić I, Peraković D. A Quantum Physics Approach for Enabling Information-Theoretic Secure Communication Channels. InInternational Conference on Digital Forensics and Cyber Crime 2023 Nov 30 (pp. 3-22). Cham: Springer Nature Switzerland.

[97] Sattler L, Pacella D. Quantum Key Distribution (QKD): Safeguarding for the Future. Global Communications. 2024 Jan;2024.

[98] Zhao P, Zhong W, Du MM, Li XY, Zhou L, Sheng YB. Quantum secure direct communication with hybrid entanglement. Frontiers of Physics. 2024 Oct;19(5):51201.

[99] Pan D, Song XT, Long GL. Free-space quantum secure direct communication: Basics, progress, and outlook. Advanced Devices & Instrumentation. 2023 Apr 12;4:0004.

[100] Liu S, Lv Y, Wang X, Wang J, Lou Y, Jing J. Deterministic all-optical quantum teleportation of four degrees of freedom. Physical Review Letters. 2024 Mar 8;132(10):100801.

[101] 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.

[102] Liu S, Lv Y, Wang X, Wang J, Lou Y, Jing J. Deterministic all-optical quantum teleportation of four degrees of freedom. Physical Review Letters. 2024 Mar 8;132(10):100801.

[103] Ribeiro GA, Rigolin G. Detecting quantum critical points at finite temperature via quantum teleportation: Further models. Physical Review A. 2024 Jan;109(1):012612.

[104] Porras MA, Casado-Álvaro M, Gonzalo I. Teleportation of a quantum particle in a potential via quantum Zeno dynamics. Physical Review A. 2024 Mar;109(3):032207.

[105] Hosseiny SM, Seyed-Yazdi J, Norouzi M, Livreri P. Quantum teleportation in Heisenberg chain with magnetic-field gradient under intrinsic decoherence. Scientific Reports. 2024 Apr 26;14(1):9607.

[106] Dharkar V, Kumar S. On the Experimental Performance Measurement of Quantum Teleportation. In2024 International Conference on Computing, Networking and Communications (ICNC) 2024 Feb 19 (pp. 11-15). IEEE.

[107] 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.

[108] 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.

[109] Mohsen AW, Bahaa-Eldin AM, Sobh MA. Lattice-based cryptography. In2017 12th International Conference on Computer Engineering and Systems (ICCES) 2017 Dec 19 (pp. 462-467). IEEE.

[110] Sundaram BV, Ramnath M, Prasanth M, Sundaram V. Encryption and hash based security in Internet of Things. In2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) 2015 Mar 26 (pp. 1-6). IEEE.

[111] Butin D. Hash-based signatures: State of play. IEEE security & privacy. 2017 Aug 17;15(4):37-43.

[112] Weger V, Gassner N, Rosenthal J. A survey on code-based cryptography. arXiv preprint arXiv:2201.07119. 2022 Jan 18.

[113] 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.

[114] 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.

[115] Yang YG, Xu P, Yang R, Zhou YH, Shi WM. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. Scientific reports. 2016 Jan 29;6(1):19788.

[116] Portmann C, Renner R. Security in quantum cryptography. Reviews of Modern Physics. 2022 Apr 1;94(2):025008.

[117] Glisic S. Quantum vs post-quantum security for future networks: Survey. Cyber Security and Applications. 2024 Jan 1;2:100039.

[118] Kumar A, Garhwal S. State-of-the-art survey of quantum cryptography. Archives of Computational Methods in Engineering. 2021 Aug;28:3831-68.

[119] 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.

[120] Zhang P, Wang L, Wang W, Fu K, Wang J. A blockchain system based on quantum-resistant digital signature. Security and Communication Networks. 2021;2021(1):6671648.

[121] Unogwu OJ, Doshi R, Hiran KK, Mijwil MM. Introduction to quantum-resistant blockchain. InAdvancements in quantum blockchain with real-time applications 2022 (pp. 36-55). IGI Global.

