Quantum Networks and Cyber Security. A Simulation Case Study for Multi-Hop QKD Networks

Sorin SOVIANY, Cristina-Gabriela GHEORGHE, Maria GHEORGHE-MOISII
National Institute for Research and Development in Informatics – ICI Bucharest
sorin.soviany@ici.ro, cristina.gheorghe@ici.ro, maria.moisii@ici.ro

Abstract: The paper addresses the Quantum Networks (QN) performance with Quantum Key Distribution (QKD) protocols. The focus is on networks with multi-hop paths (multiple QKD links with intermediate nodes). QKD emerged as a promising technology to ensure unconditioned communications security by exploiting the Quantum Computing (QC) and quantum principles. While the Point-to-Point (P2P) QKD links are well understood for several QKD protocols, the challenges concern the development of QN with multiple intermediate nodes and links. The deployment of quantum-secure communication systems over very large distances requires multi-hop QN. This paper presents a simulation-based case study for multi-hop QKD networks, focusing on the performance evaluation and the Cyber Security implications. The framework could be used to evaluate end-to-end key generation rates, latency, and resilience under various network topologies and link conditions. This methodology will allow to properly investigate how the network-level security policies can be integrated with QKD protocols to detect and mitigate both passive and active attacks. One could find out the trade-offs between hop count, security margins, and throughput, providing insights into the design of robust and scalable quantum-secure communication infrastructures. This study will support the research about the integration of the QKD with the classical network management, conventional security mechanisms and advanced Cyber defense strategies.

Keywords: Quantum Networks, multi-hop, Quantum Key Distribution, Cyber Security.

INTRODUCTION

The fast advancements in Quantum Computing (QC) generate both opportunities and threats to the communications infrastructures. There are major concerns about the vulnerability of the conventional crypto-systems, especially those using public-key algorithms such as Rivest-Shamir-Adleman and Elliptic Curve Cryptography, to attacks based on quantum computers. These attacks look to break the conventional cryptography and could be executed by running algorithms like Shor's with high speed provided by the advances in the quantum technology. This provides the reason for the actual R&D efforts towards the design of

https://doi.org/10.54851/v7i2y202507

quantum-robust solutions including Quantum Key Distribution (QKD).

QKD is a promising technology that emerged to ensure absolute unconditioned security by exploiting the QC and quantum principles (entanglement, superposition). The quantum states properties allow 2 parties to securely establish and distribute a secret key. This key should be robust against any eavesdropping or any decryption attempt that could be performed either by computational techniques or by using quantum computers. The problem of building resilient Cyber Security systems in respect to attacks carried out by conventional and quantum computers is the subject of Post-Quantum Cryptography (PQC) (NIST, 2025).

The Point-to-Point (P2P) QKD links are well understood for several QKD protocols, such as BB84 (Bennett, Brassard-1984), E91 (Eckert-1991), B92 (Bennett-1992), BBM92 (Bennett, Brassard, Mermin-1992). QKD has already successful uses-cases with P2P links over fiber and Free-Space Optics channels. The practical adoption of QKD to secure the large-scale communications requires an efficient transition from P2P to multi-hop QKD networks. The extension of the QKD networks beyond the single-hop connections is constrained by physical limitations such as the photon loss, decoherence and channel noise. These constraints reduce the maximum distance for the secured keys exchange. The multi-hop QKD networks should use trusted nodes or entanglement swapping to ensure quantum-secured communications over long distances. An important challenge for the Quantum Networks (QN) evolution towards the future quantum Internet is the integration of multiple nodes and links but incorporating quantum repeaters. The deployment of the quantum-secure communication systems over very large distances requires multi-hop QN and several QKD links between the intermediate nodes to overcome the distance constraints. The multi-hop QKD networks use intermediate nodes and QKD links to enable the extension of the quantum communications. This extension will bring additional challenges in terms of the network design, key management, trust models, multiple Cyber Security risks assessment and the integration with the legacy network-level Cyber Security mechanisms.

The QN (QKD networks) deployment is also challenged by the Cyber Security risks. The quantum layer of the network stack implements the QKD functionalities but the higher layers are still vulnerable to conventional attacks like Denial-of-Service (DoS), traffic analysis, node compromising. On the other hand, the QKD protocols can be attacked using different techniques able to exploit the hardware imperfections or operational vulnerabilities. The specific attacks include (Gaur, 2020) Photon Number Splitting (PNS), Intercept-Resend (IR) (Marquardt, 2023), Faked-state attack (Sabani, 2022), Trojan horse (Brazaola-Vicario, 2024), but also Man-in-the-Middle (Kuhn, 2003), electromagnetic side-channel attack (Pantoja, 2024). The relationships between the quantum systems vulnerabilities and the conventional Cyber attacks features should be addressed to design reliable quantum communications systems.

