Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.062966

REVIEW

Edge-Fog Enhanced Post-Quantum Network Security: Applications, Challenges and Solutions

Seo Yeon Moon[1], **Byung Hyun Jo**[1], **Abir El Azzaoui**[1], **Sushil Kumar Singh**[2] **and Jong Hyuk Park**[1,*]

[1]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 01811, Republic of Korea

[2]Department of Computer Science and Engineering, Marwadi University, Rajkot, 360005, India

*Corresponding Author: Jong Hyuk Park. Email: jhpark1@seoultech.ac.kr

Received: 31 December 2024; Accepted: 18 April 2025; Published: 09 June 2025

ABSTRACT: With the rapid advancement of ICT and IoT technologies, the integration of Edge and Fog Computing has become essential to meet the increasing demands for real-time data processing and network efficiency. However, these technologies face critical security challenges, exacerbated by the emergence of quantum computing, which threatens traditional encryption methods. The rise in cyber-attacks targeting IoT and Edge/Fog networks underscores the need for robust, quantum-resistant security solutions. To address these challenges, researchers are focusing on Quantum Key Distribution and Post-Quantum Cryptography, which utilize quantum-resistant algorithms and the principles of quantum mechanics to ensure data confidentiality and integrity. This paper reviews the current security practices in IoT and Edge/Fog environments, explores the latest advancements in QKD and PQC technologies, and discusses their integration into distributed computing systems. Additionally, this paper proposes an enhanced QKD protocol combining the Cascade protocol and Kyber algorithm to address existing limitations. Finally, we highlight future research directions aimed at improving the scalability, efficiency, and practicality of QKD and PQC for securing IoT and Edge/Fog networks against evolving quantum threats.

KEYWORDS: Edge computing; fog computing; quantum key distribution; security; post-quantum cryptography; cascade protocol

1 Introduction

The Internet of Things (IoT) is a system in which various physical devices, sensors, and software are interconnected through networks to collect and exchange data, establishing itself as a key technology in various applications of modern society. IoT is utilized across diverse domains, including smart homes, smart edge devices, smart cities, healthcare systems, and industrial automation. With the proliferation of smart devices and cloud computing, the scale and complexity of data generated by IoT devices continue to grow [1,2]. However, while cloud computing provides on-demand storage and processing services for such big data, there exists a trade-off between storage and latency. Uploading data to a central server for processing and returning the results to sensors and devices imposes significant burdens on the network, particularly in terms of bandwidth and resource costs for data transmission. Moreover, as the volume of data increases, network performance deteriorates [3]. To address these challenges, Edge Computing and Fog Computing have emerged as new paradigms for data processing. Edge Computing moves IoT data processing to the edge of the network, reducing the load on central data centers, lowering latency, and meeting the demands of real-time applications. Through its distributed architecture, it balances network traffic, minimizes transmission

delays, and enhances system efficiency by offloading computational tasks from nodes with limited battery resources to more powerful nodes [4].

Fog Computing serves as an intermediate layer between cloud computing and Edge Computing, offering a distributed computing environment within the continuum between IoT devices and the cloud. Strategic deployment of fog nodes closer to the network edge enables the transition of cloud computing services to localized platforms, thereby establishing a robust Fog Computing infrastructure [5]. It performs computing, storage, networking, and data management functions between edge nodes and the cloud, thereby minimizing latency and conserving bandwidth [6]. These Edge and Fog Computing technologies enable real-time data analysis and secure transmission in IoT environments. However, they also introduce new security challenges. Fog Computing, due to its large-scale geographic distribution, heterogeneity, and mobility, as well as its distributed architecture and multi-layered structure, faces significant security and privacy risks, including threats such as data tampering, man-in-the-middle attacks, and the insertion of malicious nodes [7–9].

Unlike traditional computing systems, IoT devices operate in diverse and resource-constrained environments, making them vulnerable to weak authentication, insecure communication, physical vulnerabilities, data privacy risks, DoS attacks, malware propagation, interoperability issues, and the potential threats posed by advancements in quantum computing technology [10]. The utilization of conventional security methods such as RSA, ECC, and Diffie-Hellman continues to grow, as these are widely integrated into internet protocols like Transport Layer Security (TLS) used by both general-purpose PCs and IoT devices. However, quantum computers, with their ability to perform large-scale parallel processing, possess the capability to break widely used public-key cryptographic algorithms, such as RSA and ECC, in a significantly short amount of time. This renders IoT systems susceptible to severe security threats, including data tampering, unauthorized access, data interception, and the compromise of cryptographic protocols.

Particularly, quantum computing has the potential to exploit the vulnerabilities of existing cryptographic techniques and undermine the security framework of IoT networks. Furthermore, quantum computing is often considered an extension of cloud computing, which implies that threats such as data breaches and encryption vulnerabilities in cloud environments could similarly impact IoT, Edge and Fog Computing systems. In this context, the integration of quantum computing into IoT environments raises new privacy and security concerns, necessitating systematic security measures to ensure data integrity and system protection [11–13].

Consequently, quantum-based security technologies such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) have gained significant attention [14–16]. QKD leverages the principles of quantum mechanics to detect eavesdropping and ensure secure key exchange, while PQC provides encryption algorithms resistant to quantum computing attacks. In IoT environments, QKD can be employed to securely distribute cryptographic keys among distributed network nodes and can play a critical role in Edge and Fog Computing architectures. For instance, QKD can protect data transmission between fog nodes and edge devices or be utilized for mutual authentication between IoT devices. Additionally, Post-Quantum Cryptography, due to its low computational complexity, can be efficiently implemented in resource-constrained IoT devices, effectively mitigating threats posed by quantum computers [17,18].

The rapid advancement of the Internet of Things, Edge, and Fog Computing has revolutionized data processing and connectivity, enabling real-time analytics and automation across various industries. However, this increasing interconnectivity also brings significant security challenges, particularly concerning data confidentiality, authentication, and resilience against cyber threats. Conventional cryptographic methods, including RSA, ECC, and Diffie-Hellman key exchange, have been widely used to secure IoT networks. However, with the emergence of quantum computing, these encryption algorithms are at risk of being efficiently broken by quantum algorithms such as Shor's algorithm for integer factorization and Grover's

algorithm for search acceleration. This imminent threat necessitates the development of quantum-resistant security mechanisms that can safeguard IoT and Edge/Fog networks in the post-quantum era.

Among the most promising solutions to mitigate quantum-based security threats are Quantum Key Distribution and Post-Quantum Cryptography. QKD provides an information-theoretically secure mechanism for key exchange by leveraging quantum mechanics principles, ensuring that any eavesdropping attempts are detected. Meanwhile, PQC introduces quantum-resistant encryption algorithms based on mathematical hardness assumptions, such as lattice-based, hash-based, multivariate polynomial-based, and code-based cryptography, which remain secure against both classical and quantum adversaries. Given the unique computational constraints of resource-limited IoT devices and distributed Edge/Fog Computing environments, it is critical to explore how QKD and PQC can be effectively integrated to provide scalable, efficient, and future-proof security architectures [19].

This work is particularly important because it bridges the gap between traditional IoT security frameworks and emerging quantum-resistant techniques, focusing on their real-world applicability in Edge and Fog Computing environments. Existing literature has primarily explored either QKD or PQC separately, but little research has focused on their combined potential to enhance scalability, efficiency, and resilience in large-scale distributed computing infrastructures. This paper not only reviews existing security solutions but also proposes an enhancement to QKD using parallelized Cascade error correction and lattice-based privacy amplification (Kyber), optimizing security while addressing computational efficiency challenges.

The primary contributions of this work are stated as follows:

- Comprehensive review of QKD and PQC methodologies, emphasizing their role in securing IoT, Edge, and Fog networks against quantum threats.
- Evaluation of existing classical cryptographic frameworks, identifying their limitations in post-quantum scenarios.
- Proposed enhancement to QKD that integrates parallel processing for efficient error correction and Kyber lattice-based encryption for secure privacy amplification, reducing computational overhead while ensuring quantum resilience.
- Discussion on future research directions, including the challenges and opportunities in deploying scalable and industry-ready hybrid security frameworks.

Given the urgent need for quantum-secure communication, particularly in critical infrastructure, healthcare, finance, and industrial IoT environments, this research contributes towards establishing a secure foundation for next-generation IoT and Edge/Fog computing networks that can withstand quantum-enabled cyber threats.

The remainder of this paper is as follows. Section 2 reviews related research, focusing on core technologies, existing IoT network security protocols, and quantum-based solutions. Section 3 presents the proposed quantum key distribution enhancement, which integrates parallel processing for accelerated error correction and lattice-based encryption for improved security. Unlike conventional Cascade protocols, this proposed approach directly addresses processing efficiency and security limitations, providing a viable solution for scalable quantum-secured communication. Section 4 analyzes existing trends in quantum key distribution and post-quantum cryptography, highlighting their roles, limitations, and future research directions in IoT and Edge/Fog environments. Section 5 concludes the research.

2 Related Work

This section depicts the key technologies studied in this paper along with recent related research with their limitations. It focuses on Quantum Key Distribution and Post-Quantum Cryptography, exploring their

theoretical foundations, practical implementations, and role as foundational technologies for addressing threats posed by quantum computing. Furthermore, it examines recent research trends in these areas, providing a comprehensive basis for understanding the integration and potential impact of these key technologies in enhancing security within IoT, Edge, and Fog Computing environments.

2.1 Core Technologies

This section describes the core technologies that form the foundation of quantum-resistant security in IoT and Edge/Fog computing environments. Specifically, it covers Quantum Key Distribution and Post-Quantum Cryptography, highlighting their significance in protecting modern distributed computing systems from quantum-enabled cyber threats. These technologies address the vulnerabilities of classical encryption mechanisms, ensuring secure communication and authentication in IoT networks, Edge/Fog infrastructures, and cloud computing environments.

2.1.1 Quantum Key Distribution Protocol

Quantum Key Distribution is a security mechanism that leverages quantum mechanics principles to enable secure key exchange. Unlike traditional cryptographic key exchange protocols such as RSA and Diffie-Hellman, QKD ensures that any eavesdropping attempt is inherently detectable due to the no-cloning theorem and quantum measurement disturbance property. The BB84 protocol, developed by Bennett and Brassard, remains one of the most widely used QKD protocols, relying on photon polarization states for secure key generation. Unlike traditional cryptography, which is based on mathematical complexity, QKD utilizes quantum mechanical properties such as the non-replicability, indeterminacy, and irreversibility of quanta, making it essentially impossible to eavesdrop or intercept, providing theoretical unconditional security [20]. A representative quantum key distribution protocol, the BB84 protocol, published by Charles Bennett and Gilles Bradford in 1984, utilizes the polarization of photons [21]. The sender and receiver use a rectilinear basis (+) and a diagonal basis (x) and define the two polarizations ↕ and ↔ as bit 0 and 1, respectively, for the + basis, and define ⤢ and ⤡ as bit 0 and 1 for the x basis. Alice generates random bits through quantum random number generation and randomly selects the basis to convert the bits into polarization signals. Alice then sends the polarization corresponding to the filter to Bob through the quantum channel as shown in Fig. 1.

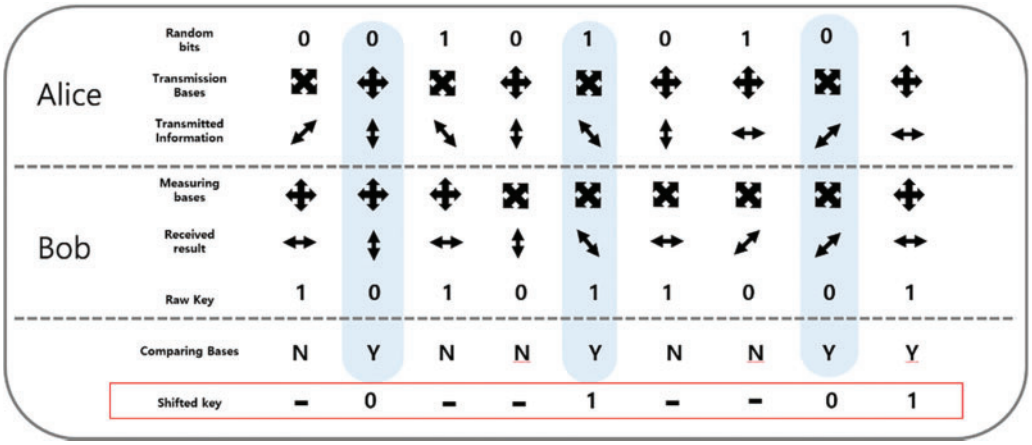

Figure 1: BB84 protocol process

To enhance the clarity of the BB84 protocol, key components such as photon states, measurement bases, and error detection steps have been explicitly labeled in Fig. 1. The photon polarization states are categorized into two bases: the rectilinear basis (+), where vertical (↕) represents bit 0 and horizontal (↔) represents bit 1, and the diagonal basis (×), where diagonal (↗) represents bit 0 and anti-diagonal (↖↘) represents bit 1. During the transmission phase, Alice encodes random bits into these quantum states and sends them to Bob, who randomly selects a basis to measure each photon. Since Bob's measurement basis may not always match Alice's, incorrect measurements introduce quantum bit errors, which are later estimated using the Quantum Bit Error Rate (QBER) analysis. The protocol then proceeds with the key sifting process, where Alice and Bob publicly compare their measurement bases and discard non-matching cases, retaining only the sifted key. To further ensure security, the error correction phase mitigates transmission errors using techniques such as the Cascade protocol, while the privacy amplification phase reduces any partial knowledge an eavesdropper may have gained. In the proposed enhancement, traditional hash-based privacy amplification is replaced with Kyber lattice-based cryptography to strengthen security against quantum adversaries. These improvements ensure a robust and practical quantum key distribution mechanism that remains resilient against both classical and quantum attacks.