[122] Zhang P, Schmidt DC, White J, Dubey A. Consensus mechanisms and information security technologies. Advances in Computers. 2019 Jan 1;115:181-209.

[123] Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics. 2019 Mar 6;15(6):3680-9.

[124] Saha S, Hota A, Chattopadhyay AK, Nag A, Nandi S. A multifaceted survey on privacy preservation of federated learning: progress, challenges, and opportunities. Artificial Intelligence Review. 2024 Jun 21;57(7):184.

[125] 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.

[126] Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Computers in Biology and Medicine. 2024 Jan 28:108036.

[127] Rane N, Choudhary S, Rane J. Machine Learning and Deep Learning: a Comprehensive Review on Methods, Techniques, Applications, Challenges, and Future Directions. Techniques, Applications, Challenges, and Future Directions (May 31, 2024). 2024 May 31.

[128] Kumar A, Bhatia S, Kaushik K, Gandhi SM, Devi SG, Diego AD, Mashat A. Survey of promising technologies for quantum drones and networks. Ieee Access. 2021 Sep 1;9:125868-911.

[129] 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.

[130] Kaiwartya O, Prasad M, Prakash S, Samadhiya D, Abdullah AH, Abd Rahman SO. An Investigation on Biometric Internet Security. Int. J. Netw. Secur.. 2017 Mar 1;19(2):167-76.

[131] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[132] Khan HU, Ali N, Ali F, Nazir S. Transforming future technology with quantum-based IoT. The Journal of Supercomputing. 2024 Jun 23:1-35.

[133] Larasati HT, Kim H. Quantum cryptanalysis landscape of shor's algorithm for elliptic curve discrete logarithm problem. InInformation Security Applications: 22nd International Conference, WISA 2021, Jeju Island, South Korea, August 11–13, 2021, Revised Selected Papers 22 2021 (pp. 91-104). Springer International Publishing.

[134] Nitaj A. Post quantum cryptography. Malaysian Journal of Mathematical Sciences. 2017 Aug 31;11:1-28.

[135] Petrenko A. Applied Quantum Cryptanalysis. River Publishers; 2023 Apr 13.

[136] Ahmed N. Quantum Computing Algorithms for Integer Factorization: A Comparative Analysis. Modern Dynamics: Mathematical Progressions. 2024 May 25;1(1):6-9.

[137] 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.

[138] Ye G, Jiao K, Huang X, Goi BM, Yap WS. An image encryption scheme based on public key cryptosystem and quantum logistic map. Scientific Reports. 2020 Dec 3;10(1):21044.

[139] Kazmirchuk S, Ilyenko A, Ilyenko S, Prokopenko O, Mazur Y. The Improvement of digital signature algorithm based on elliptic curve cryptography. InAdvances in Computer Science for Engineering and Education III 3 2021 (pp. 327-337). Springer International Publishing.

[140] Soni L, Chandra H, Gupta DS, Keval R. Quantum-resistant public-key encryption and signature schemes with smaller key sizes. Cluster Computing. 2024 Feb;27(1):285-97.

[141] Sood N. Cryptography in Post Quantum Computing Era. Available at SSRN 4705470. 2024.

[142] Pandey AK, Banati A, Rajendran B, Sudarsan SD, Pandian KS. Cryptographic challenges and security in post quantum cryptography migration: A prospective approach. In2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA) 2023 Sep 8 (pp. 1-8). IEEE.

[143] 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.

[144] Lindsay JR. Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. Security Studies. 2020 Mar 14;29(2):335-61.

[145] Brijwani GN, Ajmire PE, Thawani PV. Future of quantum computing in cyber security. InHandbook of Research on Quantum Computing for Smart Environments 2023 (pp. 267-298). IGI Global.

[146] Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proceedings. 2021 Jan 1;37:2653-9.

