2024 33rd International Conference on Computer Communications and Networks (ICCCN) | 979-8-3503-8461-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCCN61486.2024.10637630

Advancing Network Security with Quantum-Safe System Integration

Jianzhou Mao, Guobin Xu, Eric Sakk, and Shuangbao(Paul) Wang
The Department of Computer Science
Morgan State University
Baltimore, USA

***Abstract*—As quantum computing continues to advance, it poses unprecedented risks to traditional factor-based encryption methods, such as RSA, undermining the security of current cryptographic protocols. To address this pivotal security concern, this paper explores a quantum-safe solution that includes two cutting-edge Quantum Key Distribution (QKD) systems, two integrated encryptors, and various networking devices to establish a fortified framework for secure communication. We introduce a system environment setup encompassing the initial configuration, software updates, and management using CM7 software. Next, we delve into the essential configuration and integration steps for deploying a quantum-safe communication network. Moreover, we highlight the strategic implementation of automated script deployment processes, which are instrumental in configuring the QKD system and encryptors. Furthermore, we perform a performance evaluation of the quantum-safe network system, which provides valuable insights into the system's resilience through experimental simulations of beam-splitting attacks. This study provides crucial insights into operational dynamics and showcases the effectiveness of securing communications against cyber threats, underlining the significant potential of quantum-safe solutions in fortifying network security.**

***Index Terms*—Security, Quantum-Safe Networking, Symmetric Key Encryptor, Quantum Key Distribution**

I. Introduction

In the past few years, quantum computing has experienced rapid development as an emerging technology. For example, in 2021, quantum processors just exceeded 100 quantum bits (qubits) [1], and only two years later, IBM raised the number of qubits to 1,121 with the launch of Condor processor [2]. Quantum computing is based on the physics principles of quantum mechanics and utilizes characteristics like quantum superposition of states and quantum entanglement to achieve efficient information processing and computing. Unlike classical computers that use binary bits for computing, quantum computers use quantum bits as information units. The ability of qubits to be in multiple states simultaneously allows quantum computers to perform complex operations with high parallelism. This unique property gives quantum computers the potential to outperform classical computers, enabling them to achieve exponential speedups on specific problems such as prime factorization of large numbers [3], optimization tasks [4], and artificial intelligence applications [5].

As quantum computing evolves, it becomes crucial to reconsider our current information security strategies, particularly in encryption technologies. Traditional encryption algorithms, such as RSA, derive their security from the computational difficulty of specific mathematical problems, deemed nearly insurmountable with today's computing capabilities. However, the advent of quantum computers, bringing parallel computing capabilities and specialized algorithms like Shor's algorithm [6], offers the ability to solve these problems in polynomial time, thereby directly threatening the security foundation of these traditional encryption methods. With the digital economy anticipated to reach a value of $20.8 trillion by 2025 [7], the implications of quantum computing's threat to traditional encryption could lead to profound economic and societal impacts [8], [9].

To address the threats posed by quantum computing, Post-Quantum Cryptography (PQC), and Quantum Key Distribution (QKD) have garnered extensive attention as two principal quantum-safe solutions [10]–[12]. PQC, by developing new encryption algorithms, offers quantum-resistant solutions that are compatible with existing security protocols, thereby ensuring data security in a quantum computing environment. Conversely, QKD, leveraging principles of quantum mechanics such as the no-cloning theorem and the Heisenberg Uncertainty Principle, achieves absolute security in key distribution on a physical level, providing a safeguard for communication that is impervious to any computational power [13]–[15]. Exhibiting its potential as a next-generation encryption technology, QKD introduces a groundbreaking new technique for communication security by distributing encrypted keys through quantum channels, thereby pioneering a novel path for safeguarding the confidentiality and security of communications in the quantum era.

In this paper, we focus on integrating quantum-safe systems with network security infrastructures to address the challenges presented by quantum computing advancements. Specifically, we compare hardware and physics-based implementations with mathematical ones, highlighting QKD and PQC as the principal methodologies for establishing quantum-safe networks. Our quantum-safe network system's structural framework and operational workflow are presented, detailing the essential configuration and integration steps for deploying a secure communication network including the comprehensive installation, initial configuration, and subsequent adjustments of CN4010 encryptors, strongly emphasizing establishing secure connections and enhancing operational efficiency. Moreover, we introduce an automated script deployment process essen-

979-8-3503-8461-1/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

tial for configuring the network and encryptors, laying the foundation for a robust quantum-safe communication network architecture. The paper highlights the system's security efficiency in mitigating potential quantum computing threats, particularly by evaluating the Quantum Bit Error Rate (QBER) as a pivotal indicator of quantum channel security. Through this examination, we strive to offer valuable insights into the realm of quantum-safe communications, demonstrating the capability of such systems to reinforce network security against the backdrop of evolving cyber threats.

The main contributions of this paper are summarized as follows:

- We propose a quantum-safe communication network comprising CN4010 encryptors and the Cerberis3 QKD system.
- We design key configuration and integration steps integrating the quantum-safe networking system.
- We develop an automated deployment script that enhances operational efficiency and significantly reduces the likelihood of human error.
- We evaluate the security performance of the quantum-safe networking system under different eavesdropping intensity.