Bob has a raw key of the transmitted polarization, each measured using a randomized basis. If Alice and Bob use the same basis, they have a 100% chance of having the same polarization, and if they use different basis, there is a 50% chance of a measurement error. The receiver records both the measurement and the randomized basis used during the measurement process, and after the measurement is complete, the receiver compares the recorded basis through the classical channel to filter out the value when the same basis is used to create the key, resulting in a sifted key with the same value.

Then, in order to check the measurement error caused by the noise generated by the quantum channel and the error of the control signal controlling the optical component, some of the sifted keys are released and compared to measure the Quantum Bit Error Rate and decide whether to use the shifted key. If an acceptable QBER value is obtained, post-processing of information correction, secrecy amplification, and authentication is performed to obtain the final secret key between Alice and Bob. QKD is impossible to excerpt due to the physical nature of quanta, and it is impossible to duplicate an arbitrary quanta due to the non-clonability of quanta. Assuming the eavesdropper measures the quanta in the same way as the sender and receiver and sends them back to Bob, there is a 1/2 chance of choosing the wrong basis, and a 1/2 chance that Bob's basis is different from the one chosen, for a total error of 25%.

2.1.2 Post Quantum Cryptography

Unlike QKD, which requires dedicated quantum communication channels, Post-Quantum Cryptography provides quantum-resistant encryption algorithms that can be implemented using classical infrastructure. PQC algorithms are designed to withstand attacks from Shor's algorithm (which breaks RSA and ECC) and Grover's algorithm (which weakens symmetric encryption). The National Institute of Standards and Technology (NIST) has identified several promising PQC algorithms, including lattice-based, code-based, multivariate, and hash-based cryptographic schemes [22]. Quantum-based attacks, such as Shor's and Grover's algorithms, quantum Fourier transform, quantum walk algorithms for solving search problems, and adiabatic quantum algorithms for solving optimization problems, pose significant threats to the security of current IoT infrastructure. These attacks can efficiently factorize large integers and solve discrete logarithm problems, which are the foundation of many classical cryptographic schemes [23].

Fig. 2 presents an overview of the key categories in Post-Quantum Cryptography, each relying on distinct mathematical principles to resist quantum attacks. Lattice-based cryptography, one of the most promising approaches, derives its security from problems like Learning with Errors and Shortest Vector

Problem (SVP), making it both efficient and scalable, particularly for IoT applications. Notably, Kyber (for key exchange) and Dilithium (for digital signatures) have been selected by NIST as part of the new PQC standards. Code-based cryptography, built on error-correcting codes like McEliece, offers high security but comes with the drawback of large key sizes, posing challenges for resource-constrained devices. Multivariate polynomial cryptography, which relies on complex quadratic equations, includes schemes like Rainbow for digital signatures. While fast in computation, it faces potential structural vulnerabilities. Hash-based cryptography, exemplified by SPHINCS+, is another viable PQC approach that leverages collision-resistant hash functions for signatures, but at the cost of larger signature sizes. Lastly, Supersingular Isogeny Key Encapsulation (SIKE), which was once considered promising due to its reliance on isogeny graphs of elliptic curves, has lost traction following recent cryptanalysis breakthroughs that exposed weaknesses. Overall, while lattice-based and hash-based cryptographic methods appear to be the most practical for real-world applications, research into other categories continues to refine and improve quantum-resistant security frameworks.

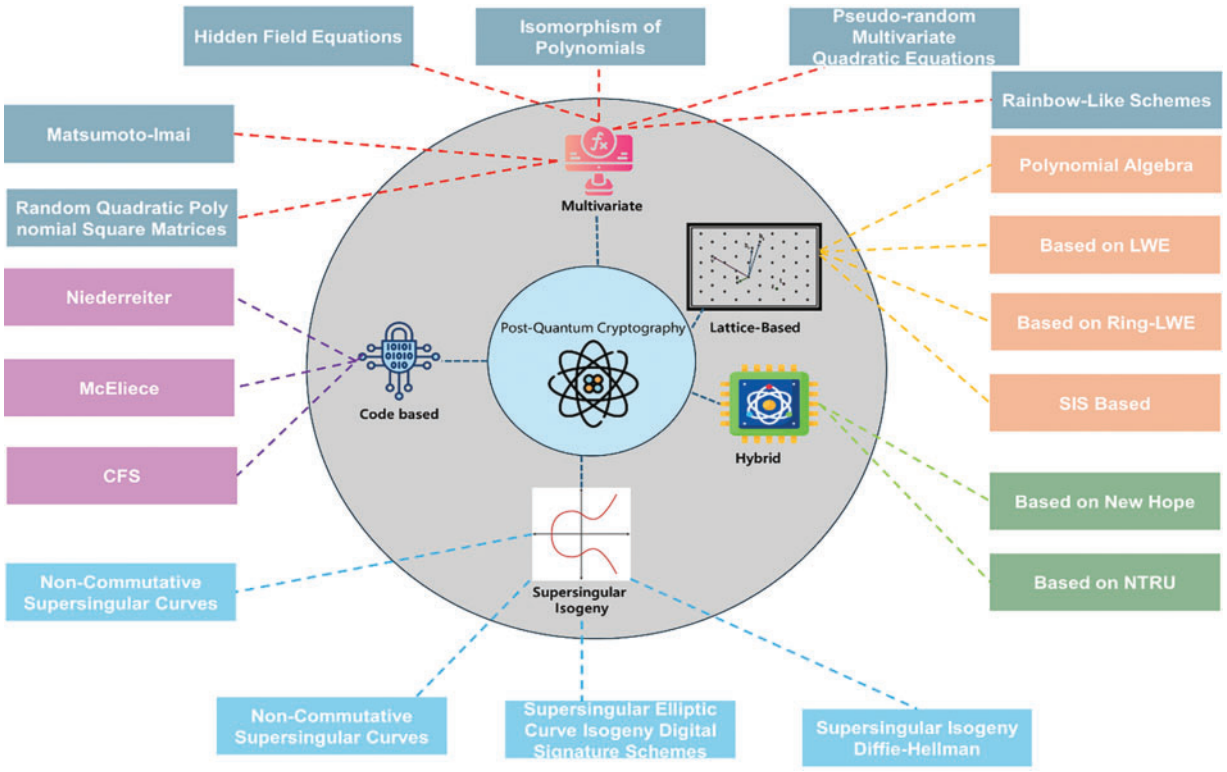

Figure 2: Type of post-quantum cryptography

PQC is specifically engineered to maintain security in quantum computing environments and is based on a variety of mathematical foundations [24]. Based on the taxonomy provided in Fig. 2, major approaches include lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, hash-based signatures, and super singular elliptic curve isogeny cryptography [25,26].

The integration of IoT and PQC has rapidly gained traction due to the increasing demand for security in IoT devices and the advancements in quantum computing. In IoT environments, PQC is being actively researched to meet the unique requirements of real-time data transmission, distributed networks, and resource-constrained devices. Lightweight PQC algorithms, such as lattice-based cryptography, emerge as

suitable solutions for IoT devices with limited computational and energy resources. Furthermore, security protocols utilizing PQC are being developed to ensure data integrity and authentication within IoT networks. International initiatives like the NIST standardization process play a critical role in identifying and evaluating quantum-resistant cryptographic algorithms suitable for IoT security, providing a framework for diverse application scenarios. These research efforts contribute significantly to defending IoT environments against quantum threats and establishing secure communication infrastructures for the quantum computing era.

The previous section provided an overview of the fundamental security technologies, namely Quantum Key Distribution and Post-Quantum Cryptography, which serve as foundational solutions to counteract emerging quantum threats. However, securing IoT and Edge/Fog environments requires not only these core technologies but also the implementation of effective communication protocols that can support secure and efficient data exchange. The next section examines existing network security protocols used in IoT environments and evaluates their vulnerabilities against quantum-based attacks.

2.2 Existing Protocols

The rapid proliferation of Internet of Things devices has necessitated the development of efficient communication protocols tailored to diverse application requirements and resource constraints. In particular, the integration of Edge and Fog Computing paradigms has emerged as a pivotal solution to address the limitations of traditional cloud-centric models, enhancing data processing capabilities and reducing latency by bringing computational resources closer to the data sources. This shift has led to the adoption of various protocols optimized for low power consumption, minimal latency, and reliable data transmission within IoT ecosystems. Protocols such as MQTT, CoAP, and AMQP have been extensively utilized to facilitate seamless communication between IoT devices and Edge/Fog nodes, each offering unique features to accommodate specific use cases and performance requirements [27,28]. The selection and implementation of these protocols are critical in ensuring the efficiency and scalability of IoT deployments, particularly in environments where real-time data processing and immediate responsiveness are essential.

Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol designed to facilitate communication between resource-constrained IoT devices and centralized servers, such as cloud systems. Operating on a publisher-subscriber model (Pub/Sub), MQTT efficiently transmits messages through a broker that intermediates between publishers and subscribers. With low bandwidth requirements and energy-efficient operations, MQTT is well-suited for environments such as smart homes and industrial automation. In Edge and Fog Computing, it enables real-time data exchange between IoT devices and nearby nodes, reducing latency by processing messages closer to the data source and offloading computation from the cloud [29,30].

Constrained Application Protocol (CoAP) is a web transfer protocol optimized for constrained devices and low-power IoT networks. It operates over UDP, ensuring reduced latency and overhead compared to HTTP. Security is enhanced by integrating Datagram Transport Layer Security (DTLS), allowing encrypted communication in resource-constrained environments. CoAP is particularly effective in applications such as environmental monitoring and smart sensors. In Edge and Fog Computing, CoAP facilitates efficient communication between IoT devices and local edge nodes, supporting lightweight data aggregation and decision-making processes at the edge level [31–33].

HTTP is the foundational protocol for transferring hypertext documents and is widely used for IoT device-to-server communication. HTTPS, an encrypted version of HTTP using TLS/SSL, ensures the confidentiality and integrity of transmitted data. While HTTP is often considered resource-intensive for constrained IoT devices, its compatibility with existing web infrastructure makes it suitable for managing

IoT data through edge nodes or fog servers. In Edge and Fog Computing, HTTP/HTTPS is used for API communication, system integration, and secure data transfer between distributed components [34,35].

Advanced Message Queuing Protocol (AMQP) is a message-oriented protocol designed for reliable and secure message delivery. It supports message queuing, delivery acknowledgment, and sequence preservation, making it ideal for IoT platforms requiring robust data exchange. In Edge and Fog Computing, AMQP facilitates seamless data flow between IoT devices and distributed nodes, ensuring the reliability of mission-critical applications such as financial services or industrial automation [36–38].

Zigbee is a low-power wireless protocol used for creating short-range mesh networks between IoT devices. It supports device-to-device communication and forms the basis for smart home applications such as lighting and appliance control. In Edge Computing, Zigbee hubs often act as gateways, collecting data from Zigbee-enabled IoT devices and forwarding it to edge nodes or fog servers for further analysis and processing [39].

Bluetooth Low Energy (BLE) is a wireless communication protocol designed for short-range and low-power data exchange. It is widely used in wearable devices and healthcare applications where energy efficiency is critical. In Edge Computing, BLE-enabled devices transmit data to edge nodes for real-time analytics or storage, supporting applications like fitness tracking and remote health monitoring [40–42].

LoRaWAN (Long Range Wide Area Network) is a long-range communication protocol designed for low-power IoT devices. It is particularly effective in applications such as smart agriculture and environmental monitoring, where devices are deployed over large geographic areas. In Fog Computing, LoRaWAN gateways aggregate data from multiple IoT devices and process it locally or relay it to cloud servers via fog nodes, reducing latency and bandwidth usage [43,44].

Open Platform Communications Unified Architecture (OPC UA) is a standard communication protocol used in industrial automation for secure and reliable data exchange. It supports cross-platform compatibility and enhanced security features, making it suitable for smart factories and Industry 4.0 applications. In Fog Computing, OPC UA facilitates integration between industrial IoT devices and fog nodes, enabling distributed data processing and system interoperability [45,46].