[147] Abed SE, Jaffal R, Mohd BJ, Al-Shayeji M. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Cluster computing. 2021 Dec;24:3065-84.

[148] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain: research and applications. 2022 Jun 1;3(2):100067.

[149] 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.

[150] Tariq Z, e Zainab B, Hussain MZ. Evaluating the Effectiveness and Resilience of SSL/TLS, HTTPS, IPSec, SSH, and WPA/WPA2 in Safeguarding Data Transmission. UCP Journal of Engineering & Information Technology. 2023;1(2):01-7.

[151] Sharp R. Network Security. InIntroduction to Cybersecurity: A Multidisciplinary Challenge 2023 Oct 13 (pp. 171-233). Cham: Springer Nature Switzerland.

[152] Vondráček M, Pluskal J, Ryšavý O. Automated Man-in-the-Middle Attack Against Wi-Fi Networks. Journal of Digital Forensics, Security and Law. 2018;13(1):9.

[153] 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.

[154] Paul S, Kuzovkova Y, Lahr N, Niederhagen R. Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3. InProceedings of the 2022 ACM on Asia Conference on Computer and Communications Security 2022 May 30 (pp. 727-740).

[155] 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.

[156] 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.

[157] Thakor VA, Razzaque MA, Khandaker MR. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access. 2021 Jan 19;9:28177-93.

[158] Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021 Feb;27(2):1515-55.

[159] Dhanda SS, Singh B, Jindal P. Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications. 2020 Jun;112(3):1947-80.

[160] Rana M, Mamun Q, Islam R. Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems. 2022 Apr 1;129:77-89.

[161] 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.

[162] 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.

[163] Zhou I, Tofigh F, Piccardi M, Abolhasan M, Franklin D, Lipman J. Secure Multi-Party Computation for Machine Learning: A Survey. IEEE Access. 2024 Apr 15.

[164] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (Csur). 2018 Jul 25;51(4):1-35.

[165] Chase M, Derler D, Goldfeder S, Orlandi C, Ramacher S, Rechberger C, Slamanig D, Zaverucha G. Post-quantum zero-knowledge and signatures from symmetric-key primitives. InProceedings of the 2017 acm sigsac conference on computer and communications security 2017 Oct 30 (pp. 1825-1842).

[166] Sahu DR, Tiwari H, Tomar DS, Pateriya RK. Quantum-Resistant Cryptography to Prevent from Phishing Attack Exploiting Blockchain Wallet. InSustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications 2024 Apr 3 (pp. 171-191). Singapore: Springer Nature Singapore.

[167] Zhang H, Ma J, Qiu Z, Yao J, Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Multi-GPU Parallel Pipeline Rendering with Splitting Frame. InComputer Graphics International Conference 2023 Aug 28 (pp. 223-235). Cham: Springer Nature Switzerland.

[168] Arshinov NA, Butakova NG. Vulnerability research of confidential information transmitted over quantum channels in bank infrastructure. In2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) 2019 Jan 28 (pp. 1726-1730). IEEE.

[169] Udeh EO, Amajuoyi P, Adeusi KB, Scott AO. Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology. Finance & Accounting Research Journal. 2024 Jun 6;6(6):851-67.

[170] Dam DT, Tran TH, Hoang VP, Pham CK, Hoang TT. A survey of post-quantum cryptography: Start of a new race. Cryptography. 2023 Aug 14;7(3):40.

[171] 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.

[172] Stebila D, Wilson S. Quantum-safe account recovery for webauthn. InProceedings of the 19th ACM Asia Conference on Computer and Communications Security 2024 Jul 1 (pp. 1814-1830).

[173] 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.

[174] 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.

[175] 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.

[176] 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.

[177] 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.

[178] Zhao P, Linghu K, Li Z, Xu P, Wang R, Xue G, Jin Y, Yu H. Quantum crosstalk analysis for simultaneous gate operations on superconducting qubits. PRX quantum. 2022 Apr 1;3(2):020301.