The paper addresses the QN performance with QKD protocols. The focus is on the networks with multi-hop paths (multiple QKD links with intermediate nodes). The simulation-based case study for multi-hop QKD networks is focused on the performance evaluation and Cyber Security implications. The framework could be used to evaluate end-to-end key generation rates, latency, and resilience under various network topologies and link conditions. Also it should allow to investigate how the network-level security policies can be integrated with QKD protocols to detect and mitigate passive and active attacks. One could find out the trade-offs between hop count, security margins, and throughput, providing insights into the design of the robust and scalable quantum-secure communication infrastructures. This study will support the research about the integration of QKD with the classical network management, conventional security mechanisms and advanced Cyber defense strategies. The remainder of the paper contains: Section 2 - related works; Section 3- a case study for a simulated multi-hop QKD network; Section 4 that concludes this paper.

RELATED WORKS AND CURRENT DEVELOPMENTS IN THE MULTI-HOP QKD NETWORKS

A QN (QKD network) is based on an infrastructure with several quantum links connecting multiple nodes that can be used to secure the cryptographic keys exchange with key agreement, using QKD protocols (Alléaume, 2014), (Soviany et al., 2024). QN is a collection of nodes connected through a network such as they can transmit quantum states between them, also enabling the entanglement sharing between the remote nodes (QuNetSim Project, 2019). The recent developments in QN/QKD systems use different categories of QKD networks, depending on the topology, deployment architecture, key distribution methods and the underlaying technology for the quantum information transfer (Figure 1):

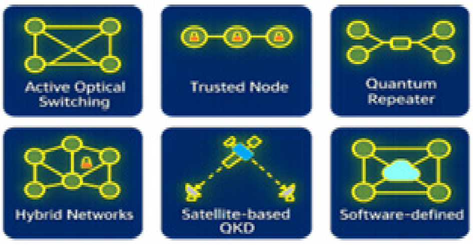

Figure 1. *Types of QKD networks*

- **Active Optical Switching Networks**, with dynamic optical signal switching to establish direct P2P links between the selected nodes. Switching occurs at the Physical layer, enabling rapid pairing of nodes for the QKD protocol initiation. This model ensures a high level of security since no intermediate nodes are involved. The performance is negatively affected by switch-induced losses, and the maximum inter-node distance remains limited (Tsai et al., 2021);
- **Trusted Node Networks**, in which the keys are distributed over short segments between adjacent nodes using local quantum links. The inter-segment transmission is performed classically through intermediate, trusted nodes. This approach is scalable and allows long-distance QKD communication, supporting the integration of heterogeneous QKD technologies. The security depends on the integrity of each intermediate node (Tsai et al., 2021);
- **Quantum Repeater Networks,** relying on quantum repeaters that enable the communication extension without requiring trust in the intermediate nodes. They operate through quantum entanglement and processes such as quantum teleportation and entanglement swapping. Theoretically, this architecture provides the highest level of security and enables virtually unlimited communication distances. It remains in an early research stage and demands advanced technologies such as quantum memory, resulting in high costs and technical complexity (Tsai et al., 2021);
- **Hybrid QKD Networks**, that combine features from various architectures — including direct channels, trusted nodes, and satellite links — to balance flexibility, security, and scalability. The hybrid networks can be dynamically optimized via software-defined networking (SDN), allowing programmable control of the routes and adaptable topologies (e.g. star, mesh, ring). This versatility increases the management and key distribution complexity, and requires standardization for the interoperability across different QKD technologies (Tessinari et al., 2023);
- **Satellite-Based QKD Networks**, in which the quantum signals are transmitted from low-Earth orbit satellites to ground stations, enabling the intercontinental key exchange over thousands of kilometers, unconstrained by fiber optics. While this allows global communication without terrestrial infrastructure, it is sensitive to weather conditions and satellite-ground synchronization. High deployment and operational costs are involved due to the need for highly performant optical and tracking equipment (Government of Canada, 2025);

- **Software-Defined QKD Networks (SDN-QKD):** An emerging trend involves the integration of QKD networks within SDN architectures, allowing programmable control over both quantum and classical channels. This enables the dynamic route allocation, traffic prioritization, and automatic interconnection of heterogeneous nodes. This direction aims to reduce the operational complexity of hybrid QKD networks and enhances the compatibility with the existing IP-based infrastructures (Nosouhi et al., 2024).

(Cao et al., 2022) provide an overview of the QKD networks evolution towards the quantum internet. The authors reviewed numerous implementations and described the general 3-layered architecture (infrastructure, control/management, and application layers) with its components. They present techniques belonging to the Physical and Networking layers, ongoing standardization efforts, possible scenarios, and research directions for building the future quantum internet.

An introduction to QN control is made in (Valls et al., 2024), explaining basic concepts (qubits, entanglement) and their impact over the control operations. The relevant control operations include entanglement swapping and quantum teleportation. The authors proposed a model for the entanglement distribution in multi-hop QN to enable distributed QKD and quantum computation.