Data Distribution Service (DDS) is a real-time communication protocol based on a publisher-subscriber model. It supports low-latency and high-throughput communication, making it ideal for time-sensitive applications like autonomous vehicles and smart cities. In Edge and Fog Computing, DDS enables efficient data sharing between IoT devices and edge nodes, ensuring timely decision-making in distributed systems [47–49].

Datagram Transport Layer Security is a security protocol used to encrypt and authenticate UDP-based communication. It is often paired with lightweight protocols like CoAP to ensure secure data exchange in resource-constrained environments. In Edge and Fog Computing, DTLS provides end-to-end security for data transmitted between IoT devices, edge nodes, and fog servers, safeguarding against unauthorized access and data breaches [50,51], as shown in Table 1.

Table 1: Summary of protocol of IoT environment

Protocol	Methods	Quantum attack vulnerability/Limitation
MQTT, CoAP, HTTPS	RSA, ECC	Asymmetric key encryption broken by Shor's algorithm
AMQP, DDS	RSA, ECC	Asymmetric key encryption broken by Shor's algorithm

(Continued)

Table 1 (continued)

Protocol	Methods	Quantum attack vulnerability/Limitation
Zigbee, BLE	AES	Reduced to the square root of the key length by Grover's algorithm
LoRaWAN	AES	Quantum attack defense is possible only when key length is increased
DTLS	RSA, ECC, AES	Vulnerable to Shor algorithm during key exchange, AES needs key length extension

While existing protocols such as MQTT, CoAP, and HTTPS provide essential communication frameworks for IoT, they were designed for classical cryptographic environments and remain vulnerable to quantum attacks. Addressing these vulnerabilities requires integrating quantum-resistant security mechanisms, such as QKD and PQC, into these network architectures. The following section explores quantum-based security solutions that enhance the resilience of IoT networks, focusing on recent advancements and practical implementations.

2.3 Existing Quantum-Based Solutions for IoT Network Security

Quantum technology has emerged as a promising solution to tackle the increasing security challenges in IoT environments. The rapid proliferation of IoT devices and the growing complexity of network structures have exposed the limitations of traditional cryptographic methods in ensuring robust security. Quantum Key Distribution and Post-Quantum Cryptography are two critical approaches gaining significant attention in quantum-based security. QKD utilizes the principles of quantum mechanics to provide unconditional security in key exchange, effectively protecting IoT communications from eavesdropping and data breaches. Meanwhile, PQC introduces quantum-resistant cryptographic algorithms designed to counter the computational power of quantum computers, offering scalable security solutions for resource-constrained IoT systems. This section examines the application potential of QKD and PQC in IoT security, highlighting their capabilities to overcome the vulnerabilities of existing frameworks and meet the demands of next-generation IoT networks.

2.3.1 Post-Quantum Cryptography for IoT Security

IoT devices often operate in resource-constrained environments, making them vulnerable not only to existing cyber threats but also to increasingly sophisticated quantum-based attacks. These vulnerabilities pose serious risks to the integrity, confidentiality, and availability of IoT networks. To address this, various studies are currently being conducted to integrate PQC into IoT environments.

Kumar et al. [52] classified the types of quantum-based attacks considering the resource constrained environment of IoT devices and conducted an extensive analysis of lattice-based, hash-based, code-based, and multivariate polynomial cryptography for quantum cryptography in IoT network environment. Since the Elliptic Curve Diffie-Hellman (ECDH) protocol, which is basically used in the IoT environment, has the disadvantage of being vulnerable to quantum attacks, the authors recommended using post-quantum key exchange algorithms such as lattice-based and hash-based cryptography rather than traditional security methods to enhance the security of IIoT devices.

Xu et al. [53] proposed a method that integrates Nested Hash Access (NHA) with Post-Quantum Encryption. By employing preamble coding at the Physical Layer (PHY), this approach encodes and hashes

preamble sequences in a randomized manner, enabling secure retrieval of preamble sequences from multiple devices while ensuring protection against attacks. Additionally, a privacy-preserving protocol based on the Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) code is incorporated, achieving a security standard of 128 bits or more to safeguard against quantum computing-based attacks. This innovative method effectively protects against both quantum and other sophisticated attacks while maintaining the reliability and efficiency of systems in critical IoT environments.

Yuan et al. [54] proposed a post-quantum based blockchain architecture for IoT using the Nth degree Truncated Polynomial Ring Unit (NTRU) lattice to address quantum-related security issues and recommended the use of post-quantum based cryptographic algorithms with quorums between multiple administrative domains such as NTRU for secure service coordination to address the shortcomings of IoT architectures utilizing traditional blockchains being vulnerable to quantum attacks. A post-quantum secure multiparty cooperative signature scheme was proposed to address data leakage and privacy threats using formal security proofs and prototypes for resource-constrained IIoT devices.

Yi [55] proposed a post-quantum blockchain technique based on post-quantum ring signature scheme. This technique is introduced to ensure security and privacy in the Social Internet of Things (SIoTs) environment. It utilizes post-quantum ring signatures signed by a group of users, allowing other users to verify the messages while keeping the identity of the message owner confidential.

Blanco-Romero et al. [56] proposed the integration of post-quantum cryptography into lightweight IoT communication protocols, specifically the Constrained Application Protocol and MQTT for Sensor Networks (MQTT-SN), by enhancing the libcoap and Paho MQTT-SN Gateway libraries using the wolfSSL library, which supports PQC algorithms like Kyber512. The modified protocols were tested on devices such as Raspberry Pi 4 to evaluate the feasibility and performance impact of using PQC in constrained environments. Their results demonstrated that Kyber512, both in standalone and hybrid configurations, provided better performance than traditional cryptographic algorithms like P-256 in certain scenarios, with minimal impact on communication latency. This paper validated the applicability of PQC in IoT systems while addressing the challenges of computational overhead and memory consumption, highlighting the potential of PQC to enhance IoT security against quantum threats.

Samandari et al. [57] proposed integrating post-quantum cryptographic methods into the MQTT protocol to address authentication and security challenges in IoT systems, focusing on two approaches: CRYSTALS-Dilithium digital signatures and CRYSTALS-Kyber key encapsulation mechanisms (KEM). The study implemented these methods and evaluated their impacts on CPU, memory, and disk usage in resource-constrained environments. Results demonstrated that while both methods effectively enhanced security, the KEM-based approach significantly improved connection speeds, achieving a 71% reduction in authentication time compared to digital signatures, albeit with slightly higher memory overhead. These findings highlight the practicality of KEM-based authentication for lightweight and secure IoT communication.

Rampazzo et al. [58] investigated the performance impact of integrating hybrid post-quantum cryptography into the MQTT protocol within an Industrial IoT (IIoT) context. By utilizing hybrid TLS, which combines classical cryptographic algorithms with PQC methods like DILITHIUM and FALCON, the study evaluated memory consumption, CPU usage, and network data transmission in secure MQTT communication scenarios. Testing was conducted in a simulated IIoT environment with constrained edge devices acting as MQTT publishers. The findings demonstrated that hybrid protocols significantly increased data transmission volumes due to larger PQC-based certificates, with FALCON requiring less memory and CPU cycles than DILITHIUM. Despite the additional overhead, the computational demand remained manageable for devices with moderate resources, ensuring enhanced security against quantum threats without excessive

performance degradation. These results highlight the feasibility of adopting hybrid PQC for MQTT in IIoT environments, paving the way for more secure communication in a post-quantum era.

Castiglione et al. [59] proposed an innovative approach to integrate post-quantum cryptography and blockchain technology to enhance the security of low-cost IoT devices, focusing on the Dilithium-5 digital signature algorithm. The study utilized ESP32 microcontrollers, leveraging their hardware-accelerated cryptographic capabilities to ensure quantum-resistant security while maintaining energy efficiency and cost-effectiveness. A case study involving a portable device for monitoring blood oxygen levels and heart rate demonstrated the feasibility of the proposed solution in real-world healthcare applications. The results validated the practicality of implementing PQC on resource-constrained IoT devices, ensuring secure data transmission and resilience against quantum attacks, thus paving the way for broader adoption of quantum-secure IoT infrastructures.

Ye et al. [60] introduced a highly efficient lattice-based post-quantum cryptography processor tailored for IoT applications. Their design incorporates a customized Single-Instruction-Multiple-Data (SIMD) architecture to execute polynomial operations and accelerate the Keccak algorithm, essential for lattice-based schemes like Kyber and Dilithium. By implementing data shuffling units to manage dependencies and a dual-issue path for memory access, the processor achieves over a tenfold speed increase compared to baseline RISC-V processors and a fivefold improvement over ARM Cortex M4 implementations. Operating at 200 MHz with minimal power consumption, this processor presents a promising solution for securing IoT communications and storage in a post-quantum era. The summary of the above-mentioned researches are depicted in Table 2.

Table 2: Summary of post-quantum cryptography

Paper	Year	Findings	Contributions
[52]	2022	Identified quantum vulnerabilities in ECDH and recommended lattice-based and hash-based PQC for secure key exchange.	Conducted a comprehensive analysis of quantum-resistant cryptographic schemes for secure IIoT environments.
[53]	2023	Proposed Nested Hash Access with Post-Quantum Encryption and a QC-MDPC-based privacy-preserving protocol, achieving a security level of 128 bits.	Ensured secure preamble retrieval and protection against quantum and sophisticated attacks while maintaining efficiency in IoT contexts.
[54]	2023	Introduced NTRU lattice-based post-quantum blockchain with a multiparty cooperative signature scheme to secure IoT systems against quantum threats.	Enhanced secure coordination across multiple administrative domains using PQC and addressed data leakage in IIoT architectures.
[55]	2021	Developed a post-quantum ring signature technique to ensure security and privacy, allowing group signature verification while protecting the sender's identity.	Provided a privacy-preserving mechanism for SIoT environments, safeguarding communication against quantum-based attacks.

(Continued)

Table 2 (continued)

Paper	Year	Findings	Contributions
[56]	2024	Integrated Kyber512 PQC into CoAP and MQTT-SN protocols with minimal impact on latency, achieving better performance than traditional cryptographic algorithms like P-256 in constrained environments.	Demonstrated PQC integration feasibility in lightweight IoT protocols and addressed computational overhead and memory constraints.
[57]	2023	Showed that CRYSTALS-Kyber KEM-based authentication reduced authentication time by 71% compared to digital signatures, with manageable memory overhead.	Highlighted the practicality of PQC-based KEM for enhancing lightweight and secure MQTT communication in IoT systems.
[58]	2023	Hybrid PQC protocols like FALCON and DILITHIUM increased transmission volumes but provided quantum-resistant security with manageable resource demands.	Paved the way for integrating hybrid PQC into MQTT for secure IIoT communication while addressing performance and scalability challenges.
[59]	2024	Demonstrated the feasibility of implementing PQC (Dilithium-5) on ESP32 microcontrollers, ensuring quantum-resistant security in resource-constrained healthcare devices.	Integrated PQC and blockchain technology to enhance IoT security and tested solutions in real-world applications like health monitoring systems.
[60]	2024	Developed a SIMD-based lattice processor for PQC, achieving over 10× speed improvement compared to RISC-V processors and 5× improvement over ARM Cortex M4 with minimal power consumption.	Presented an efficient, energy-saving PQC processor design tailored for IoT, ensuring secure communications and data storage in post-quantum environments.

Recent research on post-quantum cryptography in IoT and Edge/Fog Computing environments has been progressing toward enhancing security, efficiency, and practical deployment feasibility. Since IoT devices operate with limited resources, researchers are exploring lightweight PQC implementations that minimize computational overhead while maintaining strong security. Ongoing studies focus on integrating PQC into existing IoT communication protocols, such as MQTT and CoAP, to ensure seamless adoption without significant performance degradation. Additionally, hybrid cryptographic frameworks that combine traditional cryptographic methods with post-quantum cryptography are being proposed to maintain compatibility with existing systems while supporting a gradual transition to PQC.

Meanwhile, research is being conducted on hardware acceleration techniques, such as FPGA-based accelerators and SIMD-optimized cryptographic processors, to enhance the execution speed of PQC and address latency issues in real-time IIoT applications. Furthermore, studies are exploring the use of blockchain and decentralized architectures to ensure data integrity and secure key exchange mechanisms. Moving forward, research is expected to focus on strengthening the scalability, interoperability, and standardization of PQC solutions, ensuring that they can be effectively deployed across heterogeneous IoT infrastructures.

The ultimate goal is to establish a secure and reliable post-quantum environment for Edge and Fog Computing networks.