[179] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[180] Wintersperger K, Dommert F, Ehmer T, Hoursanov A, Klepsch J, Mauerer W, Reuber G, Strohm T, Yin M, Luber S. Neutral atom quantum computing hardware: performance and end-user perspective. EPJ Quantum Technology. 2023 Dec 1;10(1):32.

[181] Ash-Saki A, Alam M, Ghosh S. Analysis of crosstalk in nisq devices and security implications in multi-programming regime. InProceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design 2020 Aug 10 (pp. 25-30).

[182] Smith AW, Khosla KE, Self CN, Kim MS. Qubit readout error mitigation with bit-flip averaging. Science advances. 2021 Nov 17;7(47):eabi8009.

[183] Riste D, Poletto S, Huang MZ, Bruno A, Vesterinen V, Saira OP, DiCarlo L. Detecting bit-flip errors in a logical qubit using stabilizer measurements. Nature communications. 2015 Apr 29;6(1):6983.

[184] Funcke L, Hartung T, Jansen K, Kühn S, Stornati P, Wang X. Measurement error mitigation in quantum computers through classical bit-flip correction. Physical Review A. 2022 Jun;105(6):062404.

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

[186] Ding Y, Gokhale P, Lin SF, Rines R, Propson T, Chong FT. Systematic crosstalk mitigation for superconducting qubits via frequency-aware compilation. In2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO) 2020 Oct 17 (pp. 201-214). IEEE.

[187] Niu S, Todri-Sanial A. Enabling multi-programming mechanism for quantum computing in the NISQ era. Quantum. 2023 Feb 16;7:925.

[188] 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.

[189] Niu S, Todri-Sanial A. Multi-programming mechanism on near-term quantum computing. InQuantum Computing: Circuits, Systems, Automation and Applications 2023 Aug 7 (pp. 19-54). Cham: Springer International Publishing.

[190] Saki AA, Ghosh S. Qubit sensing: A new attack model for multi-programming quantum computing. arXiv preprint arXiv:2104.05899. 2021 Apr 13.

[191] Moon P, Yenurkar G, Nyangaresi VO, Raut A, Dapkekar N, Rathod J, Dabare P. An improved custom convolutional neural network based hand sign recognition using machine learning algorithm. Engineering Reports. 2024:e12878.

[192] Saki AA, Alam M, Phalak K, Suresh A, Topaloglu RO, Ghosh S. A survey and tutorial on security and resilience of quantum computing. In2021 IEEE European Test Symposium (ETS) 2021 May 24 (pp. 1-10). IEEE.

[193] Abidin A. On detecting relay attacks on RFID systems using qubits. Cryptography. 2020 May 8;4(2):14.

[194] Schlosshauer M. Quantum decoherence. Physics Reports. 2019 Oct 25;831:1-57.

[195] Bogdanov SI, Boltasseva A, Shalaev VM. Overcoming quantum decoherence with plasmonics. Science. 2019 May 10;364(6440):532-3.

[196] Suter D, Álvarez GA. Colloquium: Protecting quantum information against environmental noise. Reviews of Modern Physics. 2016 Oct 1;88(4):041001.

[197] Daley AJ. Quantum trajectories and open many-body quantum systems. Advances in Physics. 2014 Mar 4;63(2):77-149.

[198] Battistel F, Chamberland C, Johar K, Overwater RW, Sebastiano F, Skoric L, Ueno Y, Usman M. Real-time decoding for fault-tolerant quantum computing: Progress, challenges and outlook. Nano Futures. 2023 Aug 9;7(3):032003.

[199] 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).

[200] 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.

[201] Resch S, Karpuzcu UR. Benchmarking quantum computers and the impact of quantum noise. ACM Computing Surveys (CSUR). 2021 Jul 18;54(7):1-35.