The remainder of this paper is organized as follows: Section II introduces the common quantum-safe networking methods and our experimental approach involving the quantum-safe networking system, which integrates CN4010 encryptors and the Cerberis 3 System. Section III elaborates on the methodical approach for configuring a quantum key generation and distribution system with the involvement of encryptors. Then, Section IV discusses the implementation of the configuration script within the quantum-safe system. Section V reports experimental results on performance and security. Finally, Section VI presents concluding remarks and future work.

II. Quantum-Safe Networking

A. Hardware and Physics vs. Math-based Implementations

Given the concerns about quantum-safe networking, a growing research and development effort in both industry and academia has been devoted to creating numerous algorithms and applications to address the security challenges posed by quantum computing [16]. Fig. 1 lists commonly adopted quantum-safe networking technologies. These solutions for ensuring robust network security can be categorized into two principal camps: QKD and PQC, representing the hardware and physics-based implementations versus mathematically-based implementations, respectively.

QKD is emerging as a critical solution to security challenges in the quantum era, using quantum mechanics to ensure encryption key secrecy through optical fibers. Prominent protocols such as BB84 [17] and E91 [18] serve as prime examples of QKD, which are fundamentally divided into two main categories based on the quantum properties they utilize: Prepare and Measure protocols and Entanglement-Based protocols. Furthermore, Recent advancements in QKD,

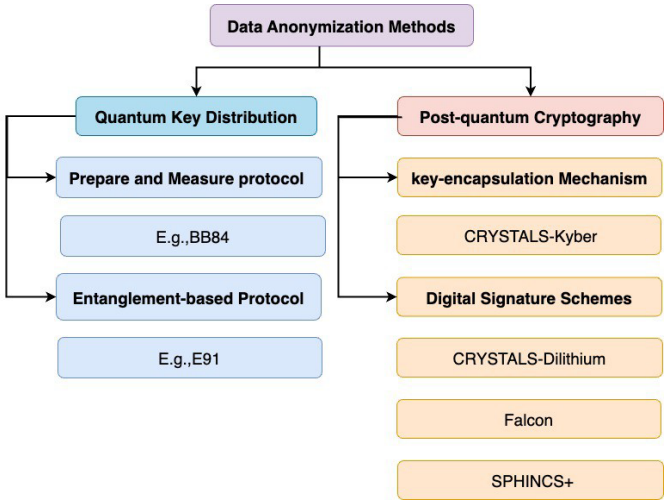

Fig. 1: Quantum-Safe Networking Technologies

such as improved device-independent approaches [19], scalable quantum networks [20], and long-distance secure communication tests [21], highlight its growing impact on quantum-safe applications.

Unlike QKD, which utilizes quantum mechanics to achieve secure communication, Post-quantum cryptography focuses on developing classical cryptographic techniques that can resist the threat of quantum computing. The National Institute of Standards and Technology (NIST) has made significant progress in the field of PQC by introducing a suite of quantum-resistant encryption algorithms in July 2022, including a public-key encryption and key establishment algorithm, and three digital signature algorithms [22]. These algorithms include CRYSTALS-Kyber [23], [24], CRYSTALS-Dilithium, Falcon, and SPHINCS+ [25]–[27], designed to ensure that digital communication is not affected by the future quantum computer, and to ensure compatibility with the existing technology infrastructure. Recently witnessed the development of the optimization of PQC hardware architecture [28], new PQC algorithm performance analysis [29], development based on lattice KEM Advances in high-speed hardware [30], addressing hardware security issues in lattice-based cryptography [31], and evaluating side-channel leakage in PQC implementations [32], These contribute to the global transition to quantum-safe protocols.

B. The Quantum-Safe Networking Systems

Although PQC only requires software upgrades to existing systems for deployment, its long-term security cannot be fully guaranteed because PQC algorithms are based solely on mathematical problems. In contrast, while QKD imposes higher demands on network infrastructure, its security is theoretically guaranteed by the principles of quantum mechanics. To fully leverage and validate the advantages of QKD technology in ensuring communication security, we design and deploy a quantum-safe network system architecture. As shown in Fig.2, this system integrates the Cerberis 3 QKD system with the

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

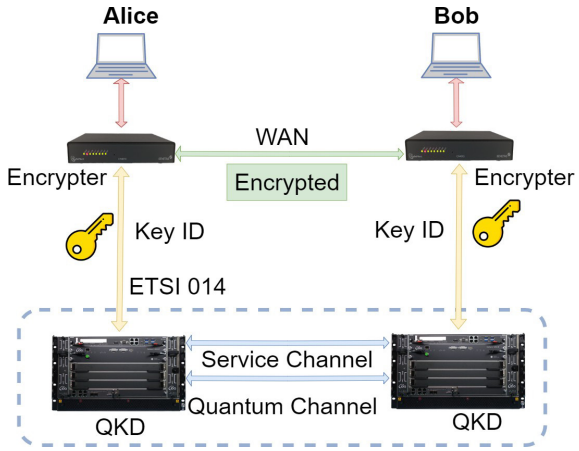

Fig. 2: The Scheme of Quantum-Safe Networking System

CN4010 encryptors, combining QKD technology with the AES 256-bit encryption standard to protect communication between user Alice and user Bob. Within this framework, the Cerberis 3 QKD system is tasked with the secure distribution of keys between two CN4010 encryptors using the ETSI protocol. The encryptors then employ these quantum keys to encrypt and decrypt data, thereby ensuring the confidentiality and integrity of the communication process.