2.3.2 Quantum Key Distribution for IoT Security

IoT environments require distributed computing models, such as Edge and Fog Computing, to handle data processing and meet real-time demands. These models enable localized data processing and analysis without relying on central cloud infrastructure, thereby reducing latency and network load while improving efficiency. Existing IoT networks lack quantum-resistant secret key sharing methods capable of meeting the confidentiality requirements of wide-area mobile applications, positioning Quantum Key Distribution as a critical alternative [61]. QKD systems, like post-quantum cryptography, are technologies that can create secure environments against quantum-based attacks [62]. In IoT environments, which involve distributed networks and resource-constrained devices, implementing secure key exchanges through QKD is considered a significant challenge. QKD offers the ability to detect eavesdropping and ensures data integrity during the key exchange process, significantly enhancing the reliability and security of IoT networks. However, the implementation of QKD is currently limited by hardware and cost constraints, and various research and technological advancements are underway to address these challenges.

Pham et al. [63] proposed a security solution for 5G-based IoT networks using Quantum Key Distribution integrated with a Radio-over-Fiber (RoF) system. In this approach, quantum keys are encoded into the intensity of radio-frequency subcarriers, transmitted through optical fibers to base stations (gNBs), and wirelessly forwarded to IoT gateways. The system leverages continuous-variable QKD with subcarrier intensity modulation to securely distribute secret keys. Results demonstrated a low quantum bit error rate and a high secret key rate, highlighting the method's efficiency and practicality for securing IoT communications in 5G environments.

Mukherjee et al. [64] proposed a QKD-based geospatial Fog Computing model to enhance security in fog networks against attacks such as denial-of-service and resource abuse. This system integrates quantum key distribution for secure symmetric key negotiation between fog nodes, ensuring information-theoretic security while maintaining forward secrecy and long-term protection. The methodology utilizes polarized photons for secure key generation and transmission through quantum and classical channels, allowing data encryption and secure transfer between edge, fog, and cloud layers. The results demonstrated the proposed model's capability to withstand various security threats and improve the overall security framework of Fog Computing systems.

Zhu et al. [65] proposed a resource allocation strategy for QKD-secured data center networks (DCNs) with cloud–edge collaboration, aiming to optimize the allocation of communication, computation, caching, and cryptographic (4C) resources. They developed an Integer Linear Programming (ILP) model and a heuristic algorithm named CryptoD-4CRA to minimize cryptographic resource consumption. The proposed system integrates QKD to generate secure keys and address security challenges in distributed networks. Their simulations demonstrated that the CryptoD-4CRA algorithm effectively reduces cryptographic resource usage while maintaining high service success ratios, showing its feasibility and efficiency in securing data center networks with cloud–edge collaboration.

Cicconetti et al. [66] proposed a framework for integrating Quantum Key Distribution with Multi-access Edge Computing (MEC) to enhance security in distributed computing systems. The solution leverages ETSI MEC and ETSI QKD standards to create secure communication channels between edge applications using quantum-secured key exchange protocols. Through a detailed software architecture, the authors describe the interaction between edge applications and QKD components, such as QKD devices and key

management entities, to establish secure contexts for encrypted communication. The proposed approach addresses current technological gaps and explores the potential for federating Edge Computing domains. The study highlights the feasibility of combining QKD with Edge Computing while identifying deployment challenges, such as high infrastructure costs and limited scalability, and provides recommendations for future research to overcome these issues.

Turjya et al. [67] proposed a secure architecture combining QKD and sugar-salt encryption within a Cloud-Fog Computing framework for online banking data protection. The QKD generates quantum-secured keys at the fog layer, identifying interception attempts via quantum state alterations. Data is categorized by security levels, with critical information stored in the cloud and non-sensitive data in the fog. Sugar-salt encryption introduces fake data for incorrect key guesses, mitigating brute-force attacks. Experimental results demonstrated reduced encryption time, improved performance, and stronger resilience against cyber threats compared to conventional methods.

Mangla et al. [68] proposed a secure data transmission framework for Fog Computing using Quantum Key Distribution. They identified security challenges across cloud, edge, and end-device layers in Fog Computing and addressed them with QKD protocols like BB84, Coherent One-Way (COW), and others. These protocols leverage quantum properties, such as superposition and entanglement, to secure data against attacks like DoS, sniffing, and node tampering. A healthcare use case demonstrated the framework's ability to encrypt sensitive patient data and ensure secure communication between fog nodes and cloud servers. The proposed system enhances data security and paves the way for future quantum-secured Fog Computing applications.

Hossain et al. [69] proposed the Quantum-Edge Cloud Computing (QECC) paradigm, which integrates quantum computing, Edge Computing, and cloud computing to address scalability, latency, and security issues in IoT applications. The framework leverages quantum cryptography, including QKD, to ensure data integrity and confidentiality, while Edge Computing reduces latency through localized processing, and cloud computing provides scalability and resource abundance. Through case studies in Bangladesh's smart cities and healthcare sectors, the authors demonstrated significant improvements in processing speeds, response times, and error rates. The study highlighted the potential of QECC to overcome limitations of traditional IoT frameworks and outlined future research directions, including quantum-resistant cryptography and optimized quantum algorithms.

Chen et al. [70] proposed the DDKA-QKDN (Dynamic On-Demand Key Allocation Scheme) to enhance security in the Quantum Internet of Things (Q-IoT) using a QKD network. This scheme addresses challenges of low quantum key generation rates and resource scarcity by dynamically allocating quantum keys through Quantum Key Pools (QKPs) placed at edge gateways. It prioritizes key requests based on arrival time, quantity, and security needs, ensuring efficient allocation and on-demand supplementation. Simulations demonstrated improved efficiency in responding to IoT key requests, reduced delays, and enhanced key utilization, highlighting its applicability to scalable and secure Q-IoT frameworks. The summary of the above-mentioned research is depicted in Table 3.

Table 3: Summary of quantum-key-distribution

Paper	Year	Findings	Contributions
[63]	2022	Proposed a QKD integrated with RoF system for 5G IoT networks.	Demonstrated low QBER and high secret key rate for secure IoT communication.

(Continued)

Table 3 (continued)

Paper	Year	Findings	Contributions
[64]	2022	Developed a QKD-based geospatial Fog Computing model for secure fog networks.	Showed robustness against DoS and resource abuse while maintaining forward secrecy.
[65]	2023	Presented a QKD-secured resource allocation strategy for DCNs with cloud-edge collaboration.	Optimized cryptographic resource usage with CryptoD-4CRA, maintaining high success ratios.
[66]	2024	Integrated QKD with MEC to enhance security in distributed computing systems.	Proposed a secure edge framework following ETSI standards with quantum-secured channels.
[67]	2024	Combined QKD with sugar-salt encryption in a cloud-fog framework for online banking.	Improved encryption time and resilience against cyber threats in cloud-fog frameworks.
[68]	2022	Implemented QKD protocols in a Fog Computing framework for secure data transmission.	Enhanced IoT security with QKD-based protocols addressing various attack vectors.
[69]	2024	Introduced the QECC paradigm integrating quantum, edge, and cloud computing for IoT.	Showed improvements in processing speed and error rates in IoT use cases.
[70]	2022	Developed the DDKA-QKDN scheme for dynamic quantum key allocation in Q-IoT.	Improved key request response efficiency and scalability in Q-IoT using QKD.

Recent research on Quantum Key Distribution for IoT and Edge/Fog Computing environments has primarily focused on ensuring interoperability, scalability, and real-world deployment feasibility. Given the integration challenges between quantum and classical cryptographic frameworks, studies have explored standardized QKD protocols and hybrid security architectures that combine QKD with traditional encryption methods. For instance, research has proposed QKD-based secure key exchange models in Multi-access Edge Computing and geospatial Fog Computing to enhance secure communication while maintaining compatibility with existing infrastructure. Additionally, studies have developed dynamic quantum key allocation mechanisms and resource-optimized QKD frameworks to efficiently manage key distribution in large-scale IoT networks. Testing and verification methodologies, such as QKD implementations in 5G-based IoT and cloud-edge collaborative environments, have demonstrated the practicality of quantum-secured communications with reduced quantum bit error rate. Moving forward, research is increasingly focusing on standardization, real-time key management optimization, and cost-effective QKD hardware solutions to ensure scalable and seamless integration of quantum security into diverse IoT and Edge/Fog Computing infrastructures.

2.4 Key Consideration

The primary considerations for the integration of Quantum Key Distribution and Post-Quantum Cryptography into IoT, Edge, and Fog Computing environments are outlined as follows:

- Scalability: The scalability of QKD and PQC systems is essential for successful deployment in distributed IoT architectures. In environments where millions of devices interact in real-time, scalable key distribution networks for QKD and high-efficiency cryptographic algorithms for PQC are critical. These solutions must support the dynamic and extensive nature of IoT ecosystems while avoiding bottlenecks.
- Efficiency: Given the limited resources of IoT devices, computational and communication efficiency is vital. QKD and PQC often introduce significant computational overhead, which can hinder real-time data processing. To address this, lightweight cryptographic algorithms must be designed, and communication protocols must be optimized to minimize resource consumption while maintaining security.
- Security and Privacy: Ensuring the security and privacy of data in IoT environments is essential. QKD provides a theoretically unbreakable key distribution mechanism, while PQC ensures resilience against quantum attacks. Implementing these technologies at the edge layer can protect sensitive data and prevent eavesdropping or tampering. Furthermore, encrypting transmitted data and restricting sensitive information to trusted network components can enhance privacy.
- Data Integrity: Data integrity is a critical issue in IoT networks, as unauthorized manipulation or tampering can lead to severe consequences. QKD protocols must be robust against interception attempts, and PQC schemes should protect against data modification attacks. Integrating integrity-checking mechanisms, such as digital signatures, can ensure that transmitted data remains reliable and unaltered.

3 Cascade Error Identification-Based Quantum Key Distribution Protocol

In this section, we present the proposed enhancement to Quantum Key Distribution for securing IoT and Edge/Fog computing environments, addressing the limitations of existing QKD implementations. While traditional Cascade-based error correction ensures key reconciliation, its sequential nature introduces processing inefficiencies in large-scale networks. Additionally, conventional hash-based privacy amplification methods are vulnerable to quantum-based attacks. To overcome these challenges, we propose a parallelized Cascade error correction mechanism that significantly reduces error reconciliation time and integrates Kyber lattice-based cryptography for privacy amplification, enhancing quantum resistance. This section provides a detailed explanation of the proposed approach, outlining its architectural design, implementation methodology, and expected performance benefits. Through these improvements, the proposed QKD framework aims to enhance scalability, computational efficiency, and security robustness in distributed IoT and Edge/Fog infrastructures.

This paper proposes a novel enhancement to the Cascade protocol in Quantum Key Distribution by introducing parallel processing techniques for error correction and integrating lattice-based cryptography (Kyber) for privacy amplification. The traditional Cascade protocol, widely used in QKD systems, relies on a sequential error correction process that introduces computational delays, particularly in large-scale quantum networks. This inefficiency is due to the iterative nature of block parity checks and binary search for error detection, which significantly increases processing time as the key length grows. To overcome this limitation, we introduce a parallelized version of the Cascade protocol, where multiple blocks of the key are processed simultaneously instead of sequentially. This approach significantly reduces error reconciliation time, improving the scalability of QKD systems in real-world applications such as IoT and Edge/Fog Computing networks, where low-latency key exchange is essential.

Additionally, conventional privacy amplification techniques in QKD rely on hash-based methods, which, while effective in classical environments, are vulnerable to quantum adversaries using Grover's algorithm, making them less secure in a post-quantum world. To address this, we replace traditional hash-based privacy amplification with Kyber lattice-based encryption, a quantum-resistant cryptographic algorithm based on the Module Learning with Errors (MLWE) problem. This approach ensures that even

if an eavesdropper intercepts partial information about the key, it remains computationally infeasible to reconstruct the full key, thus maintaining strong security guarantees against quantum-enabled attacks. By integrating parallel error correction and post-quantum privacy amplification, the proposed enhancement provides both efficiency and robustness, making QKD more practical for large-scale, real-time quantum-secured networks.

Quantum Key Distribution utilizes the principles of quantum mechanics to distribute encryption keys with guaranteed security. A representative example of this is the BB84 protocol. However, due to practical limitations in the quantum channel connecting Bob and Alice, such as measurement errors caused by noise, the implementation of QKD requires addressing error correction processes to compensate for transmission errors, as well as privacy amplification to minimize information that a potential eavesdropper could exploit [71,72]. The Cascade protocol is widely employed as a representative error correction protocol in QKD, owing to its simplicity and efficiency [73]. When using the Cascade protocol for QKD, an error correction factor of approximately 1.1 to 1.2 can be achieved within a broad range of QBER from 0% to over 11%, but it has the drawback of requiring highly interactive communication [74]. Furthermore, due to the sequential nature of the Cascade protocol, it can lead to inefficiencies, particularly in channels with high error rates, as it significantly increases processing time. Additionally, conventional hash functions used in the privacy amplification process are increasingly vulnerable to security threats posed by the advent of quantum computing.