(Alshowkan et al., 2024) implemented the entanglement distribution between 2 qubits via an optical fiber-based QN at Oak Ridge National Laboratory (ORNL). Their SDN-based QN used wavelength-selective switches and included a quantum data plane in addition to the traditional data and control planes. The flexible mesh topology enabled the entanglement distribution across 6 nodes and 3 sub-networks. The adaptive resource management was used to optimize the fidelity and transmission rate. They emphasized the essential role of the multi-hop networking in building scalable, resilient, and resource-efficient quantum infrastructures — critical for future QC platforms and a global quantum internet.

(Ikken et al., 2025) demonstrated how the quantum communication can be optimized in multi-hop QN using a novel method called Bidirectional Quantum Teleportation via Modified Dijkstra Algorithm and Quantum Walk. This approach was based on different entangled states, and allowed solving the shortest-path problem for both unidirectional and bidirectional quantum teleportation. The authors tackled combinatorial optimization problems through QC concepts and entangled channels, supported by the simulation and quantum circuit-based experimentation.

The feasibility of the trusted multi-hop QKD networks and the need for an efficient key management across the intermediate nodes were already approached in some metropolitan and backbone QN/QKD networks.

A flagship achievement was reported by (Toshiba Europe Ltd & Orange, 2024), that demonstrated QKD integration in an operational telecom network, securing a 100 Gbps channel within a 400 Gbps multiplex over 184 km. This was achieved via 3 QKD links and 2 trusted nodes, validating the technological feasibility of QKD in the existing infrastructures.

On a metropolitan scale, the Tokyo QKD Network, launched in 2011, serves as a model of interoperability and resilience. Featuring a mesh topology, it interconnects 4 access points and 6 QKD systems from multiple vendors (NTT, NEC, Mitsubishi Electric, AIT, ID-Quantique, Toshiba Research Europe), allowing real-world multi-hop routing tests alongside classical traffic (Eriksson et al., 2019), (NICT, 2021), (Stanley et al., 2022).

An example from Singapore is a successful implementation of a QKD field trial within a commercial data centre environment using the existing fibre network infrastructure. Their achievements- an average Secret Key Rate (SKR) of 2.392 kbps and an average Quantum Bit Error Rate (QBER) of less than 2% - prove the feasibility of QKD in real-world scenarios (Qiu et al., 2024).

China hosts the most extensive reported multi-hop QKD network, with a ~2000 km backbone connecting 4 Quantum Metropolitan-Area Networks (Beijing, Jinan, Hefei, Shanghai), involving 700 QKD links and 32 trusted relay nodes. The network extends via 2 satellite–ground links, reaching a total span of ~2600 km and a key generation rate of ~47.8 kbps (Chen, 2021), (Liao et al., 2017), (Liao et al., 2017). The large-scale QKD networks evolved from metropolitan projects to national-spanning infrastructures, proving the reliability of the end-to-end operations with systematic key management. The China Quantum Communication Network was described as an operational long-range and trusted-relay network exceeding 10,000 km and linking several metropolitan domains. This proved notable advances in multi-hop QKD hybrid networking and long-range QN operation with reliable performance-security trade-offs and providing a proper reasoning for simulation methodologies, tools and framework able to model heterogeneous QKD links and relays (Chen, 2025), (Chen et al., 2021), (Chen, 2024).

In South Korea, the Seoul–Busan route (~490 km) exemplifies a hybrid, multi-hop architecture tested by SK Broadband and ID-Quantique for secure multi-site services and large-scale service evaluation (Stanley et al., 2022), (Toshiba, 2022).

In the USA, a commercial QKD network ("Phio" by Quantum Xchange and ID-Quantique) was launched, along with a testbed in 2020 connecting Argonne National Laboratory and Illinois (26 miles), later extended by 35 miles southward to Chicago. This fiber-based infrastructure supports quantum-safe security protocols with key generation rates exceeding 80 kbps (Toshiba technology) (University of Chicago, 2022).

In Canada, the QEYSSat mission marks a critical step in satellite–ground QKD using the flying trusted node paradigm to enable secure inter-station links over >400 km (Podmore, 2021). These efforts underscore the shift toward hybrid, scalable, and integrated quantum communication architectures being essential for the future global quantum internet.

In Europe, the R&D efforts have been made towards the QKD integration into carrier and enterprise settings. EuroQCI initiative represents a milestone in the cross-border quantum communication through practical interoperability demonstrations. It aims to support an EU-wide quantum-secure communication layer integrated with the existing infrastructures, while the multiple UK trials (e.g., BT–Toshiba) have demonstrated quantum-secured services across metropolitan fiber and industrial sites. The addressed problem concerns the quantum links interfacing with the conventional network infrastructures and their service-level objectives, further reasoning for interoperable control planes (HaDEA, n.d.), (BT&Toshiba, 2022), (BT&Toshiba, 2020).

A notable example is the Trieste–Postojna–Ljubljana–Rijeka experimental network, using a multi-hop topology with 2 trusted nodes and 3 QKD links, confirming the national and international integration under real-world conditions (Stanley et al., 2022).