Delving into the communication process, which starts with user Alice, the generated data is directed to a CN4010 encryptor. Then, the data undergoes encryption processing via the AES 256-bit encryption standard, thus safeguarding it throughout the transmission process. Concurrently, the Cerberis QKD system establishes a secure quantum channel between the two CN4010 encryptors to exchange quantum keys. The distribution of these keys, grounded in the principles of quantum physics, ensures the elevated security of the distribution process, with any eavesdropping attempts being promptly identified and thwarted. Subsequently, the encrypted data is securely transmitted to user Bob, where the CN4010 encryptor at Bob's end utilizes the received keys to decrypt the data, restoring it to its original state for use. This process not only secures the data transmission but also showcases the advanced capabilities of the Quantum Security Network System in ensuring communication security.

The Cerberis QKD system, as a pivotal component of the Quantum Security Network System, plays a crucial role in the secure distribution of keys between encryptors. It uses the unique principles of quantum physics, including quantum entanglement and the uncertainty principle, to facilitate key distribution in a manner theoretically impervious to decryption. The QKD system comprises two essential channels: the Quantum Channel and the Service Channel. The Quantum Channel, conducting quantum communication via standard optical fiber SMF-28, is responsible for exchanging qubits at the quantum level to generate secure keys. This process fundamentally leverages quantum physical properties, ensuring absolute communication security. On the other hand, the Service Channel undertakes the responsibilities of system clock synchronization and data post-processing, maintaining temporal consistency among system components, and handling necessary post-data collection processes, thus facilitating subsequent data analysis or storage.

The role of the CN4010 encryptor is equally critical, tasked with the high-strength encryption and decryption of data. Employing the widely acknowledged AES 256-bit encryption standard, the encryptor guarantees the confidentiality and integrity of data transmission. Renowned for its efficiency, versatility, and cost-effectiveness, the encryptor is suitable for organizations of various sizes. The design of the CN4010 leverages state-of-the-art technologies, such as FPGA, to achieve continuous low-latency processing and encryption flexibility, further enhancing the system's security and reliability.

By integrating the Cerberis QKD system and CN4010 encryptors, our Quantum Security Network System offers users a comprehensive end-to-end security solution. Capable of addressing current security challenges and protecting against future quantum computing threats, the design and implementation of this system underscore the significant potential and advantages of quantum communication and modern encryption technologies in securing data.

III. System Configuration and Integration

In this section, we outline the essential configuration and integration steps for deploying a quantum-safe communication network. Beginning with the pre-configuration of the QKD system, we detail the installation, initial setup, and subsequent adjustments of CN4010 encryptors, emphasizing the establishment of secure connections and operational efficiency. Further, we discuss the integration with the QKD system and the adjustment of the operational settings, highlighting the system's resilience by testing QKD parameters. These steps collectively ensure the robustness and security of the quantum-safe network, enabling effective management and operational oversight.

A. Quantum Key Generation and Distribution System Pre-Configuration

In our previous research [33], we outlined a methodical approach for pre-configuring a Cerberis 3 system, focusing on the initial setup steps without involving encryptors. This process begins with establishing SSH connections to Alice's and Bob's QKD and Quantum Node Control (QNC) modules, allowing remote access from any device within the same subnet. Date synchronization is critical, manually or through a Network Time Protocol (NTP) server configured on the quantum management server. This ensures that the QKD and QNC modules are time-aligned for effective quantum channel connections. Authentication is managed by generating and sharing an authentication key between Alice's and Bob's QNC modules and setting up a certificate authority (CA) in QNC. The embedded REST WebAPI is activated for network setup and monitoring, collecting vital parameters like the QBER and facilitating the distribution of this data to third-party systems.

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

Nodes deployment involves installing and configuring QNET on the quantum management server, assigning IP addresses to represent Alice's and Bob's QKD and QNC modules within the same subnet, and deploying these nodes. Key exchanging commences post-deployment, and key exchange rates and QBER are continuously monitored. Finally, a Graphic User Interface (GUI) is available for real-time monitoring and configuration of the QKD and QNC nodes, accessed through a web browser, enhancing the system's operability and oversight.

B. Installation and Initial Configurations

1) Installation of CN4010 Encryptors: The experimental setup begin with the installation of a pair of CN4010 encryptors. These devices, fundamental to our quantum-safe networking system, are methodically installed to establish a foundational network for quantum-safe communications.

2) Initial Configuration via Serial/Console Interface: Following installation, initial configuration is essential. This process involves interfacing with the CN4010 encryptors via a serial/console connection. This step is critical for assigning IP addresses to the devices and activating them for local operations. The methodical approach ensures secure and effective communication between devices in the subsequent stages.

3) Software Updates: The CN4010 encryptors are upgraded to the latest software release to optimize performance. This update ensures that the devices have the most advanced security and operational features. The CM7 management software, a pivotal system component, is also installed on a local Windows PC. This software plays a key role in managing and configuring the encryptors.

C. Configuration Using CM7

1) Certification of Trust Between Encryptors: A vital step in the configuration process involves certifying trust between the two encryptors. This is achieved by creating a root Certificate Authority *rootCA* and associated public/private key pairs. The establishment of a *rootCA* is a fundamental security practice in networking, ensuring secure and authenticated communications between the encryptors.

2) Integration with the QKD System: Integration with the QKD system is another key focus. Trust between the encryptors and the QKD system is certified by loading a *rootCA* that is previously generated in a controlled lab environment. This process also involves the generation of new public/private key pairs for each encryptor, further enhancing the security measures.