The proposed enhancement to the Cascade protocol in Quantum Key Distribution introduces parallel processing for accelerated error correction and lattice-based encryption for quantum-resistant privacy amplification, distinguishing it from existing QKD implementations. In traditional QKD systems, the Cascade error correction process is sequential, requiring multiple iterations of block-wise parity checks and binary search, leading to exponential processing delays as key lengths grow. To overcome this inefficiency, the proposed parallelized Cascade protocol divides the sifted key into multiple sub-blocks and applies simultaneous parity checks and error corrections across these blocks. This modification reduces computational complexity from $O(n \log n)$ to $O(\log n)$, significantly decreasing key reconciliation time and making QKD more efficient for high-speed, real-time quantum communication networks. Furthermore, traditional privacy amplification in QKD relies on hash-based methods, which are vulnerable to quantum attacks—particularly Grover's algorithm, which reduces the security level of hashed keys. To address this vulnerability, the proposed approach replaces classical hash-based privacy amplification with Kyber lattice-based encryption, a quantum-resistant cryptographic algorithm based on the Module Learning with Errors problem. Unlike hash-based techniques, Kyber remains secure even against quantum adversaries, ensuring long-term security and scalability for QKD deployments in IoT and Edge/Fog computing environments. By integrating parallel error correction and post-quantum privacy amplification, this enhancement not only accelerates QKD operations but also ensures robust security, making it a practical solution for large-scale, resource-constrained IoT and Edge networks.

Step 1. Block Partitioning: Alice and Bob divide the shared key into fixed-size blocks, which allows them to perform independent parity checks on smaller sections of the key.

Step 2. Parity Check: Alice and Bob compare the parity (odd/even) of each block to detect if there is an error within that block.

Step 3. Binary Search: If there is a parity mismatch, they divide the block in half and repeat the parity check, narrowing down the search to efficiently locate the erroneous bit.

Step 4. Error Correction: Once the erroneous bit is found, Alice and Bob correct it by matching their bits, ensuring both share the same secret key.

Step 5. Block Size Doubling and Repetition: After one pass, the block size is doubled, and the process is repeated to efficiently detect and correct any remaining errors in larger blocks.

Step 6. Random Permutation (Optional): Random permutations may be applied to the key bits to evenly distribute errors and prevent clustering, making error detection more efficient.

Step 7. Multiple Pass Repetition: The entire process is repeated through multiple passes, ensuring that all errors are detected and corrected, and Alice and Bob end up with identical keys.

The Cascade protocol is a method primarily used for error correction in the BB84 protocol. It plays a crucial role in detecting and correcting errors that occur during quantum key distribution. As shown in Fig. 3, the Cascade protocol corrects bit errors through multiple passes, with each pass depending on the results of the previous one. Empirical analysis of the Cascade protocol suggests using $k_1 = 0.73/p$ as the optimal value, where p is the estimated QBER. It has been confirmed that the original CASCADE protocol is sufficient with four iterations for effective key reconciliation [75]. However, because the initial block length depends on the estimated QBER, it is safe to perform all iterations unless the block length k_i is equal to the key length [76]. Due to the iterative nature of this process, the computational load can increase exponentially, and since each pass is executed sequentially, the time required also increases as the key length grows.

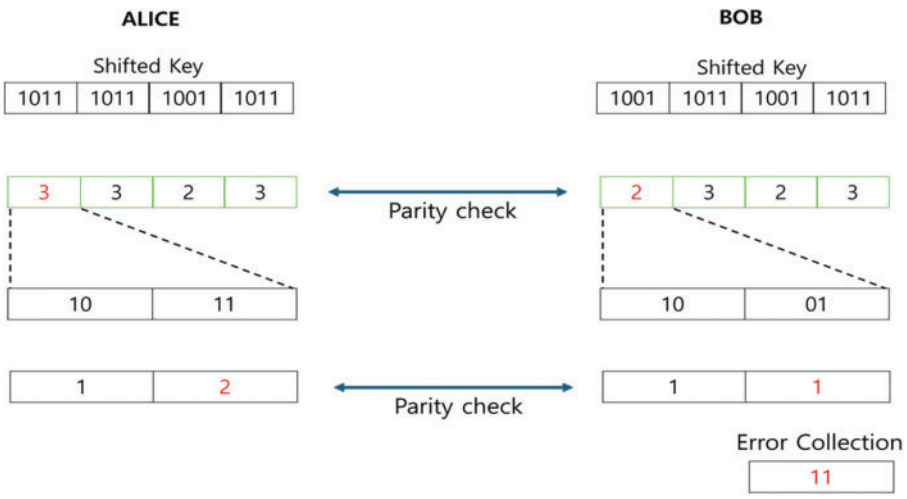

Figure 3: Basic cascade protocol

The Cascade protocol is a widely used error correction method in quantum key distribution systems, designed to ensure that Alice and Bob can share the same secret key even after the quantum communication stage, despite errors caused by noise during transmission. The protocol operates by dividing the shared key into smaller blocks and performing parity checks to detect errors within those blocks. When a parity mismatch is found, binary search is used to efficiently locate and correct the erroneous bit within the block.

To enhance error correction, the process is repeated over multiple passes, adjusting the block size to effectively identify and correct any remaining errors. Each pass of the Cascade protocol not only performs error correction but also applies random permutation through shuffling to the key bits, helping to evenly distribute errors and prevent clusters of errors from being hidden in specific parts of the key [77]. After multiple passes (typically 3 to 4), Alice and Bob can be confident that all errors have been corrected, and they share the same key. Due to its iterative nature, the protocol achieves high error correction efficiency while minimizing the amount of information exposed to a potential eavesdropper.

Step 1. Data Collection and Error Location Identification: The error correction process begins with Alice and Bob collecting the shared bit strings and identifying initial error locations.

Step 2. Block Division and Parallel Error Correction: The bit string is divided into multiple blocks, and parallel processing techniques are used to correct errors in each block simultaneously.

Step 3. Synchronization and Interaction: The parallel-processed blocks are synchronized to maintain consistency, and interaction between Alice and Bob is used to exchange corrected information.

Step 4. Repetition of Passes and Block Repartitioning: To enhance error correction, the blocks are redistributed, and the parallel correction process is repeated as necessary.

Step 5. Final Result Integration and Verification: After completing error correction in all blocks, the corrected bit strings are integrated, and the final result is verified.

Step 6. Result Verification: The final bit strings are checked for consistency to ensure that the error correction process has been successfully completed.

Fig. 4 illustrates the traditional CASCADE protocol, which is widely used for error correction in quantum key distribution systems. This protocol sequentially detects and corrects errors in shared keys through multiple iterations, ensuring both parties obtain identical keys despite transmission noise. However, due to its sequential nature, the traditional CASCADE protocol suffers from increased processing time, making it less suitable for large-scale or high-speed quantum communication systems. Parallel processing enables multiple blocks of a selected key to be checked for errors simultaneously rather than sequentially, thereby reducing the overall correction time. Each segment of the key is checked for parity, and if there is a mismatch, a binary search is performed to find and correct errors within the block. This parallel approach ensures faster error correction while maintaining the reliability and security of the CASCADE protocol, making it more suitable for large-scale or high-speed quantum communication systems.

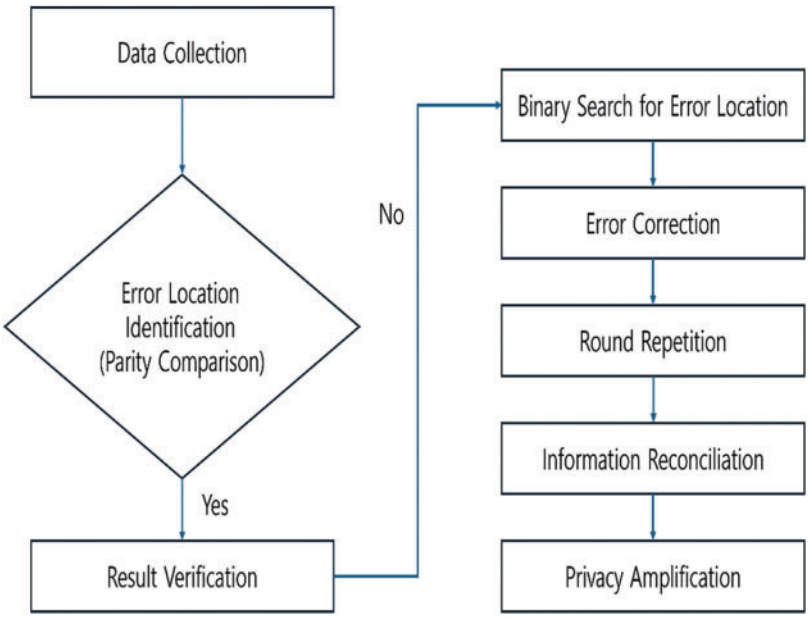

Figure 4: Existing cascade error identification process

In the conventional Cascade protocol, all error correction tasks are performed sequentially. However, with the introduction of parallel processing, multiple blocks can be processed simultaneously, significantly

accelerating the overall process. The main differences between the conventional Cascade protocol and the parallel processing algorithm become apparent in steps 2 through 5. In the conventional Cascade protocol, error correction is carried out sequentially, correcting one block at a time. In contrast, the parallel processing algorithm performs error correction on multiple blocks simultaneously, and the error correction results for each block are integrated through a synchronization process, substantially reducing the total error correction time. Furthermore, in the traditional approach, blocks are re-divided, and the error correction process is repeated sequentially. However, in the parallel processing algorithm, multiple blocks can still be processed concurrently even after re-division, improving the efficiency of the iterative process. Ultimately, the integration of error-corrected blocks to generate the final secret key is completed more quickly, significantly enhancing overall processing speed and efficiency while ensuring fast error correction with maintained reliability and security, making it suitable for large-scale or high-speed quantum communication systems.

The BB84 protocol has traditionally relied on hash functions for privacy amplification. However, with advancements in quantum computing, concerns have been raised about the security of hash function-based approaches. Hash functions based on addition or multiplication are vulnerable to quantum attacks that exploit hidden subgroup algorithms on quantum computers, and in particular, quantum computers can utilize Grover's algorithm to increase the likelihood of hash function collisions, potentially rendering traditional hash-based privacy amplification ineffective [78]. The proposed approach introduces CRYSTALS Kyber [79] in place of hash functions to maintain computational efficiency while enhancing resistance to quantum attacks. CRYSTALS Kyber is one of the first post-quantum cryptography algorithms selected by the U.S. National Institute of Standards and Technology [80]. It is quantum-resistant, as it is based on the hardness of solving the Module Learning with Errors problem in lattice-based cryptography, and it also provides resistance against various cryptographic attacks [81]. The proposed method consists of the following steps and will be used to compare performance and verify security against existing methods:

Step 7. Bit String Acquisition after Error Correction: After completing the error correction process, Alice and Bob obtain a shared bit string that serves as the basis for generating the final secure key.

Step 8. Block Division of the Bit String: The acquired bit string is divided into multiple blocks to facilitate the encryption process and ensure manageability during subsequent steps.

Step 9. Kyber Key Generation and Exchange: Alice and Bob use the Kyber algorithm to generate cryptographic keys and securely exchange them, establishing the necessary parameters for encryption.

Step 10. Encryption of the Bit String Using Kyber: Each block of the bit string is encrypted using the Kyber algorithm, transforming the data into a secure format resistant to quantum attacks.

Step 11. Storage and Transmission of the Encrypted Bit String: The encrypted blocks are securely stored and transmitted between Alice and Bob, ensuring the integrity and confidentiality of the data.

Step 12. Reduction of Encrypted Data Length: The length of the encrypted data is reduced through a process that retains security while making the key more compact and efficient.

Step 13. Security Evaluation of the Reduced Bit String: The reduced encrypted bit string is evaluated to ensure it maintains strong security properties, particularly against potential quantum-based threats.

Step 14. Decryption and Final Key Extraction: Bob decrypts the received encrypted bit string using the Kyber key to retrieve the final shared key that matches Alice's key.

Step 15. Estimation of Eavesdropper's Information and Security Verification: The potential information gained by an eavesdropper is estimated, and the security of the final key is verified to ensure its robustness against unauthorized access.

The proposed enhancement to the Cascade protocol introduces two key modifications to improve both efficiency and security in Quantum Key Distribution systems. First, parallel processing techniques are integrated into the error correction phase (Step 7), allowing multiple blocks of the key to undergo simultaneous error detection and correction. Unlike the traditional Cascade protocol, which sequentially processes each block, this parallelized approach significantly reduces the time required for error reconciliation, making it more suitable for large-scale or high-speed quantum networks. By dynamically adjusting block sizes based on real-time error distributions, this method optimizes resource utilization and minimizes latency.