The Madrid Quantum Communication Infrastructure operates as a metropolitan test platform integrated with classical optical networks and managed via SDN (Lopez, 2021). It employs both dark and lit fiber to support QKD systems at various TRLs, and includes CV-QKD devices based on continuous variables (CV). The architecture allows dynamic, scalable services and interoperability testing across vendors (Martin, 2019).

In the UK, (Stanley et al. 2022) reported the deployment of a fiber-based QKD network interconnecting Cambridge, London, Reading, and Bristol, with extensions to Southampton and the National Physical Laboratory. Using trusted nodes and multi-hop segmentation, a test on the Cambridge–Duxford route (66 km loop, 16 dB loss) demonstrated the encryption of high-speed traffic (~200 Gbps) using QKD-generated keys (~80 kbps). The 2019 activation of the Bristol metropolitan QN and a 6 km QKD industrial link between the National Composites Centre and the Centre for Modelling & Simulation further validated the trusted-node architectures under operational conditions.

In Greece, the HellasQCI project (led by the Greek Research & Technology Network and the National and Kapodistrian University of Athens) demonstrated a ring-topology QKD network across 45 km with 3 interconnected nodes.

The system supports the Layer 1 encryption and automatic fallback to the quantum-safe symmetric encryption upon the quantum channel failure (GRNET, 2024), (HellasQCI.eu, 2024).

Germany has launched multiple initiatives, including QuNET, which is testing a 125 km metropolitan QKD network with 6 nodes in Berlin. It integrates both optical fiber and free-space optics (FSO) and aims to achieve interoperability and scalability in dense urban environments (BerlinQuantum.de, 2025).

On the protocol side, recent advances such as Twin-Field QKD (TF-QKD) push beyond the P2P rate-loss limit, addressing the distance limit by reducing the number of trusted hops required for long ranges. The proposed approach could enable the advance towards the future large-scale QN (Liu et al., 2023).

Regarding the standardization, ITU-T's Y.3800 provides an architectural overview for QKD networks, describing layers (quantum, key management, application) and functional entities across domains. ETSI GS QKD 014 specifies an application-facing API and data formats for requesting and delivering key material, as a reliable support interoperable policy-aware multi-hop key routing (ITU-T, 2019), (ETSI, 2019).

Another problem is the way in which QKD could be integrated into the conventional security mechanisms enlarging the Cyber Security stack. Hybrid approaches combine QKD-derived keys with conventional/IPsec frameworks. The interest for layered defense strategy together with the integration or co-deployment of quantum-based security (QKD and PQC) reshape the requirements to ensure monitoring and incident response in QN. These trends are guidance factors for simulation case studies including not only physical/quantum impairments and routing, but also attack models and scenarios, hybrid-key usage, and policy enforcement (Industrial Cyber, 2024), (ENISA, 2021), (ENISA, 2024), (Blanco-Romero et al., 2025).

These initiatives illustrate the global shift from the experimental setups toward operational multi-hop QKD infrastructures, as the technological basis for the future national and transnational QN. Despite these advances, currently there are still gaps concerning the multi-hop QN/QKD networks development. The real multi-hop QN/QKD networks have still a relatively small number of nodes. Most of the current implementations only use trusted nodes while the quantum repeaters are still in an experimental stage. The advanced QKD protocols such as E91, graph states, Measurement-Device-Independent QKD (MDI-QKD) are still not applied on a large-scale in the commercial networks.

A CASE STUDY WITH SIMULATION FOR MULTI-HOP (QKD) QUANTUM NETWORKS

The simulation-based case study for a multi-hop QKD network contains: a presentation of the QNetSim simulator, the network topology specification, the simulation process for the multi-hop QKD network with noise, the performance estimation. The proposed framework could be used to evaluate end-to-end key generation rates, latency, and resilience under various network topologies and link conditions.

Depending on the real application design requirements, the simulation of the multi-hop QN/QKD networks should look for the following parameters/isssues: SKR, QBER, Fidelity, channel loss (attenuation), the noise effects over the key rate and security, latency. The present case study mainly focuses on SKR and QBER. SKR (bps) evaluates the speed of the secret (secured) key generation and establishment between the sender and receiver in a typical QKD process. QBER evaluates the error rates for the qubits between the sender and receiver. The following definitions are assumed for the simulation outputs, as concerning the achievable *rate of the secret key extraction (SK) from the sifted key* (Bebrov, 2024):

$$SK=1-H_2(\delta)-H_2(\delta_p) \qquad (1)$$

in which $H_2(X)$ is the Shannon entropy of a random variable X. For QKD, the amount H_2 (δ) estimates the fraction of the sifted key bits that are discarded *for the error correction* and H_2 (δ_p) estimates the fraction of the sifted key bits that are removed *for the privacy amplification.*