[202] Bravyi S, Dial O, Gambetta JM, Gil D, Nazario Z. The future of quantum computing with superconducting qubits. Journal of Applied Physics. 2022 Oct 28;132(16).

[203] Erhard A, Wallman JJ, Postler L, Meth M, Stricker R, Martinez EA, Schindler P, Monz T, Emerson J, Blatt R. Characterizing large-scale quantum computers via cycle benchmarking. Nature communications. 2019 Nov 25;10(1):5347.

[204] Siddiqi I. Engineering high-coherence superconducting qubits. Nature Reviews Materials. 2021 Oct;6(10):875-91.

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

[206] Jain N, Stiller B, Khan I, Elser D, Marquardt C, Leuchs G. Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics. 2016 Jul 2;57(3):366-87.

[207] Grote O, Ahrens A, Benavente-Peces C. Small Quantum-safe Design Approach for Long-term Safety in Cloud Environments. In2021 International Conference on Engineering and Emerging Technologies (ICEET) 2021 Oct 27 (pp. 1-5). IEEE.

[208] Rand L, Rand T. The" Prime Factors" of Quantum Cryptography Regulation. Notre Dame J. on Emerging Tech.. 2022;3:37.

[209] Lindsay JR. Surviving the quantum cryptocalypse. Strategic Studies Quarterly. 2020 Jul 1;14(2):49-73.

[210] Vijay Nikhil U, Stamenkovic Z, Raja SP. A Study of Elliptic Curve Cryptography and Its Applications. International Journal of Image and Graphics. 2024 Mar 12:2550062.

[211] 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.

[212] Shah SM, Khan RA. Secondary use of electronic health record: Opportunities and challenges. IEEE access. 2020 Jul 22;8:136947-65.

[213] Price WN, Cohen IG. Privacy in the age of medical big data. Nature medicine. 2019 Jan;25(1):37-43.

[214] Saki AA, Alam M, Ghosh S. Study of decoherence in quantum computers: A circuit-design perspective. arXiv preprint arXiv:1904.04323. 2019 Apr 8.

[215] Hetényi B, Wootton JR. Tailoring quantum error correction to spin qubits. Physical Review A. 2024 Mar;109(3):032433.

[216] De Leon NP, Itoh KM, Kim D, Mehta KK, Northup TE, Paik H, Palmer BS, Samarth N, Sangtawesin S, Steuerman DW. Materials challenges and opportunities for quantum computing hardware. Science. 2021 Apr 16;372(6539):eabb2823.

[217] Papadogiannaki E, Ioannidis S. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. ACM Computing Surveys (CSUR). 2021 Jul 13;54(6):1-35.

[218] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[219] Kuang R, Barbeau M. Quantum permutation pad for universal quantum-safe cryptography. Quantum Information Processing. 2022 Jun 14;21(6):211.

[220] Fang W, Ying M. Symbolic execution for quantum error correction programs. Proceedings of the ACM on Programming Languages. 2024 Jun 20;8(PLDI):1040-65.

[221] Park J, Cho S, Lim T, Tehranipoor M. QEC: A quantum entropy chip and its applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2020 Mar 12;28(6):1471-84.

[222] Zhou J, Ding W, Yang W. A secure encoding mechanism against deception attacks on multisensor remote state estimation. IEEE Transactions on Information Forensics and Security. 2022 May 16;17:1959-69.

[223] Swathi M, Rudra B. A novel approach for asymmetric quantum error correction with syndrome measurement. IEEE Access. 2022 Apr 25;10:44669-76.

[224] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[225] Srinivasan K, Moses Y, Manohar R. Opportunistic mutual exclusion. In2023 28th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC) 2023 Jul 16 (pp. 1-9). IEEE.

[226] Balla A, Habaebi MH, Elsheikh EA, Islam MR, Suliman FM. The effect of dataset imbalance on the performance of scada intrusion detection systems. Sensors. 2023 Jan 9;23(2):758.