The privacy amplification phase (Step 9) replaces conventional hash functions with Kyber-based lattice encryption to enhance resistance against quantum-based attacks. Traditional hash-based privacy amplification methods, such as those relying on addition or multiplication operations, are vulnerable to Grover's algorithm, which can efficiently find hash collisions, weakening security against quantum adversaries. In contrast, Kyber encryption is based on the Module Learning with Errors problem, which is known to be resistant to quantum computing attacks. This ensures that even if an adversary gains partial information about the shared key, reconstructing the final key remains computationally infeasible.

By integrating these two enhancements, the proposed approach not only accelerates the error correction process but also strengthens security in the face of emerging quantum threats. The combination of parallel error correction and lattice-based cryptographic techniques establishes a more efficient and robust framework for QKD, ensuring secure and scalable key distribution in future quantum communication networks.

One of the key advantages of using the Kyber algorithm instead of hash functions is the enhanced security it offers in a quantum computing environment. Designed as a quantum-resistant encryption algorithm, Kyber provides resilience against quantum computer-based attacks, ensuring the security of the privacy amplification process even in environments where quantum attacks are possible. Additionally, Kyber is highly efficient and performs well across a variety of environments, making it a robust solution for quantum-resistant cryptographic systems [82].

The Kyber algorithm is designed with structural efficiency and security in mind, enabling relatively fast and efficient key generation and exchange. The computational resources required for the privacy amplification stage of the BB84 protocol decrease, leading to improved overall process performance. In addition to its superior security, the Kyber algorithm achieves excellent performance in both hardware and software implementations across multiple platforms, and it integrates well with most existing internet protocols and cryptographic algorithm applications [83]. Therefore, using the Kyber algorithm instead of hash functions is a strategic choice that not only enhances security in the quantum computing era but also improves practical performance.

The QKD protocol proposed in this paper improves the traditional sequential Cascade error correction protocol by introducing parallel processing techniques and replaces hash functions with the CRYSTALS Kyber algorithm in the privacy amplification process, as shown in Fig. 5. The parallelized Cascade protocol in the proposed QKD system allows for simultaneous error correction across multiple blocks, significantly reducing error correction time and improving overall system efficiency. Additionally, by incorporating the Kyber algorithm, the protocol offers a higher level of security that is resistant to quantum computer-based attacks, enabling stronger encryption during the privacy amplification stage. These improvements greatly enhance the performance of the QKD system and ensure secure communication in the quantum computing era.

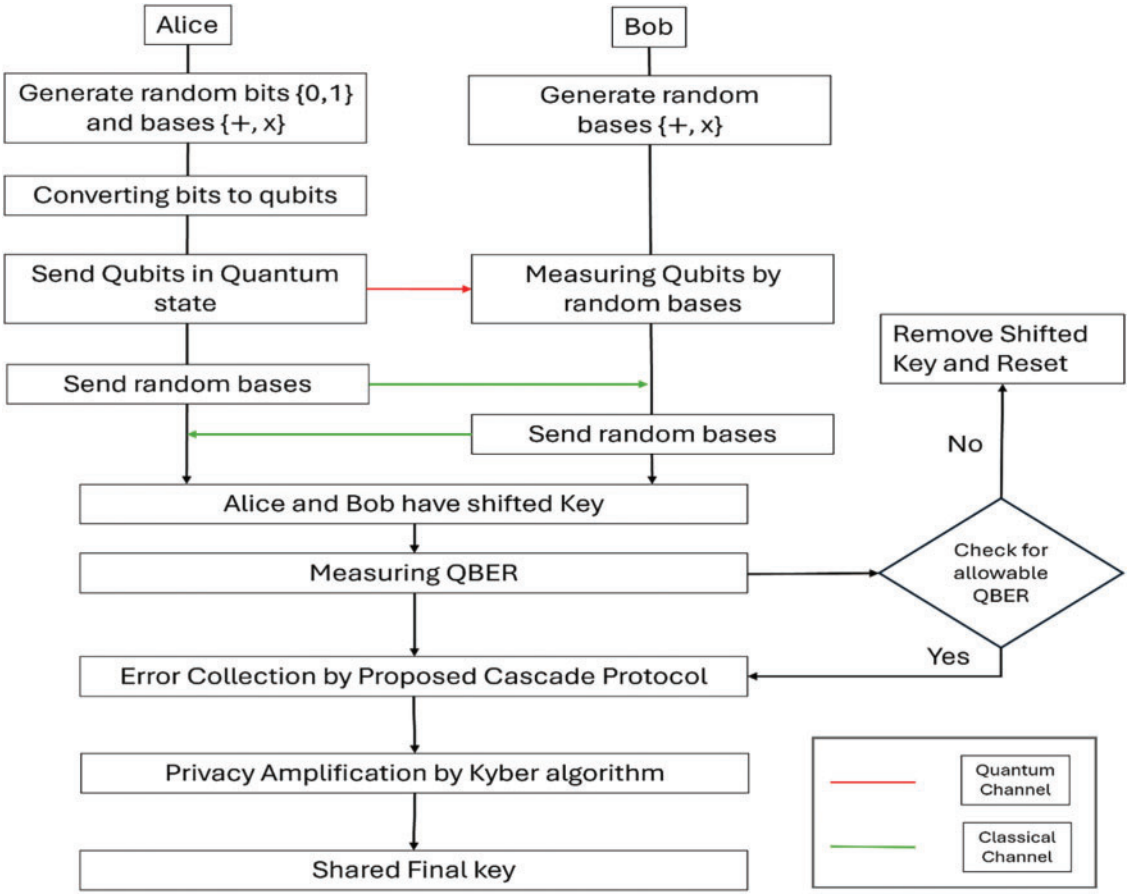

Figure 5: Proposed cascade error identification process

4 Discussion

The integration of Edge Computing and Fog Computing plays a crucial role in efficiently processing the vast amounts of data generated by sensors attached to IoT devices, enabling meaningful insights to be extracted [84]. This section summarizes and analyzes Post-Quantum Cryptography including Quantum Key Distribution technology and existing Edge network technology trends identified in the previous sections as depicted as follows;

In the field of Post-Quantum Cryptography, a variety of security technologies are currently being researched to address the threats posed by quantum computing. These researches particularly emphasize security threats in the Internet of Things and Industrial Internet of Things environments, with several research groups leading the development of new algorithms and protocols in anticipation of the post-quantum era. These studies are laying an important foundation for improving the efficiency, cost, and performance of security systems in the post-quantum age, and are opening new frontiers for data security and privacy protection in IoT environments.

The current state of Post-Quantum Cryptography faces challenges such as slow processing speeds and compatibility issues across diverse computing environments. Additionally, the rapid advancement of quantum computing technology necessitates the continuous reevaluation of the security of existing algorithms. To address these issues, fundamental improvements and advancements in post-quantum cryptographic technology are required. Consequently, the future research direction is as follows:

- Diversity and Efficiency Improvement of Algorithms: There is a continual need for the enhancement of current algorithms, as well as the development of new ones. In particular, increasing the efficiency and execution speed of current algorithms is critical.
- Integration with Hardware: The integration of PQC algorithms with both existing and new hardware architectures will become an important area of research, playing a key role in enhancing the efficiency and practicality of security solutions.
- Standardization Efforts: The standardization of PQC algorithms remains an ongoing and significant research area. Standardization facilitates the selection, evaluation, and deployment of algorithms.
- Testing and Verification in Real-World Environments: Conducting tests and verification of PQC solutions beyond laboratory settings is essential for evaluating their ability to respond to security threats in real-world scenarios.
- Interoperability between Quantum and Traditional Computing Environments: Enhancing interoperability between quantum computing and traditional computing environments is also a critical direction for research, allowing security solutions to remain compatible across various computing environments.

The current research trends in Quantum Key Distribution systems focus on enhancing security in Edge/Fog Computing and IoT environments. QKD is being applied to various IoT infrastructures, including 5G-based networks, fog networks, and cloud-edge collaborative environments, to ensure the confidentiality and integrity of data transmission. Furthermore, QKD enables secure key distribution between IoT devices and Edge/Fog nodes, while improving the efficiency of network resource allocation and cryptographic resource utilization. These trends address security threats in the distributed architecture of IoT devices and networks, contributing to the scalability and reliability of Edge/Fog environments.

Quantum Key Distribution systems currently face challenges such as the complexity of integration with Edge/Fog networks and IoT environments, limitations in transmission distance, and hardware constraints. Additionally, the rapid advancement of quantum computing necessitates the continuous reevaluation of QKD protocols' security and efficiency to meet the unique requirements of IoT and Edge/Fog networks. To address these challenges and enable the practical deployment and scalability of QKD systems in IoT and Edge/Fog computing environments, the following research directions are essential:

- Extending Transmission Range for Edge/Fog Networks: Research is needed to expand the transmission range of QKD systems to support secure data communication between IoT devices and Edge/Fog nodes.
- Enhancing Integration with IoT and Edge Networks: Developing methodologies to seamlessly integrate QKD systems into IoT and Edge/Fog networks is crucial for ensuring compatibility and functionality.
- Improving QKD Hardware Efficiency: Innovations in hardware components, such as photon detectors and quantum sources, are necessary to enhance the performance of QKD systems in Edge/Fog nodes.
- Increasing Key Generation Rates: Enhancing key generation rates is critical to meet the high-speed communication and real-time data processing requirements of IoT and Edge/Fog networks.
- Developing Scalable QKD Solutions: Designing scalable QKD architectures that support the distributed nature of Edge/Fog networks is vital for broader deployment.
- Fostering Standardization and Interoperability: Efforts to standardize QKD protocols and ensure interoperability with various IoT and Edge/Fog network architectures are essential for widespread implementation.

The proposed method has achieved significant advancements in both error correction and privacy amplification within the Quantum Key Distribution framework, specifically by utilizing parallel processing techniques for the Cascade protocol and lattice-based cryptography (Kyber) for privacy amplification. Traditional QKD implementations often suffer from high computational overhead and latency due to their sequential error correction process, which can be particularly detrimental in resource-constrained Edge

Computing environments. The proposed enhancement mitigates this issue by introducing parallel processing within the Cascade protocol, enabling simultaneous block-wise error correction, thereby significantly reducing error correction time. This approach ensures that large-scale edge networks can maintain low-latency cryptographic operations, which are essential for real-time data transmission in IIoT systems.

Furthermore, compatibility between PQC and QKD remains a major challenge, as legacy cryptographic infrastructures rely on classical encryption methods that were not inherently designed to coexist with quantum-resistant algorithms. The proposed solution addresses this by integrating Kyber-based lattice encryption into the privacy amplification phase, replacing conventional hash functions with a computationally efficient and inherently quantum-resistant alternative. Unlike existing PQC implementations that often require substantial modifications to network architectures, Kyber's efficient key encapsulation mechanism allows for seamless integration into existing IoT security frameworks, reducing the need for extensive hardware or software modifications.

From a technical perspective, this integration distinguishes itself from existing solutions by enhancing both security and performance simultaneously. The parallelized error correction mechanism ensures that quantum-secured key distribution remains feasible even in latency-sensitive environments, while lattice-based cryptographic techniques reinforce post-quantum security without introducing excessive computational overhead. These advancements collectively provide a scalable and efficient security framework for IoT and IIoT, ensuring resilience against both conventional and quantum-based cyber threats in future Edge/Fog computing infrastructures.

A practical example of embedding QKD and PQC in an IoT and Edge/Fog environment is a secure industrial IoT deployment for smart grid communication. In this setup, QKD is used to generate encryption keys at a central control station, which are then distributed via Quantum Key Management Systems (QKMS) to edge devices and fog nodes managing real-time energy distribution. These keys secure communication channels between IoT sensors, edge servers, and cloud systems. However, since not all devices are QKD-compatible, PQC algorithms (Kyber for key exchange, Dilithium for authentication) are used for non-quantum-enabled devices, ensuring backward compatibility.

For example, an IoT smart meter at a consumer's home would communicate securely with a fog computing node using Kyber-based key exchange, while the fog node itself interacts with the central grid using QKD-secured channels. This hybrid model ensures both quantum security and practical integration into existing infrastructure, making it easier for industries to transition into post-quantum security without overhauling their entire network.

However, there are several open research directions that can further enhance the performance, scalability, and security of QKD systems, especially in the context of emerging quantum technologies. Below are key areas for future investigation. While the introduction of parallel processing significantly improves the efficiency of the Cascade protocol, further research is needed to explore optimization strategies for parallel error correction. Investigating how to dynamically adjust the number and size of blocks based on real-time channel conditions, such as varying error rates and noise levels, could lead to even more efficient resource utilization. Additionally, exploring more sophisticated synchronization techniques between parallel threads could minimize latency and further enhance the overall speed of the error correction process.