The amounts δ and δ_p depend on QBER for the quantum channel, therefore the definition (1) becomes (Bebrov, 2024):

$$SK0=1\text{-}f\_EC{\cdot}H_2\,(QBER)\text{-}H_2\,(QBER) \qquad (2)$$

where *f_EC* is the efficiency of the errors correction *(f_EC≥1)*. This definition can be used in a completed form with factors featuring specific phases of the QKD protocol: *s* - the fraction of *raw key bits* remaining after the sifting; *p* - the fraction of *sifted key bits* remaining after the parameter estimation; *d* - the fraction of qubits (or key bits generated out of these qubits) remaing just after the decoy-state method or single-photon weak coherent pulses/single qubits; *q* - the fraction of qubits remaining after the procedure of transfer/measurement (that could lead to a certain loss of qubits during the communication process) and needing the detection at the receiver (Bebrov, 2024):

$$SK1=s{\cdot}p{\cdot}[q{\cdot}d{\cdot}(1\text{-}H_2\,(QBER))\text{-}q{\cdot}f\_EC{\cdot}H_2\,(QBER)] \qquad (3)$$

This amount *(SK1)* includes factors featuring the procedures required to be performed by a QKD protocol (Bebrov, 2024), (Luo, 2024): transfer/measurement (*q*), decoy-state method (*d*), sifting- to remove the invalid data (*s*), parameter estimation (*p*), error correction *(f_EC·H_2 (QBER))* and privacy amplification *(H_2 (QBER))*. This is not a rate by definition, as being given in bits. In order to be a true rate (in bps), the definition of SKR includes the clock rate/pulse repetition frecquency, in Hz (Bebrov, 2024):

$$SKR=R_{clock}{\cdot}SK1 \qquad (4)$$

QuNetSim (Quantum Network Simulator) - a Python framework for QN simulations

Quantum Network Simulator (QuNetSim) is a Python-based framework for QN simulations. It allows to make simulations of networks with classical and quantum connections. The users can define their own topologies also specifying the types of connections. The framework includes tools for tasks such as sending an EPR (Einstein–Podolsky–Rosen) entangled pair from one node to another. This tool can be used to develop and test applications and protocols designed for QN on the Network and Application layer, such as teleportation and EPR generation over multi-hop QN (QuNetSim Project, 2019). The multi-hop networks may require more complicated routes. QuNetSim includes common networking tasks already developed, such as teleporting qubits, distributing entanglement, sending superdense coded messages, and generating secret keys with QKD. Other relevant features of QuNetSim include (QuNetSim Project, 2019):

- a layer of thread synchronization to properly handle the waiting phases of the network protocols;
- requiring the availability of routes allowing to transfer information from one node to another;
- using an entanglement swapping procedure to generate entanglement between remote hosts;
- possibility to write custom routing functions. The Python library networkx (Networkx.org, n.d.) is used to describe the network structures. The framework allows to design and evaluate the routing algorithms in a flexible way, based on both the classical connections and quantum network states;
- event-driven simulator. Events are asynchronously and arbitrarily happening. The users should design robust protocols to avoid out of order arrivals at the hosts.

A QN is approached through a layered network architecture (Figure 2) with quantum and classical connections (QuNetSim Project, 2019). The hosts are nodes that can process and store classical and quantum information. A node can operate either as an end node or a relaying node. The end node runs the application, also sends and receives messages and stores the information. The relaying node relays messages forward and can be set to act as an eavesdropper. The quantum information processing means the qubits generation and manipulation (through quantum gates), their transmission by routing in the network. Each node can be programmed to run any particular task by using Python functions.

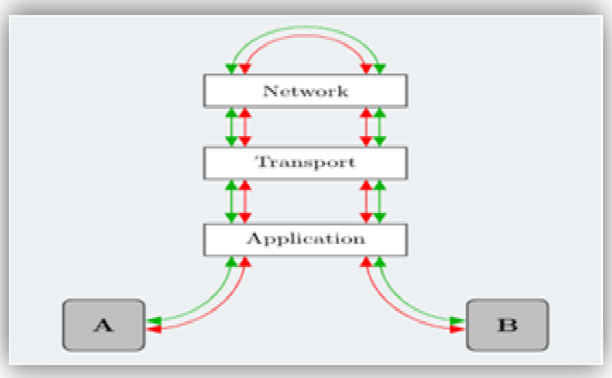

Figure 2. *The layered architecture of a QN in QuNetSim (QuNetSim Project, 2019)*

The work is still in progress to enhance the overall framework. This is why the simulations require specific assumptions and they only concern the quantum networking issues and less quantum physics (QuNetSim Project, 2019). QuNetSim can be used in Google Colab or locally while setting a virtual environment.

The multi-hop QKD network topology specification

The simplified multi-hop topology (Figure 3) contains: the source (Alice) and destination (Bob), 3 intermediate nodes (Node 1, Node 2, Node 3) and their QKD links. More complex multi-hop topologies will be considered in future case studies, where the simulation scenarios will assume settings quite similar to those on some existing QKD networks.