[227] Arunakumari BN, Shreyas R, Vora SN, Shreyas R, Venkatesh SG. Unbreakable Passwords: Fortifying Cryptographic Security with Derangement Keys. InInternational Conference on Data Management, Analytics & Innovation 2024 Jan 19 (pp. 475-485). Singapore: Springer Nature Singapore.

[228] Korobko M, Südbeck J, Steinlechner S, Schnabel R. Mitigating quantum decoherence in force sensors by internal squeezing. Physical Review Letters. 2023 Oct 6;131(14):143603.

[229] Guo X, Yu Z, Wei F, Jin S, Chen X, Li X, Zhang X, Zhou X. Quantum precision measurement of two-dimensional forces with 10-28-newton stability. Science Bulletin. 2022 Nov 30;67(22):2291-7.

[230] Gabrian CA. Impact Zones: How cybercrime disrupts and shapes the landscape of data security. InInternational Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings 2024 Jul 16 (Vol. 1, pp. 59-68).

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

[232] Cimorelli Belfiore R, De Santis A, Ferrara AL, Masucci B. Hierarchical Key Assignment Schemes with Key Rotation. InProceedings of the 29th ACM Symposium on Access Control Models and Technologies 2024 Jun 24 (pp. 171-182).

[233] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of things Journal. 2018 Jun 15;6(2):1606-16.

[234] Alexeev Y, Bacon D, Brown KR, Calderbank R, Carr LD, Chong FT, DeMarco B, Englund D, Farhi E, Fefferman B, Gorshkov AV. Quantum computer systems for scientific discovery. PRX quantum. 2021 Feb 1;2(1):017001.

[235] Marchesi L, Marchesi M, Tonelli R. Reviewing Crypto-Agility and Quantum Resistance in the Light of Agile Practices. InInternational Conference on Agile Software Development 2022 Jun 13 (pp. 213-221). Cham: Springer Nature Switzerland.

[236] Ikeda K. Security and privacy of blockchain and quantum computation. InAdvances in Computers 2018 Jan 1 (Vol. 111, pp. 199-228). Elsevier.

[237] Mihaljević MJ, Oggier F. Security evaluation and design elements for a class of randomised encryptions. IET Information Security. 2019 Jan;13(1):36-47.

[238] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[239] Stipčević M, Batelić M, Charbon E, Bruschini C, Antolović IM. Random flip-flop: adding quantum randomness to digital circuits for improved cyber security, artificial intelligence and more. InEmerging Imaging and Sensing Technologies for Security and Defence VI 2021 Sep 12 (Vol. 11868, pp. 64-74). SPIE.

[240] Kuang R, Perepechaenko M, Barbeau M. A new quantum-safe multivariate polynomial public key digital signature algorithm. Scientific Reports. 2022 Aug 1;12(1):13168.

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

[242] Kichna A, Farchane A. Secure and efficient code-based cryptography for multi-party computation and digital signatures. InComputer Sciences & Mathematics Forum 2023 May 26 (Vol. 6, No. 1, p. 1). MDPI.

[243] Liu Z, Choo KK, Grossschadl J. Securing edge devices in the post-quantum internet of things using lattice-based cryptography. IEEE Communications Magazine. 2018 Feb 13;56(2):158-62.

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

[245] 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.

[246] Kuang R, Lou D, He A, Conlon A. Quantum safe lightweight cryptography with quantum permutation pad. In2021 IEEE 6th international conference on computer and communication systems (ICCCS) 2021 Apr 23 (pp. 790-795). IEEE.

[247] Pothos EM, Busemeyer JR, Shiffrin RM, Yearsley JM. The rational status of quantum cognition. Journal of Experimental Psychology: General. 2017 Jul;146(7):968.

[248] Tannu SS, Qureshi M. Ensemble of diverse mappings: Improving reliability of quantum computers by orchestrating dissimilar mistakes. InProceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture 2019 Oct 12 (pp. 253-265).