D. Operational Settings and Parameters

1) Activation of Line Mode and eQKD Mode: The operational setup of the quantum-safe networking system involves activating the *Line Mode* on the CN4010 encryptors. This mode is pivotal for establishing a point-to-point topology and QKD process.

Subsequently, the *eQKD mode* is enabled, marking a significant step towards leveraging quantum mechanics for secure key distribution. This mode is instrumental in integrating conventional encryption techniques with QKD, ensuring a robust quantum-safe environment.

2) Global Mode and Key Request Interval Settings: To enhance the system's operational efficiency, the encryptors are set to *Global Mode: Encrypt All*. This setting ensures comprehensive encryption coverage for all forms of data traversing the network, including voice, video, and other data communications. Additionally, the key request interval is meticulously set to one minute. This interval determines the frequency at which the CN4010 encryptors request new quantum keys, striking a balance between security needs and system performance.

3) Tunnel Mode Configuration: The final step of the operational setup involves configuring the tunnel mode to *Encrypt QKD*. This configuration is central to the quantum-safe networking system, as it dictates how the encryptors handle the data encryption process in conjunction with the QKD system. By setting the tunnel mode to *Encrypt QKD*, the system ensures that all data is encrypted using quantum-safe keys, significantly enhancing the security against potential quantum computing threats.

E. Integration and Testing of QKD Parameters

A critical integration involves configuring the QKD parameters to align seamlessly with the IDQ QKD system. This configuration is crucial for establishing a secure quantum communication channel. Specific settings are adjusted, including Key Interface options and Peer Encryptor IP addresses, which are vital for creating a reliable quantum link between the components of our quantum-safe networking system.

In addition to these configurations, an important strategic decision is made to set the failure mode of the system to use Classical Keys (CNET). This setting ensures that in case of any failure in the QKD process, the system defaults to using classical cryptographic keys, thereby maintaining continuous encryption and data security in transit. This fail-safe mechanism is essential for maintaining operational integrity and security, particularly when QKD is interrupted or compromised.

IV. Automated Script Deployment for Quantum-safe Networking System

In this section, we delve into the automated script deployment process critical for configuring the QKD and the encryptor, laying the foundation for a secure quantum-safe communication network architecture. These automated scripts are meticulously crafted to facilitate the seamless and efficient setup of quantum network components, embodying a methodical approach to establishing a secure, authenticated quantum network management environment. By using automation, we ensure the robust orchestration of network components, making the configuration process within a quantum-safe framework. This emphasis on automated deployment enhances operational efficiency and significantly reduces the potential for human error, ensuring a high degree of reliability and security in the network setup.

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

Script 1: Group Management

```
qnet delete group Group1
qnet create group Group1 --desc TestLab
qnet list group
```

A. Authentication

The initial step in configuring a quantum-safe networking system involves authenticating the QNET user to the Quantum Management System (QMS). We achieve the authentication through the command *qnet config qnetwebapi*, which is used to set up the QNET web API. QNET is a command-line interface that offers a comprehensive set of commands to manage QKD network configuration. The parameters include the URL of the QMS server, which is typically hosted locally, and the credentials for the administrative user *-user Admin -pwd Admin*. This step is crucial as it establishes a secure connection to the QMS, enabling further configuration and management of the QKD system. It ensures that only authorized personnel can alter the system's settings, thereby maintaining the integrity and security of the entire setup.

B. Group Management

Next, the script deals with managing groups within the QNET system. Initially, it checks for the existence of a group named *Group1*. If this group already exists, the command *qnet delete group Group1* removes it, ensuring a fresh setup. Subsequently, a new group named *Group1* is created using *qnet create group Group1 –desc TestLab*. The *–desc* flag is used to provide a description (*TestLab*) for the group, which can be helpful for identification and documentation purposes. Finally, the command *qnet list group* is executed to list all groups within the system. This step is for verifying the new group's successful creation and maintaining a clear organizational structure within the QNET system, which is pivotal for managing multiple nodes and links in a complex QKD network.

C. Node Configuration

Following group management, the script configures individual nodes within the newly created group. This step is crucial for establishing the network's basic structure. Nodes *QNCA* and *QNCB* are created with specific IP addresses, aligning with their respective management port IPs. The *–node-uid* parameter assigns a unique identifier to each node, enhancing the system's organization and security. After creating these nodes, the *qnet list node* command is executed to display all configured nodes. This verification ensures that the system correctly sets up and recognizes each node, forming the foundation for subsequent secure communications.

D. Node Link Configuration

Moving forward, the script addresses establishing node links, an essential aspect of network configuration. A link, denoted as *KMSLINK*, is created between nodes *QNCA* and

Script 2: Node Configuration

```
qnet create node QNCA Group1 -ip QNCAIP --node
    -uid a429c85a7af748edbf19f917d45d9317
qnet create node QNCB Group1 -ip QNCBIP --node
    -uid 2bc8fe7327294ef79fde23b744e3467b
qnet list node
```

Script 3: Node Link Configuration

```
qnet create node-link --algorithm BlockCipher
    KMSLINK QNCA QNCB
qnet list node-link
```

QNCB using the BlockCipher algorithm. This algorithm choice determines the method of secure data transmission between the nodes. Creating this node-link is a significant step in the configuration process, as it facilitates secure communications paths within the network. The *qnet list node-link command*, executed afterward, confirms the node-link's successful establishment. It ensures that the nodes are correctly interconnected, enabling efficient and secure data exchange, which is fundamental to operating a QKD network.