While Post-Quantum Cryptography provides enhanced security against quantum attacks, it introduces computational overhead that poses challenges for resource-constrained IoT devices. One of the primary trade-offs is the increased key size in PQC algorithms compared to classical cryptographic methods. For example, lattice-based cryptographic schemes, such as Kyber and CRYSTALS-Dilithium, require significantly larger public and private keys than traditional RSA or ECC systems. This increase in key size leads

to higher memory consumption, greater computational complexity, and increased energy usage, which may impact the performance of battery-operated IoT devices. Additionally, the encryption and decryption times in PQC algorithms tend to be longer, which can introduce latency in real-time applications, such as autonomous systems and industrial IoT networks. To mitigate these performance constraints, researchers are exploring lightweight PQC implementations tailored for IoT environments, optimizing cryptographic computations through hardware acceleration (FPGA-based PQC), hybrid cryptographic frameworks, and efficient key exchange protocols. Balancing security and efficiency remains a critical challenge in deploying PQC within large-scale IoT and Edge/Fog computing environments.

The integration of Post-Quantum Cryptography and Quantum Key Distribution in Edge/Fog computing enhances processing efficiency and compatibility for IoT and IIoT security. Traditional cryptographic methods, such as RSA and ECC, face scalability and quantum vulnerability issues, while existing QKD implementations suffer from high latency and hardware constraints. The proposed parallelized Cascade protocol significantly reduces error correction time (from $O(n \log n)$ to $O(\log n)$), making QKD more practical for high-speed Edge/Fog networks. Additionally, replacing hash-based privacy amplification with Kyber lattice-based encryption ensures quantum resistance while maintaining low computational overhead, making it compatible with resource-limited IoT devices. Unlike traditional QKD frameworks, this hybrid approach enables seamless integration into existing network infrastructures, ensuring efficient, scalable, and future-proof security for real-time IIoT applications.

Ensuring interoperability between QKD and traditional computing is crucial for real-world IoT and Edge/Fog deployments. Current research trends focus on hybrid cryptographic frameworks, where QKD-generated keys are used alongside post-quantum encryption (Kyber, Dilithium) to maintain seamless compatibility with existing network protocols (TLS, IPsec, and MQTT-SN). Additionally, emerging Quantum Key Management Systems (QKMS) facilitate secure key distribution across heterogeneous classical and quantum infrastructure, ensuring backward compatibility with existing PKI-based security architectures.

For testing and verification, real-world pilot deployments are being conducted in 5G-enabled IoT networks, integrating ETSI-standardized QKD interfaces for latency and security benchmarking. Simulation environments using Quantum Network Simulators (QKDNetSim, SimulaQron) are used to assess key throughput, error rates, and resilience against eavesdropping. Further, hybrid quantum-classical testbeds, such as Japan's Tokyo QKD Network and Europe's OPENQKD project, validate secure edge-to-cloud data transfer under real-world constraints. These mechanisms ensure that QKD can be efficiently deployed alongside traditional security frameworks, making it viable for Edge/Fog computing and industrial IoT applications.

The proposed approach enhances PQC execution speed and hardware compatibility for IoT and Edge/Fog computing. To reduce computational overhead, Number Theoretic Transform (NTT) optimizations accelerate Kyber key exchange and Dilithium signatures, while hybrid encryption (Kyber + AES-GCM) balances security and efficiency. Hardware integration includes FPGA acceleration and RISC-V cryptographic cores, improving modular arithmetic performance. Additionally, lightweight PQC implementations on ARM Cortex-M and Edge TPU processors enable low-power, real-world deployment. These optimizations ensure scalable, efficient, and quantum-secure cryptographic operations in resource-constrained environments.

The current proposal outlines the repartition of blocks during the error correction phase. Future work could focus on adaptive repartitioning mechanisms that automatically adjust the number of passes and block sizes in response to ongoing error detection feedback. Machine learning techniques could be applied to predict the optimal block size and number of passes based on previous communication sessions, further reducing processing time and enhancing error correction accuracy.

5 Conclusion

The current Edge/Fog computing environment and IoT systems built upon it are continuously exposed to security threats, with the vulnerabilities of traditional encryption methods becoming more pronounced due to advancements in quantum computing technology. To address these challenges, extensive research is being conducted on security frameworks that combine Quantum Key Distribution and Post-Quantum Cryptography. QKD leverages the principles of quantum mechanics to enable secure key distribution, while Post Quantum Cryptography employs quantum-resistant algorithms to enhance data protection across IoT networks. This paper reviewed the latest research trends in QKD and PQC and discussed approaches for integrating these technologies with the security requirements of Edge/Fog computing environments and IoT systems.

Future research should focus on the practical implementation and scalability of QKD and PQC technologies. For QKD, technical challenges such as extending transmission distances, improving key generation rates, and ensuring seamless integration with Edge/Fog networks must be addressed. For PQC, it is crucial to compare and analyze the performance and security of various algorithms and design lightweight cryptographic solutions tailored to the constraints of IoT devices.

A key challenge in transitioning to quantum-resistant security is the reluctance of industries to immediately replace existing Public Key Infrastructure (PKI)-based systems with post-quantum cryptographic solutions due to concerns over compatibility, performance overhead, and deployment costs. A promising approach to mitigate these challenges is the hybrid cryptographic framework, where classical cryptography and PQC coexist to ensure a gradual transition. Hybrid security models integrate traditional encryption schemes (RSA, ECC, AES) with PQC algorithms (Kyber, CRYSTALS-Dilithium, NTRU), allowing organizations to maintain backward compatibility while progressively adopting quantum-resistant mechanisms. This dual-layer approach ensures that even if classical encryption becomes vulnerable to quantum attacks, a secondary post-quantum security layer remains intact, safeguarding sensitive data. Additionally, hybrid cryptography enables adaptive security policies, allowing industries to switch to full PQC implementations once standardization efforts such as NIST PQC initiatives and hardware acceleration techniques mature. Future research should explore the optimal trade-offs between security, computational efficiency, and scalability in hybrid cryptographic deployments, ensuring that industries can transition smoothly into the post-quantum era without disrupting existing infrastructures.

Acknowledgement: None.

Funding Statement: This research was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2022K1A3A1A61014825). Fund receiver: Jong Hyuk Park. https://www.nrf.re.kr/index (accessed on 31 December 2024).

Author Contributions: Seo Yeon Moon: conceptualization, methodology, formal analysis, writing—original draft, visualization; Byung Hyun Jo: investigation, methodology, validation; Abir El Azzaoui: data collection, visualization, writing—review & editing; Sushil Kumar Singh: supervisor, conceptualization, review, fund acquisition; Jong Hyuk Park: supervisor, conceptualization, review, fund acquisition. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data not available due to commercial restrictions.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

QKD	Quantum Key Distribution
PQC	Post-Quantum Cryptography
IoT	Internet of Things

References

1. Kim T, Yoo SE, Kim Y. Edge/fog computing technologies for IoT infrastructure. Sensors. 2021;21(9):3001. doi:10.3390/s21093001.
2. Li K, Wang H, Mu X, Chen X, Shin H. Dynamic logical resource reconstruction against straggler problem in edge federated learning. Hum Centric Comput Inf Sci. 2024;14:25. doi:10.22967/HCIS.2024.14.025.
3. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. Sensors. 2019;19(8):1788. doi:10.3390/s19081788.
4. Yu W, Liang F, He X, Hatcher WG, Lu C, Lin J, et al. A survey on the edge computing for the Internet of Things. IEEE Access. 2017;6:6900–19. doi:10.1109/ACCESS.2017.2778504.
5. Wang J, Huang D. Visual Servo Image real-time processing system based on fog computing. Hum-Centric Comput Inf Sci. 2023;13(48):1–14. doi:10.22967/HCIS.2023.13.048.
6. Yousefpour A, Fung C, Nguyen T, Kadiyala K, Jalali F, Niakanlahiji A, et al. All one needs to know about fog computing and related edge computing paradigms: a complete survey. J Syst Archit. 2019;98:289–330. doi:10.1016/j.sysarc.2019.02.009.
7. Ometov A, Molua O, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022;22(3):927. doi:10.3390/s22030927.
8. Alwakeel AM. An overview of fog computing and edge computing security and privacy issues. Sensors. 2021;21(24):8226. doi:10.3390/s21248226.
9. Ben Daoud W, Obaidat MS, Meddeb-Makhlouf A, Zarai F, Hsiao KF. TACRM: trust access control and resource management mechanism in fog computing. Hum Centric Comput Inf Sci. 2019;9(1):28. doi:10.1186/s13673-019-0188-3.
10. Raeisi-Varzaneh M, Dakkak O, Alaidaros H, Avci İ. Internet of things: security, issues, threats, and assessment of different cryptographic technologies. J Commun. 2024;19(2):78–89. doi:10.12720/jcm.19.2.78-89.
11. Alhakami H. Enhancing IoT security: quantum-level resilience against threats. Comput Mater Continua. 2024;78(1):329–56. doi:10.32604/cmc.2023.043439.
12. Sharma M, Choudhary V, Bhatia RS, Malik S, Raina A, Khandelwal H. Leveraging the power of quantum computing for breaking RSA encryption. Cyber Phys Syst. 2021;7(2):73–92. doi:10.1080/23335777.2020.1811384.
13. Joshi S, Bairwa AK, Pljonkin AP, Garg P, Agrawal K. From pre-quantum to post-quantum RSA. In: Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security; 2023 May 24–26; Larache, Morocco. doi:10.1145/3607720.3607721.
14. Liu T, Ramachandran G, Jurdak R. Post-quantum cryptography for Internet of Things: a survey on performance and optimization. arXiv:2401.17538v1. 2024.
15. Fernández-Caramés TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet Things J. 2020;7(7):6457–80. doi:10.1109/JIOT.2019.2958788.
16. EL Azzaoui A, Arif T, Park H, Chen H, Camacho D, Park JH. A comprehensive study on quantum computing technologies in smart city: review and future directions. Hum-Centric Comput Inf Sci. 2024;14(65):1–31. doi:10.22967/HCIS.2024.14.064.
17. Khalid A, McCarthy S, O'Neill M, Liu W. Lattice-based cryptography for IoT in a quantum world: are we ready? In: Proceedings of the 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI); 2019 Jun 13–14; Otranto, Italy. doi:10.1109/iwasi.2019.8791343.
18. Chen YJ, Hsu CL, Lin TW, Lee JS. Design and evaluation of device authentication and secure communication system with PQC for AIoT environments. Electronics. 2024;13(8):1575. doi:10.3390/electronics13081575.

19. Chung CC, Pai CC, Ching FS, Wang C, Chen LJ. When post-quantum cryptography meets the Internet of Things: an empirical study. In: Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services; 2022 Jun 27–Jul 1; Portland, OR, USA. doi:10.1145/3498361.3538766.
20. Adu-Kyere A, Nigussie E, Isoaho J. Quantum key distribution: modeling and simulation through BB84 protocol using Python3. Sensors. 2022;22(16):6284. doi:10.3390/s22166284.
21. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing; 1984 Dec 9–12; Bangalore, India.
22. Alomari A, Kumar SAP. Securing IoT systems in a post-quantum environment: vulnerabilities, attacks, and possible solutions. Internet Things. 2024;25(3):101132. doi:10.1016/j.iot.2024.101132.
23. Dam DT, Tran TH, Hoang VP, Pham CK, Hoang TT. A survey of post-quantum cryptography: start of a new race. Cryptography. 2023;7(3):40. doi:10.3390/cryptography7030040.
24. Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, et al. Transitioning organizations to post-quantum cryptography. Nature. 2022;605(7909):237–43. doi:10.1038/s41586-022-04623-2.
25. Bavdekar R, Jayant Chopde E, Agrawal A, Bhatia A, Tiwari K. Post quantum cryptography: a review of techniques, challenges and standardizations. In: Proceedings of the 2023 International Conference on Information Networking (ICOIN); 2023 Jan 11–14; Bangkok, Thailand. doi:10.1109/ICOIN56518.2023.10048976.
26. Kumar M, Pattnaik P. Post quantum cryptography (PQC)—an overview. In: Proceedings of the 2020 IEEE High Performance Extreme Computing Conference (HPEC); 2020 Sep 22–24; Waltham, MA, USA. doi:10.1109/hpec43674.2020.9286147.
27. Dizdarević J, Carpio F, Jukan A, Masip-Bruin X. A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. ACM Comput Surv. 2019;51(6):1–29. doi:10.1145/3292674.
28. Lalhriatpuii R, Wasson V. Comprehensive exploration of IoT communication protocol: coap, MQTT, HTTP, LoRaWAN and AMQP. In: Proceedings of the International Conference on Machine Learning Algorithms 2024; 2024 Feb 22–23; Himachal Pradesh, India. doi:10.1007/978-3-031-75861-4_23.
29. Dinculeană D, Cheng X. Vulnerabilities and limitations of MQTT protocol used between IoT devices. Appl Sci. 2019;9(5):848. doi:10.3390/app9050848.
30. Chen F, Huo Y, Zhu J, Fan D. A review on the study on MQTT security challenge. In: Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud); 2020 Nov 6–8; Washington, DC, USA. doi:10.1109/smartcloud49737.2020.00032.
31. Iglesias-Urkia M, Orive A, Urbieta A, Casado-Mansilla D. Analysis of CoAP implementations for industrial Internet of Things: a survey. J Ambient Intell Humaniz Comput. 2019;10(7):2505–18. doi:10.1007/s12652-018-0729-z.
32. Arvind S, Anantha Narayanan V. An overview of security in CoAP: attack and analysis. In: Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS); 2019 Mar 15–16; Coimbatore, India. doi:10.1109/icaccs.2019.8728533.
33. Jung JH, Gohar M, Koh SJ. CoAP-based streaming control for IoT applications. Electronics. 2020;9(8):1320. doi:10.3390/electronics9081320.
34. Al-Masri E, Kalyanam KR, Batts J, Kim J, Singh S, Vo T, et al. Investigating messaging protocols for the Internet of Things (IoT). IEEE Access. 2020;8:94880–911. doi:10.1109/ACCESS.2020.2993363.
35. Jaloudi S. Communication protocols of an industrial Internet of Things environment: a comparative study. Future Internet. 2019;11(3):66. doi:10.3390/fi11030066.
36. Yakupov D. Overview and comparison of protocols Internet of Things: mQTT and AMQP. Int J Open Inf Technol. 2022;10(9):90–8.
37. Caiza G, Llamuca ES, Garcia CA, Gallardo-Cardenas F, Lanas D, Garcia MV. Industrial shop-floor integration based on AMQP protocol in an IoT environment. In: Proceedings of the 2019 IEEE Fourth Ecuador Technical Chapters Meeting (ETCM); 2019 Nov 11–15; Guayaquil, Ecuador. doi:10.1109/etcm48019.2019.9014858.