[249] Ortigoso J. Twelve years before the quantum no-cloning theorem. American Journal of Physics. 2018 Mar 1;86(3):201-5.

[250] Morimae T. Quantum randomized encoding, verification of quantum computing, no-cloning, and blind quantum computing. arXiv preprint arXiv:2011.03141. 2020 Nov 5.

[251] Altman E, Brown KR, Carleo G, Carr LD, Demler E, Chin C, DeMarco B, Economou SE, Eriksson MA, Fu KM, Greiner M. Quantum simulators: Architectures and opportunities. PRX quantum. 2021 Feb 1;2(1):017003.

[252] 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.

[253] Kim J, Min D, Cho J, Jeong H, Byun I, Choi J, Hong J, Kim J. A Fault-Tolerant Million Qubit-Scale Distributed Quantum Computer. InProceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2 2024 Apr 27 (pp. 1-19).

[254] Awan U, Hannola L, Tandon A, Goyal RK, Dhir A. Quantum computing challenges in the software industry. A fuzzy AHP-based approach. Information and Software Technology. 2022 Jul 1;147:106896.

[255] Liao SK, Cai WQ, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren JG, Liu WY, Li Y. Satellite-relayed intercontinental quantum network. Physical review letters. 2018 Jan 19;120(3):030501.

[256] Lai J, Yao F, Wang J, Zhang M, Li F, Zhao W, Zhang H. Application and Development of QKD-Based Quantum Secure Communication. Entropy. 2023 Apr 6;25(4):627.

[257] Pelucchi E, Fagas G, Aharonovich I, Englund D, Figueroa E, Gong Q, Hannes H, Liu J, Lu CY, Matsuda N, Pan JW. The potential and global outlook of integrated photonics for quantum technologies. Nature Reviews Physics. 2022 Mar;4(3):194-208.

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

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

[260] Mavroeidis V, Vishi K, Zych MD, Jøsang A. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200. 2018 Mar 31.

[261] Dejpasand MT, Sasani Ghamsari M. Research trends in quantum computers by focusing on qubits as their building blocks. Quantum Reports. 2023 Sep 13;5(3):597-608.

[262] Saki AA, Alam M, Ghosh S. Impact of noise on the resilience and the security of quantum computing. In2021 22nd International Symposium on Quality Electronic Design (ISQED) 2021 Apr 7 (pp. 186-191). IEEE.

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

[264] Xavier GB, Lima G. Quantum information processing with space-division multiplexing optical fibres. Communications Physics. 2020 Jan 13;3(1):9.

[265] Molotkov SN. On the robustness of information-theoretic authentication in quantum cryptography. Laser Physics Letters. 2022 May 19;19(7):075203.

[266] Akrom M, Rustad S, Dipojono HK. Variational quantum circuit-based quantum machine learning approach for predicting corrosion inhibition efficiency of pyridine-quinoline compounds. Materials Today Quantum. 2024 Jun 1;2:100007.

[267] 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.

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

[269] Swetha D, Mohiddin SK. Quantum-Enhanced Security Advances for Cloud Computing Environments. International Journal of Advanced Computer Science & Applications. 2024 Jun 1;15(6).

[270] Dangi R, Choudhary G, Dragoni N, Lalwani P, Khare U, Kundu S. 6G Mobile Networks: Key Technologies, Directions, and Advances. InTelecom 2023 Dec 1 (Vol. 4, No. 4, pp. 836-876). MDPI.

[271] van Deventer O, Spethmann N, Loeffler M, Amoretti M, van den Brink R, Bruno N, Comi P, Farrugia N, Gramegna M, Jenet A, Kassenberg B. Towards European standards for quantum technologies. EPJ Quantum Technology. 2022 Dec 1;9(1):33.