E. Provider Configuration

This script segment is dedicated to setting up QKD providers within the network, which are integral to the QKD system. Providers *QKDA* and *QKDB* are associated with nodes *QNCA* and *QNCB*, respectively. Each provider is assigned a specific IP address corresponding to the QKD module port. The designation of *Cerberis3* indicates the use of the Cerberis3 system, known for its robustness in quantum-safe communications. After the providers are established, the command qnet list provider is executed to list all providers, a critical step for verifying that the QKD providers are correctly integrated into the network. This configuration ensures that each node in the network is equipped with a reliable QKD mechanism, a cornerstone for secure quantum communications.

F. Provider-Link Configuration

Following the provider setup, the script addresses the creation of a link between these QKD providers. This link, labeled *QKDLINK*, connects providers *QKDA* and *QKDB*. A notable feature of this link is the specification of a key request interval (*–key-req-interval 80*), which defines the frequency at which quantum keys are requested, balancing security needs with system performance. The establishment of this provider-link facilitates the dynamic distribution of quantum keys between

Script 4: Provider Configuration

```
qnet create provider QKDA QNCA Cerberis3 -ip
    QKDAIP
qnet create provider QKDB QNCB Cerberis3 -ip
    QKDBIP
qnet list provider
```

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

Script 5: Provider-Link Configuration

```
qnet create provider-link QKDLINK QKDA QKDB --
    key-req-interval 80
qnet list provider-link
```

Script 6: Consumer Configuration

```
qnet create consumer etsi014  EncryptorAIP
    QNCA --subject-dn "C=AU, ST=Victoria, L=
    Melbourne, O=Org, OU=Security, CN=
    CN40100912B4" --key-type QKEY --pport 443
qnet create consumer etsi014  EncryptorBIP
    QNCB --subject-dn "C=AU, ST=Victoria, L=
    Melbourne, O=Org, OU=Security, CN=
    CN401009132C" --key-type QKEY --pport 443
qnet list consumerode
```

different parts of the network. To confirm the successful creation of this link, the *qnet list provider-link* command is utilized, listing all provider-links in the system. This step ensures that a secure and efficient quantum key exchange mechanism is in place.

G. Consumer Configuration

Next, the script establishes consumers at specific IP addresses associated with the network's encryptors. The utilization of *etsi014* in the command signifies the incorporation of the ETSI GS QKD 014 protocol [34]. This protocol standardizes the secure cryptographic key delivery method, employing a REST API, HTTPS protocols, and JSON data encoding. These measures ensure a high level of security and interoperability in key distributions. The *–subject-dn* parameter assigns a distinguished name to each consumer, providing essential identification details such as country, state, locality, organization, and organizational unit. The configuration of the key type as *QKEY* and the assignment of port numbers are tailored to align with ETSI's stringent security requirements. This setup ensures that each consumer operates under a uniform and secure standard, maintaining the integrity of the QKD process.

H. Consumer-Link Configuration

The Consumer-Link Configuration in the script establishes *EncryptorLink*, directly linking the consumers, which in this setup are the encryptors. This critical linkage is facilitated through the *qnet create consumer-link* command, forming a bi-directional communication channel. This bi-directional aspect is not only significant for the two-way exchange of quantum keys, thereby enhancing the network's overall flexibility and efficiency, but it also plays a pivotal role in maintaining the security and integrity of data. The configuration's emphasis on a 256-bit default key size strategically aligns robust cryptographic security with the system's operational efficiency, ensuring a balanced approach to quantum-safe communications.

Script 7: Consumer-Link Configuration

```
qnet create consumer-link EncryptorLink
    EncryptorAIP  EncryptorBIP --mode
    BiDirectional --default-key-size 256
qnet list consumerlink
```

Script 8: Path Configuration

```
qnet create path EncryptorAIP EncryptorBIP -
    mode Automatic
qnet list path
```

I. Path Configuration

In our script, the *qnet create path* command establishes an automatic path between the encryptors within the network. This automatic setting is crucial as it enables the path to adapt dynamically to network conditions, optimizing the distribution of quantum keys for enhanced security and system efficiency. The subsequent *qnet list path* command serves as an essential verification step, listing all the established paths to ensure they are correctly configured and operational, thereby solidifying the network's QKD framework.

J. Certificate Upload

Uploading digital certificates to the QMS is used to verify device identities and safeguard the confidentiality and integrity of data exchanges. Initially, the script uploads a CA certificate, named *ChrisCA.pem*, to the QMS, marking the CA as a trusted entity responsible for validating the digital certificates of network devices and forming a trust chain, thereby enabling network devices to authenticate each other's identities and facilitating a smoother authentication process. Furthermore, the process involves uploading server certificates *QKDServer.pem* and their respective private keys *QKDServer_pkey.pem* to authenticate servers and secure communication, which is achieved by enabling the decryption of information encrypted with the server's public key. Following the successful integration of these certificates into the system, as confirmed by executing a command to list all certificates in the QMS, the final step involves executing the group configuration deployment command, activating the new certificates, and applying the changes across the network. This transition marks a significant shift to the operational phase, where the certificates begin to play a critical role in safeguarding network communications, underscoring the foundational importance of digital certificates in establishing a robust framework for secure quantum communications by setting up a trust infrastructure and validating server legitimacy within the quantum-safe network.

K. Certificate Assignment and Deployment

In the last phase of configuring the quantum-safe networking system, the script precisely focuses on updating the consumer devices, identified as EncryptorA and EncryptorB, with the server's digital certificates and corresponding private keys.