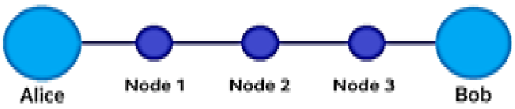

Figure 3. *The simplified multi-hop QKD network topology*

The intermediate nodes may have or not trusted repeaters (Kumar, 2024). The simulation process sub-cases are as following: with and without noise (to evaluate the influence of realistic noisy conditions over the performance), with and without attacks (to further investigate the QKD network behavior under specific attacks against the QKD protocol).

The simulation of the multi-hop QKD network behavior

The simulation is done using Python and Google Colab, with qunetsim and networkx libraries. The outputs for this simple case simulation of a multi-hop QKD network (Figure 3) are as following (QBER per hop for a setting with the noise parameter fixed to 0.05):

```
QBER per hop: [0.08, 0.12, 0.1, 0.1]
```

These results are achieved assuming *the same noise per hop*. This parameter (noise) can be varied in the range 0.01 to 0.2 to see its influence over QBER per hop. The security condition requires for QBER not to exceed 11% (0.11), otherwise the information security cannot be ensured and the key cannot be secured through reconciliation and error correction. One can see that for the 2nd hop (Node 1-Node 2) the achieved QBER exceeds the critical limit. The source of noise is not specified and the effects of the quantum decoherence are not considered but these issues will be addressed in a next case study.

Now one can *independently simulate QBER per hop* in order to see the local contribution to the error rate. The simulation process assumes that a string of bits is generated at the source. This is passed through each hop while applying the corespondent noise for that hop. The theoretical QBER E2E (end-to-end) is computed by composing binary symmetric channels (BSC), in order to verify the reliability of the simulation process. One can evaluate QBER per hop and the total QBER for the overall multi-hop path, also for the same noise per hop or for the sub-case in which each hop has a different noise level. Assuming again the same noise per hop (0.10), the following results are achieved (QBER per hop and E2E):

```
QBER per hop (empiric): [0.1, 0.097, 0.098, 0.097
QBER end-to-end (empiric): 0.279 (average)
QBER end-to-end (theoretical, composing BSC): 0.2952
```

Assuming a different noise per hop (0.05, 0.10, 0.15, 0.20), the following results are achieved:

```
QBER per hop (empiric): [0.038, 0.097, 0.147, 0.201]
QBER end-to-end (empiric): 0.339 (average)
QBER end-to-end (theoretical, composing BSC): 0.3488
```

For the ideal case (without noise, non-realistic), QBER is 0 (either per hop and end-to-end). But this is not a practical case, given the complexity of the noise sources that are present in the real QKD network scenarios or the decoherence effects in the quantum systems.

The simulation is further extended to provide *the estimation of SKR* when working with the BB84 QKD protocol, either for the ideal case -Shor-Preskill- and for a more realistic practical case with the efficiency of errors correction (Bebrov, 2024). Another provided estimation concerns *the latency* (propagation and classical rounds- reconciliation and processing). The simulation provides QBER per hop, QBER E2E, SKR per hop, SKR end-to-end (measured in bps) for network models with and without trusted relays. The latency estimation considers the extraction of a block with K bits belonging to the generated secret key. The same settings for noise per hop are applied as in the previous simulation (Alice-Node 1: 0.05, Node 1-Node 2: 0.10, Node 2-Node 3: 0.15, Node 3-Bob: 0.20).

```
[QBER] per hop (empiric): [0.0504, 0.0997, 0.1538, 0.205]
[QBER] end-to-end (empiric): 0.3511
[QBER] end-to-end (theoretical, composing BSC): 0.3488
[SKR/bit-tried] per hop (ideal): [0.2119, 0.032, 0.0, 0.0]
[SKR/bit-tried] per hop (practical): [0.1889, 0.0, 0.0, 0.0]
[SKR] per hop (ideal, bps): [211906, 31956, 0, 0]
[SKR] per hop (practical, bps): [188858, 0, 0, 0]
[SKR E2E] Trusted relays — ideal (bps):   0
[SKR E2E] Trusted relays — practical (bps): 0
[SKR E2E] Direct chain — ideal (bps):     0
[SKR E2E] Direct chain — practical (bps):   0
[LATENCY estimated] for 1000 secret bits:
Trusted relays — ideal:   ∞ (unfeasible)
Trusted relays — practical: ∞ (unfeasible)
Direct chain — ideal:     ∞ (unfeasible)
Direct chain — practical:   ∞ (unfeasible)
```

In this output, SKR/bit-tried allows to find out the average number of secret key bits that can be extracted within the QKD process starting from every bit that is generated before sifting; if multiplied by the raw-rate per link (hop) in bps it provides SKR. For trusted relays, the end-to-end secret key is constrained by the hop having the lowest SKR (bottleneck). For the direct chain (without trusted relays), the composite QBER of the chain is used, getting the SKR based on it - usually 0 or very small for higher QBER (exceeding 11%). The latency includes the following timing components: acqusition time (depending on SKR E2E), classical rounds - Round-Trip Time (RTT) and processing time.