[272] Phalak K, Ash-Saki A, Alam M, Topaloglu RO, Ghosh S. Quantum puf for security and trust in quantum computing. IEEE Journal on Emerging and Selected Topics in Circuits and Systems. 2021 May 3;11(2):333-42.

[273] Javaid MA, Ashraf M, Rehman T, Tariq N. Impact of Post Quantum Digital Signatures On Block Chain: Comparative Analysis. The Asian Bulletin of Big Data Management. 2024 Mar 31;4(1):Science-4.

[274] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[275] Asif R. Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT. 2021 Mar;2(1):71-91.

[276] Illiano J, Caleffi M, Manzalini A, Cacciapuoti AS. Quantum internet protocol stack: A comprehensive survey. Computer Networks. 2022 Aug 4;213:109092.

[277] Wang H, Yu J. A blockchain consensus protocol based on quantum attack algorithm. Computational Intelligence and Neuroscience. 2022;2022(1):1431967.

[278] Jain S. QSB: Smart Contracts, Consensus, and Quantum Cryptography. InQuantum and Blockchain-based Next Generation Sustainable Computing 2024 Jul 28 (pp. 1-18). Cham: Springer Nature Switzerland.

[279] Kalinin M, Krundyshev V. Security intrusion detection using quantum machine learning techniques. Journal of Computer Virology and Hacking Techniques. 2023 Mar;19(1):125-36.

[280] 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.

[281] 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.

[282] Alomari A, Kumar SA. Securing IoT Systems in a Post-Quantum Environment: Vulnerabilities, Attacks, and Possible Solutions. Internet of Things. 2024 Feb 20:101132.

[283] 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.

[284] Zeuner J, Pitsios I, Tan SH, Sharma AN, Fitzsimons JF, Osellame R, Walther P. Experimental quantum homomorphic encryption. npj Quantum Information. 2021 Feb 5;7(1):25.

[285] Gong C, Du J, Dong Z, Guo Z, Gani A, Zhao L, Qi H. Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing. Quantum Information Processing. 2020 Mar;19:1-7.

[286] Sriman B, Ganesh Kumar S. An efficient quantum non-interactive zero knowledge proof for confidential transaction and quantum range proof. Multimedia Tools and Applications. 2024 Apr;83(13):39411-34.

[287] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[288] Srinivas MB, Konguvel E. Era of Sentinel Tech: Charting Hardware Security Landscapes through Post-Silicon Innovation, Threat Mitigation and Future Trajectories. IEEE Access. 2024 May 13.

[289] Das S, Chatterjee A, Ghosh S. SoK: A First Order Survey of Quantum Supply Dynamics and Threat Landscapes. InProceedings of the 12th International Workshop on Hardware and Architectural Support for Security and Privacy 2023 Oct 29 (pp. 82-90).

[290] Dhar S, Khare A, Dwivedi AD, Singh R. Securing IoT devices: A novel approach using blockchain and quantum cryptography. Internet of Things. 2024 Apr 1;25:101019.

[291] Sutradhar K, Venkatesh R, Venkatesh P. Quantum Blockchain-Based Healthcare: Merging Frontiers for Secure and Efficient Data Management. InHealthcare Services in the Metaverse 2024 (pp. 190-207). CRC Press.

[292] Chorti A, Barreto AN, Köpsell S, Zoli M, Chafii M, Sehier P, Fettweis G, Poor HV. Context-aware security for 6G wireless: The role of physical layer security. IEEE Communications Standards Magazine. 2022 Mar;6(1):102-8.

[293] Karacan E, Akleylek S, Karakaya A. Pq-flat: a new quantum-resistant and lightweight authentication approach for m2m devices. In2021 9th International Symposium on Digital Forensics and Security (ISDFS) 2021 Jun 28 (pp. 1-5). IEEE.

[294] Jain A, Gupta H. A Cryptographic Model for the Enhancement of Data Security. In2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2024 Mar 14 (pp. 1-6). IEEE.

[295] 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.