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

Script 9: Certificate Management and Deployment

```
qnet add ca-cert consumer --ca-file  ./ChrisCA
    .pem
qnet add cert ./QKDServer.pem ./QKDServer_pkey
    .pem
qnet list cert
qnet deploy group Group1
```

Script 10: Certificate Management and Deployment

```
qnet update consumer etsi014 EncryptorAIP --
    cert-file QKDServer.pem --key-file
    QKDServer_pkey.pem
qnet update consumer etsi014 EncryptorBIP --
    cert-file QKDServer.pem --key-file
    QKDServer_pkey.pem
qnet deploy group Group1
```

This operation, executed through the *qnet update consumer* commands, assigns the *QKDServer.pem* certificate and its associated *QKDServer_pkey.pem* private key to both encryptor devices, equipping them with the necessary credentials to authenticate the server and establish a secure communication channel. By representing the IP addresses of EncryptorA and EncryptorB as *EncryptorAIP* and *EncryptorBIP*, the script ensures that each encryptor device is accurately configured with the server's identity verification tools, enhancing the network's security posture. The final execution of qnet *deploy group Group1* signifies deploying these configurations across the network group, effectively activating the updated security settings. This meticulous configuration process underscores the essential role of digital certificate management and deployment in reinforcing the network's defense mechanisms against potential security threats, thereby facilitating a robust framework for quantum-safe communications.

In a nutshell, commencing with the authentication of QNET users by the QMS, the script establishes a foundational security baseline for network operations. It guides the systematic creation, modification, and enumeration of network groups, nodes, and connections, ensuring an accurate topological structure and optimizing QKD pathways. The subsequent integration of quantum key providers and consumers is detailed, highlighting the establishment of provider links and consumer connections, which are pivotal for the operational integrity of quantum-safe communications. Last, the script shows the process of managing cryptographic credentials, involving uploading and allocating CA certificates, server certificates, and private keys. These procedures are crucial for safeguarding the network and facilitating a secure environment conducive to quantum-safe communication through authenticating and encrypting mechanisms. Our script encapsulates the quintessence of quantum network setup, illustrating the intricate interplay between various network entities and the pivotal role of script-driven automation in deploying resilient quantum-safe network infrastructures.

V. Performance Evaluation

In this section, we evaluate the performance of the quantum-safe network system, which integrates CN4010 encryptors and the Cerberis 3 system elaborated in Section II-B, under attack conditions. This evaluation aims to verify that the communications between users of this system are protected by a quantum distribution mechanism, thereby leveraging quantum mechanics to achieve quantum-safe communication. More specifically, we concentrate on the fluctuation of QBER as it is a crucial measure for assessing the security of quantum channels.

A. Experiment Setup

In this study, we evaluate the performance of quantum-safe network systems under beam-splitting attacks, focusing on their ability to detect and defend against potential eavesdropping threats. Beam-splitting attacks represent an advanced eavesdropping strategy, enabling attackers to extract photons from the transmission path to access critical information from encrypted communications, posing a direct threat to the security of QKD systems. Within the QKD framework, information is conveyed by the quantum states of photons, such as polarization states, which facilitate the transfer of crucial information from Alice to Bob.

The attacker, herein referred to as Eve, clandestinely installs a beam splitter within the transmission path, orchestrating an attack that bifurcates the photon stream, thereby allowing a portion of the photons to continue on their original path towards Bob while diverting the remaining photons to Eve's surveillance apparatus. Eve aims to intercept and analyze these photons covertly, without alerting Alice and Bob, to glean key information. This necessitates that Eve executes the attack with the utmost caution to prevent a significant uptick in the QBER, as such an increase would signal to Alice and Bob the presence of a security compromise.

To accurately simulate this intricate attack scenario, a specially designed eavesdropping device equipped with a dial control mechanism capable of emulating varying intensities of beam-splitting attacks was employed. By adjusting its settings, this device can mimic eavesdropping behaviors ranging from mild to extreme, thereby enabling a scientific assessment of the QKD system's security performance against beam-splitting attacks of differing intensities. The device's core functionality lies in its ability to temporarily remove a certain proportion of photons from the optical fiber and subsequently reinsert these photons back into the fiber after a delay. This process precisely simulates the actions of an eavesdropper attempting to purloin photons from the cable, subject them to some form of analysis or manipulation, and then surreptitiously reintroduce these photons back into the fiber.

Specifically, various intensity levels (0, 20, 40, 60, and 80) were established for experimental testing. These levels represent the intensity of eavesdropping, ranging from no eavesdropping (0) to extreme eavesdropping (80). Through this methodology, we scientifically evaluate the QKD system's se-

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

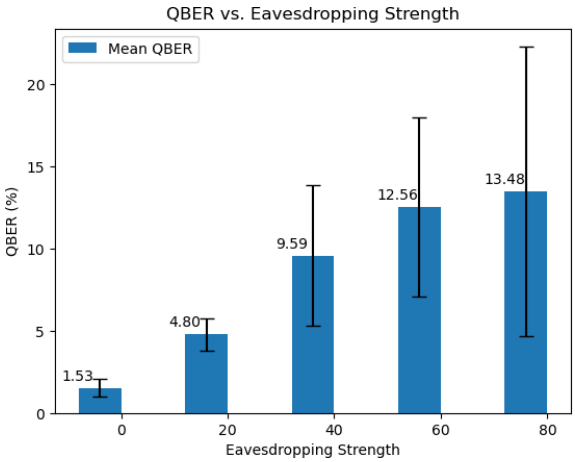

Fig. 3: Impact on QBER under Various Scenarios

curity efficacy against beam-splitting attacks across a spectrum of intensities.