38. Uy NQ, Nam VH. A comparison of AMQP and MQTT protocols for Internet of Things. In: Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS); 2019 Dec 12–13; Hanoi, Vietnam. doi:10.1109/nics48868.2019.9023812.
39. Zohourian A, Dadkhah S, Neto ECP, Mahdikhani H, Danso PK, Molyneaux H, et al. IoT Zigbee device security: a comprehensive review. Internet Things. 2023;22(2):100791. doi:10.1016/j.iot.2023.100791.
40. Pallavi S, Narayanan VA. An overview of practical attacks on BLE based IOT devices and their security. In: Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS); 2019 Mar 15–16; Coimbatore, India. doi:10.1109/icaccs.2019.8728448.
41. Khanchuea K, Siripokarpirom R. A multi-protocol IoT gateway and WiFi/BLE sensor nodes for smart home and building automation: design and implementation. In: Proceedings of the 2019 10th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES); 2019 Mar 25–27; Bangkok, Thailand. doi:10.1109/ictemsys.2019.8695968.
42. Mekki K, Bajic E, Meyer F. Indoor positioning system for IoT device based on BLE technology and MQTT protocol. In: Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT); 2019 Apr 15–18; Limerick, Ireland. doi:10.1109/wf-iot.2019.8767287.
43. Miles B, Bourennane EB, Boucherkha S, Chikhi S. A study of LoRaWAN protocol performance for IoT applications in smart agriculture. Comput Commun. 2020;164(8):148–57. doi:10.1016/j.comcom.2020.10.009.
44. Basford PJ, Bulot FMJ, Apetroaie-Cristea M, Cox SJ, Ossont SJJ. LoRaWAN for smart city IoT deployments: a long term evaluation. Sensors. 2020;20(3):648. doi:10.3390/s20030648.
45. Da Silva JT, Dias AL, Da Silva IN. A survey on OPC UA protocol: overview, challenges and opportunities. In: Proceedings of the 2023 15th IEEE International Conference on Industry Applications (INDUSCON); 2023 Nov 22–24; São Bernardo do Campo, Brazil. doi:10.1109/INDUSCON58041.2023.10375053.
46. Silva D, Carvalho LI, Soares J, Sofia RC. A performance analysis of Internet of Things networking protocols: evaluating MQTT, CoAP, OPC UA. Appl Sci. 2021;11(11):4879. doi:10.3390/app11114879.
47. Ioana A, Korodi A. DDS and OPC UA protocol coexistence solution in real-time and industry 4.0 context using non-ideal infrastructure. Sensors. 2021;21(22):7760. doi:10.3390/s21227760.
48. Fang S, Huang L, Li Z. DDS-based protocol-compatible communication platform for mining power system. IET Commun. 2020;14(1):158–64. doi:10.1049/iet-com.2019.0608.
49. Ho MH, Lai MY, Liu YT. Implementation of DDS cloud platform for real-time data acquisition of sensors for a legacy machine. Electronics. 2022;11(13):2096. doi:10.3390/electronics11132096.
50. Restuccia G, Tschofenig H, Baccelli E. Low-power IoT communication security: on the performance of DTLS and TLS 1.3. In: Proceedings of the 2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN); 2020 Dec 1–3; Berlin, Germany.
51. Abdulelah AJ, Mustafa AS. Advanced secure architecture for the Internet of Things based on DTLS protocol. In: Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT); 2020 Oct 22–24; Istanbul, Turkey. doi:10.1109/ismsit50672.2020.9254700.
52. Kumar A, Ottaviani C, Gill SS, Buyya R. Securing the future Internet of Things with post-quantum cryptography. Security Priv. 2022;5(2):e200. doi:10.1002/spy2.200.
53. Xu D, Liu L, Zhang N, Dong M, Leung VCM, Ritcey JA. Nested hash access with post quantum encryption for mission-critical IoT communications. IEEE Internet Things J. 2023;10(14):12204–18. doi:10.1109/JIOT.2023.3245360.
54. Yuan B, Wu F, Zheng Z. Post quantum blockchain architecture for Internet of Things over NTRU lattice. PLoS One. 2023;18(2):e0279429. doi:10.1371/journal.pone.0279429.
55. Yi H. Secure social Internet of Things based on post-quantum blockchain. IEEE Trans Netw Sci Eng. 2022;9(3):950–7. doi:10.1109/TNSE.2021.3095192.
56. Blanco-Romero J, Lorenzo V, Almenares F, Sánchez DD, Campo C, Rubio CG. Integrating post-quantum cryptography into CoAP and MQTT-SN protocols. In: Proceedings of the 2024 IEEE Symposium on Computers and Communications (ISCC); 2024 Jun 26–29; Paris, France. doi:10.1109/ISCC61673.2024.10733716.

57. Samandari J, Gritti C. Post-quantum authentication in the MQTT protocol. J Cybersecur Priv. 2023;3(3):416–34. doi:10.3390/jcp3030021.
58. José Aguiar Rampazzo F, Aurélio Amaral Henriques M. Assessment of the impact of hybrid post-quantum cryptography on the performance of the MQTT communication protocol. In: Proceedings of the 2023 Symposium on Internet of Things (SIoT); 2023 Oct 25–27; São Paulo, Brazil. doi:10.1109/SIoT60039.2023.10390050.
59. Castiglione A, Esposito JG, Loia V, Nappi M, Pero C, Polsinelli M. Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. IEEE Trans Ind Inf. 2025;21(2):1674–83. doi:10.1109/TII.2024.3485796.
60. Ye Z, Song R, Zhang H, Chen D, Cheung RC, Huang K. A highly-efficient lattice-based post-quantum cryptography processor for IoT applications. IACR Trans Cryptogr Hardw Embed Syst. 2024;2024(2):130–53. doi:10.46586/tches.v2024.i2.130-153.
61. Li G, Luo H, Yu J, Hu A, Wang J. Information-theoretic secure key sharing for wide-area mobile applications. IEEE Wirel Commun. 2024;31(1):118–24. doi:10.1109/MWC.012.2200289.
62. Xu G, Mao J, Sakk E, Wang SP. An overview of quantum-safe approaches: quantum key distribution and post-quantum cryptography. In: Proceedings of the 2023 57th Annual Conference on Information Sciences and Systems (CISS); 2023 Mar 22–24; Baltimore, MD, USA. doi:10.1109/CISS56502.2023.10089619.
63. Pham TA, Dang NT. Quantum key distribution: a security solution for 5G-based IoT networks. In: Proceedings of the 2022 International Conference on Advanced Technologies for Communications (ATC); 2022 Oct 20–22; Hanoi, Vietnam. doi:10.1109/ATC55345.2022.9943041.
64. Mukherjee P, Kumar Barik R. Fog-QKD: towards secure geospatial data sharing mechanism in geospatial fog computing system based on Quantum Key Distribution. In: Proceedings of the 2022 OITS International Conference on Information Technology (OCIT); 2022 Dec 14–16; Bhubaneswar, India. doi:10.1109/OCIT56763.2022.00096.
65. Zhu Q, Yu X, Zhao Y, Nag A, Zhang J. Resource allocation in quantum-key-distribution-secured datacenter networks with cloud-edge collaboration. IEEE Internet Things J. 2023;10(12):10916–32. doi:10.1109/JIOT.2023.3242725.
66. Cicconetti C, Sabella D, Noviello P, Paduanelli GD. Quantum-safe edge applications: how to secure computation in distributed computing systems. arXiv:2405.17008v1. 2024.
67. Turjya SM, Singh R, Sarkar P, Swain S, Bandyopadhyay A. Quantum-based QKD and sugar-salt encryption approach in cloud-fog computing to strengthen protection of online banking data. In: Proceedings of the 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS); 2024 Jun 28–29; Bangalore, India. doi:10.1109/ICITEICS61368.2024.10624984.
68. Mangla C, Rani S, Atiglah HK. Secure data transmission using quantum cryptography in fog computing. Wirel Commun Mob Comput. 2022;2022(2):3426811. doi:10.1155/2022/3426811.
69. Hossain MI, Sumon SA, Hasan HM, Akter F, Badhon MB, Islam MNU. Quantum-edge cloud computing: a future paradigm for IoT applications. arXiv:2405.04824v1. 2024.
70. Chen L, Chen Q, Zhao M, Chen J, Liu S, Zhao Y. DDKA-QKDN: dynamic on-demand key allocation scheme for quantum Internet of Things secured by QKD network. Entropy. 2022;24(2):149. doi:10.3390/e24020149.
71. Tupkary D, Lütkenhaus N. Using Cascade in quantum key distribution. Phys Rev Applied. 2023;20(6):064040. doi:10.1103/PhysRevApplied.20.064040.
72. Hu L, Liu H, Lin Y. Parameter optimization of cascade in quantum key distribution. Optik. 2019;181:156–62. doi:10.1016/j.ijleo.2018.12.023.
73. Brassard G, Salvail L. Secret-key reconciliation by public discussion. In: Advances in Cryptology—EUROCRYPT'93; 1993 May 23–27; Lofthus, Norway. doi:10.1007/3-540-48285-7_35.
74. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. Rev Mod Phys. 2020;92(2):025002. doi:10.1103/RevModPhys.92.025002.
75. Van Assche G. Quantum cryptography and secret-key distillation. Cambridge, UK: Cambridge University Press; 2006.
76. Mehic M, Niemiec M, Siljak H, Voznak M. Error reconciliation in quantum key distribution protocols. In: Ulidowski I, Lanese I, Schultz UP, Ferreira C, editors. Reversible computation: extending horizons of computing. Berlin/Heidelberg, Germany: Springer; 2020. p. 222–36.

77. Martinez-Mateo J, Pacher C, Peev M, Ciurana A, Martin V. Demystifying the information reconciliation protocol cascade. arXiv:1407.3257v2. 2014.
78. Garcia-Escartin JC, Gimeno V, Moyano-Fernández JJ. Quantum collision finding for homomorphic hash functions. arXiv:2108.00100v2. 2021.
79. Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, et al. CRYSTALS-kyber: a CCA-secure module-lattice-based KEM. In: Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P); 2018 Apr 24–26; London, UK. doi:10.1109/EuroSP.2018.00032.
80. Yesina MV, Ostrianska YV, Gorbenko ID. Status report on the third round of the NIST post-quantum cryptography standardization process. Radiotekhnika. 2022;2022(210):75–86. doi:10.30837/rt.2022.3.210.05.
81. Selvakumar S, Ahilan A, Ben Sujitha B, Muthukumaran N. Crystals kyber cryptographic algorithm for efficient IoT D2d communication. Wirel Netw. 2025;31(2):1053–70. doi:10.1007/s11276-024-03790-6.
82. Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. 2022;15(7779):100242. doi:10.1016/j.array.2022.100242.
83. Li S, Chen Y, Chen L, Liao J, Kuang C, Li K, et al. Post-quantum security: opportunities and challenges. Sensors. 2023;23(21):8744. doi:10.3390/s23218744.
84. Prateek K, Ojha NK, Altaf F, Maity S. Quantum secured 6G technology-based applications in Internet of everything. Telecommun Syst. 2023;82(2):315–44. doi:10.1007/s11235-022-00979-y.