B. Quantum Bit Error Rate (QBER)

As illustrated in Fig.3, our analysis of QBER under varying intensities of eavesdropping reveals a significant uptrend in both the average value and volatility of QBER as eavesdropping intensity escalates. In a scenario devoid of eavesdropping (intensity at 0), the average QBER stands at a mere 1.5% with a standard deviation of 0.54%, reflecting the system's efficiency and stability in an undisturbed state, ensuring accurate quantum information transmission. However, as the eavesdropping intensity increases to 20, the average QBER rises to 4.8%, and the standard deviation expands to 0.96%, indicating that even low-intensity eavesdropping significantly impacts system performance. Further elevation of eavesdropping intensity to 40 leads to a sharp increase in the average QBER to 9.6%, with the standard deviation widening to 4.26%. This data clearly indicates that medium-intensity eavesdropping seriously threatens the security of quantum communication systems.

When the eavesdropping intensity reached 60 and further increased to 80, an interesting phenomenon emerged: the average QBER only increased slightly from 12.6% to 13.48%. However, the rapid rise in volatility, with the standard deviation increasing to 5.44% and 8.8%, respectively. The slight difference in average QBER between 60 and 80 eavesdropping intensities, contrasted with a sharp increase in volatility, suggests a threshold effect. This effect indicates that the system's vulnerability to error saturation begins to level off, implying that quantum communication systems may be approaching the limit of error rates under extreme eavesdropping conditions. However, a significant increase in volatility means that while the average error rate may not increase dramatically after a certain point, the consistency and predictability of system performance decline dramatically. This increased volatility indicate that, at higher eavesdropping intensities, quantum communication systems experience a more comprehensive range of quantum state perturbations, resulting in more pronounced fluctuations in QBER.

This series of observations reveals the direct correlation between the increase of QBER and the increase of eavesdropping intensity and demonstrates the specific impact of eavesdropping behavior on system performance. With the increase of eavesdropping intensity, the average and volatility of QBER increase, directly reflecting the overall increase of the system error rate. In other words, these findings highlight the effectiveness of QKD systems against eavesdropping at all levels. Through the detailed analysis of QBER, we can not only accurately evaluate the system's performance in the face of a specific eavesdropping environment but also gain a deep understanding of the system's high sensitivity to eavesdropping activities. These results further confirm the ability of quantum communication networks to effectively detect and resist sophisticated eavesdropping techniques using fundamental principles of quantum mechanics, such as the uncertainty principle and quantum entanglement. Through these principles, the quantum communication system can ensure information security even in the face of future technological advances and potential advanced attack means, showing the unique advantages and potential of quantum technology in ensuring long-term communication security.

VI. Conclusion

In this study, we investigated the establishment and practical application of a quantum-safe network system, emphasizing the seamless integration of the encryptor with commercial QKD systems. Through the exploration of the setup, configuration, and experimental validation, we demonstrated a comprehensive approach to implementing quantum security solutions in networked environments.

At first, we explored the basics of quantum-safe methods, comparing hardware and physics-based implementations with mathematically based ones. We then presented the architecture and overall workflow of our quantum-safe network system. Subsequently, we detailed the key configuration and integration steps required to deploy a quantum-safe communication network, focusing on the integration of the Cerberis 3 QKD system and the CN4010 encryptor. We explored the automated script deployment process, which is crucial for configuring quantum-safe network systems, laying the foundation for building a secure quantum communication network architecture. In the performance evaluation section, we verified the system's security by simulating beam-splitting attacks and focusing on the fluctuation of QBER as a key metric. The results showed that the system can effectively detect and resist potential security threats, which proves the effectiveness of quantum-safe communication through the principles of quantum mechanics.

This study lays out a solid foundation for the integration of QKD in quantum-safe network systems. As a future direction, research could focus on the integration of quantum-safe systems into large-scale and diverse network environments,

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.

addressing challenges such as the impact of environmental noise on QBER, the stability of long-distance transmission, and other related issues. As quantum hardware continues to evolve and improve, we anticipate that QKD can be gradually extended to more complex network environments and tasks, unlocking new possibilities for quantum-safe communication technologies.

VII. Acknowledgment

This research is funded by grants from the National Science Foundation NSF 2000135, 2230462, and 2329053.

References

[1] Jerry Chow, Oliver Dial, and Jay Gambetta. Ibm quantum breaks the 100-qubit processor barrier. *IBM Research Blog*, 2, 2021.

[2] Jay Gambetta. The hardware and software for the era of quantum utility is here. https://www.ibm.com/quantum/blog/quantum-roadmap-2033, Dec 2023.

[3] Shuxian Jiang, Keith A Britt, Alexander J McCaskey, Travis S Humble, and Sabre Kais. Quantum annealing for prime factorization. *Scientific reports*, 8(1):17667, 2018.

[4] Akshay Ajagekar and Fengqi You. Quantum computing for energy systems optimization: Challenges and opportunities. *Energy*, 179:76–89, 2019.

[5] M. Cerezo, A. Arrasmith, R. Babbush, S. Benjamin, Suguru Endo, K. Fujii, J. McClean, K. Mitarai, Xiao Yuan, L. Cincio, and Patrick J. Coles. Variational quantum algorithms. *Nature Reviews Physics*, 3:625 – 644, 2020.

[6] Shaheed Nehal and Mubasheer Farhan. Shor's algorithm: A threat to rsa cryptosystem. 2021.

[7] Cebr. The digital trust index, 2022.

[8] Dr. Brijraj Singh Solanki and Apurva Saini. Quantum cryptography: An overview. *International Journal of Advanced Research in Computer Science and Technology*, 2023.

[9] Marco Fiore, Federico Carrozzino, Marina Mongiello, Gaetano Volpe, and A. M. Mangini. Modular blockchain architecture for coexistence of quantum-safe and quantum-broken blocks. In *IEEE Conference on Decision and Control (CoDIT)*, 2023.

[10] Randy Kuang, Dafu Lou, Alex He, and Alexandre Conlon. Aes-qpp: A quantum-safe lightweight cryptography approach. *Proceedings of the IEEE International Conference on Cyber Security and Cloud Computing*, 2021.

[11] Zainab Iftikhar, Malayka Iftikhar, and M. A. Shah. Wots: A quantum-safe hash-based digital signature for cloud computing. In *IEEE International Conference on Advanced Computing*, 2021.

[12] Guobin Xu, Jianzhou Mao, Eric Sakk, and S. Wang. Evaluating quantum-safe cryptography for network security. In *IEEE Conference on Computer and Communications Security*, 2023.

[13] Nicolas Gisin, Gre´goire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002.

[14] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lu¨tkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[15] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2, 2016.

[16] Amoldeep Singh, Kapal Dev, Harun Siljak, Hem Dutt Joshi, and Maurizio Magarini. Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, 23(4):2218–2247, 2021.

[17] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[18] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[19] Rahul Jain and Srijita Kundu. A direct product theorem for quantum communication complexity with applications to device-independent qkd. *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1285–1295, 2022.

[20] Teng-Yun Chen, Xiao Jiang, Shi-Biao Tang, Lei Zhou, Xiao Yuan, Hongyi Zhou, Jian Wang, Yang Liu, Luo-Kan Chen, Weiyue Liu, Hongfei Zhang, Ke Cui, Hao Liang, Xiao-Gang Li, Yingqiu Mao, Liu-Jun Wang, Si-Bo Feng, Qing Chen, Qiang Zhang, Li Li, Nai-Le Liu, Cheng-Zhi Peng, Xiongfeng Ma, Yong Zhao, and Jian-Wei Pan. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information*, 7:1–6, 2021.

[21] Hui Liu, C. Jiang, Haonan Zhu, Mi Zou, Zong-Wen Yu, Xiao-Long Hu, Hai Xu, Shi-Zhao Ma, Zhi-Yong Han, Jiu-Peng Chen, Yunqi Dai, Shi-Biao Tang, Weijun Zhang, Hao Li, L. You, Zhen Wang, Yong Hua, Hongbo Hu, Hongbo Zhang, Fei Zhou, Qiang Zhang, Xiang-Bin Wang, Teng-Yun Chen, and Jian-Wei Pan. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Physical review letters*, 126 25:250502, 2021.

[22] National Institute of Standards and Technology (NIST). Nist announces first four quantum-resistant cryptographic algorithms. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[23] Joppe Bos, Le´o Ducas, Eike Kiltz, Tancre`de Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle´. Crystals-kyber: a cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018.

[24] Roberto Avanzi, Joppe Bos, Le´o Ducas, Eike Kiltz, Tancre`de Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle´. Crystals-kyber algorithm specifications and supporting documentation. *NIST PQC Round*, 2(4):1–43, 2017.

[25] Le´o Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehle´. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018.

[26] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over ntru. *Submission to the NIST's post-quantum cryptography standardization process*, 36(5), 2018.

[27] Daniel J Bernstein, Andreas Hu¨lsing, Stefan Ko¨lbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 2129–2146, 2019.

[28] Ziying Ni, A Khalid, and M O'Neill. High performance fpga-based post quantum cryptography implementations. In *2022 32nd International Conference on Field-Programmable Logic and Applications (FPL)*, pages 456–457. IEEE, 2022.

[29] Filip Lauterbach, Patrik Burdiak, Filip Richter, and M Vozna´k. Performance analysis of post-quantum algorithms. In *2021 29th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE, 2021.

[30] V Dang, Kamyar Mohajerani, and K Gaj. High-speed hardware architectures and fpga benchmarking of crystals-kyber, ntru, and saber. *IEEE Transactions on Computers*, 72:306–320, 2023.

[31] Davide Bellizia et al. Post-quantum cryptography: Challenges and opportunities for robust and secure hw design. In *2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6. IEEE, 2021.

[32] Jungmin Park et al. Pqc-sep: Power side-channel evaluation platform for post-quantum cryptography algorithms. *IACR Cryptol. ePrint Arch.*, 2022:527, 2022.

[33] Jianzhou Mao, Guobin Xu, Eric Sakk, and Shuangbao Paul Wang. Quantum Key Distribution and Security Studies. 4 2023.

[34] ETSI. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. Technical Report ETSI GS QKD 014 V1.1.1, European Telecommunications Standards Institute, May 2019.

Authorized licensed use limited to: Morgan State University. Downloaded on September 08,2025 at 02:08:57 UTC from IEEE Xplore. Restrictions apply.