Figure 4 represents the evolution of the SKR in respect to the number of hops in the QKD network for the simulation parameters considered, with different noise levels for the different P2P links according to the measured profile (0.05, 0.10, 0.15, 0.20). The representation contains 4 curves corresponding to the following sub-cases depending on the trustness of the relays: 1) trusted-ideal (Shor–Preskill); 2) trusted-practical (more realistic, with an error correction efficiency factor setting f_EC = 1.16); 3) direct-ideal (QBER composite); 4) direct- practical (more realistic). The results are also given in Table 1.

These results are achieved from a baseline scenario which is not optimal, as much as the achieved QBER E2E significantly exceeds the threshold (11%). The same methodology is applied for the modified scenarios including lower values of the noise parameter and the cases for direct chains (without trusted relays). The results for the different scenarios are depicted in Table 2. The best results are expected to be achieved for the simulated QKD network when QBER per hop are decreased to be lower than 2%.

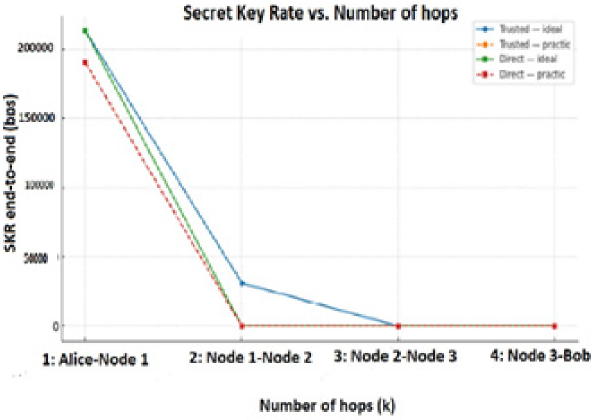

Figure 4. *SKR vs. Number of hops for the profile with different noise per hop (0.05, 0.10, 0.15, 0.20)*

Table 1. *SKR vs. hops (simulation)*

k_hops	hop_added_to_k	SKR_trusted_ideal_bps	SKR_trusted_practic_bps	SKR_direct_ideal_bps	SKR_direct_practic_bps
1	Alice-Node 1	213603	190691	213603	190691
2	Node 1-Node 2	31004	0	0	0
3	Node 2-Node 3	0	0	0	0
4	Node 3-Bob	0	0	0	0

The baseline scenario describes a realistic suboptimal multi-hop QKD network with a moderate-to-high noise level per link. This ensures QBER E2E values above the security threshold (theoretical 11%) and a null SKR. *The optimized scenario* assumes enhanced conditions (lower noise, higher raw rates) and protocol tuning. This leads to a reduced QBER E2E and a significantly improved SKR on trusted segments. *The direct-ready scenario* is defined for an ideal setting with uniformly-low noise across hops. This supports the end-to-end key generation without trusted relays allowing to simulate a future-ready and high-performance QKD link.

As expected, QBER (empirical and theoretical) is improved for simulated hops with lower noise. A lower QBER per hop decreases QBER E2E; the target for QBER E2E is not to exceed 11%. The simulation is done assuming TARGET_ SECRET_BITS = 1000. The sifting parameter set to 0.8 shows an efficient running of the QKD protocol (BB84) as concerning the increased number of useful bits after the sifting phase in which the unreliable data caused by loss and basis inconsistency are removed (Bebrov, 2024). Higher raw rates ensure the potential to increase SKR (bps). Figure 5 shows SKR direct vs. QBER E2E for the simulated scenarios given the multi-hop topology with 3 intermediate nodes.

Table 2. *The aggregated results for 3 simulation scenarios*

idx	Scenario	P_HOPS	RAW_ RATE_ BPS	SIFTING	F_EC	QBER E2E (emp)	QBER E2E (th)	SKR trusted (practic) [bps]	SKR direct (practic) [bps]	Latency trusted for 1000 bits [s]	Latency direct for 1000 bits [s]
0	Baseline	[0.05, 0.1, 0.15, 0.2]	1000000	0.5	1.16	0.3511	0.3488	0	0	Infinity	Infinity
1	Optimized	[0.02, 0.03, 0.04, 0.05]	5000000	0.8	1.08	0.1248	0.1264	1520924	0	0.023	Infinity
2	Direct-ready	[0.02, 0.02, 0.02, 0.02]	5000000	0.8	1.08	0.0741	0.0753	2760696	792684	0.0227	0.0236

QBER E2E is the error rate achieved over the full path Alice -Node 1-Node 2-Node 3-Bob. One can see the 3 domains for QBER E2E:

- low QBER E2E domain (≈ 0 – 0.1), in which SKR is high (exceeding 100.000 bps). This is the optimal operation region for the network with the given multi-hop topology. The intermediate channels have loss levels and noise. The potential attacks (if occur) cannot be detected under these circumstances or their impact is not very significant. Under this operation domain the 2 entities, sender and receiver, may establish reliable secret keys to be used in their applications -symmetric cryptography, Virtual Private Network (VPN) with QKD to ensure a quantum-secured communication channel;
- thresholding QBER E2E domain (around 0.11 or in the range ≈ 0.1 – 0.15), in which SKR suddenly drops to very low values (a few thousand or tens of bps). This is because as QBER

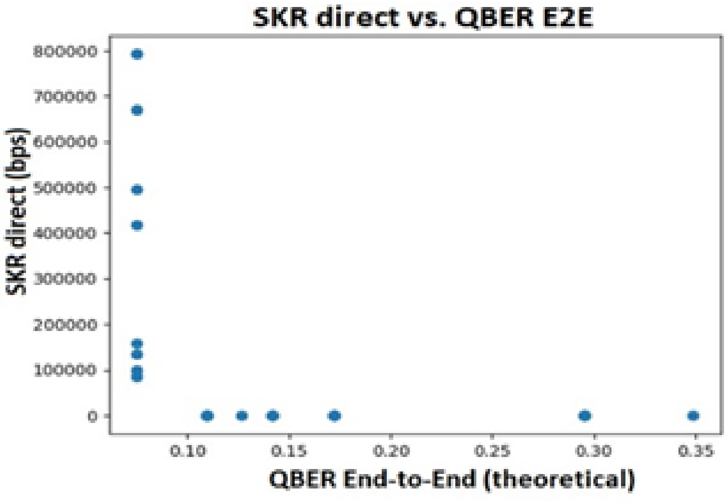

Figure 5. *The QKD Experiment Comparison Diagram*

increases, the sifting, error correction and privacy amplification process removes a large fraction of the bits, so the effective secret key rate is significantly reduced. This domain is a critical one as much as the network becomes sensitive to noise and to IR or PNS attacks. The overall performance decreases;

- completely unsecure domain for QBER E2E > 0.15 – 0.2. SKR decreases towards 0. The reason is that beyond a threshold (≈11% for BB84, ≈20–25% for other protocols), the error rate becomes too high for secrecy to be informationally guaranteed anymore. Under these circumstances, the achieved key cannot be used because the adversary could have more information than the legitimate participants. This problem is amplified in the multi-hop QKD networks in which each intermediate node introduces additional noise.

Discussion

The experiment (simulation with QuNetSim) assumed for the baseline scenario (Table 2) that the sifted key that contains the bits corresponding to the same measurement basis from Alice and Bob is about 50% from the raw input. This assumption for the raw bits that survive sifting is already expected from the theoretical BB84 basis matching. The optimized cases use a higher sifting factor (0.8) that could show further improvements as concerning the synchronization, reduced loss and potential adaptive basis selection procedures in enhanced implementations.

For a multi-hop QKD network, the performance (SKR) significantly depends on QBER E2E. In ideal scenarios (no attacks, low noise per QKD link/node), a very high SKR can be achieved if a QBER E2E significantly lower than 0.11 is ensured. On the other hands, the presence of specific attacks could have effects on SKR depending on the influence on QBER E2E.

For a typical Intercept-Resend attack one can expect to significantly increase QBER E2E up to 20-25% after sifting (under the assumption of random measurement basis). This leads to a major reduction of SKR (Figure 6). The attack is detected if QBER exceeds the threshold (11%, typical for BB84). However, in the real cases there is the problem of how accurately QBER E2E can be estimated. This factor has a major impact on the efficiency vs. security ratio for the QKD protocol (Al-Janabi, 2025). As concerning another typical attack against QKD, Photon Number Splitting, there are still a lot of debates about its detection (Ashkenazy, 2024). One can expect for this attack not to significantly increase QBER E2E, but to effectively decrease SKR by information leakage (and would require decoy states for detection). These attacks will be subject to a future detailed research work looking to further explore the implications for Cyber Security.

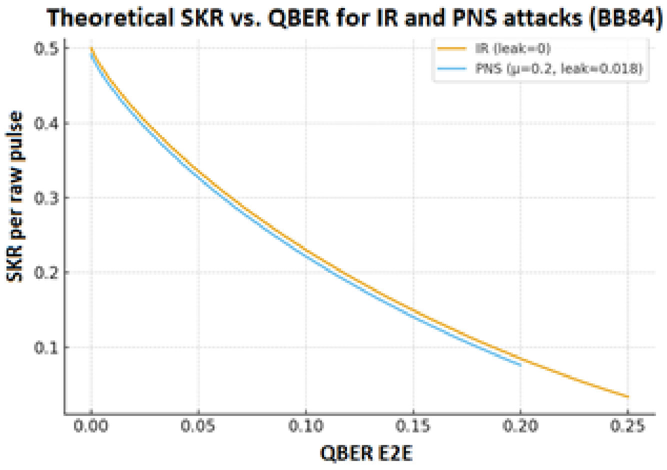

Figure 6. *The QKD Experiment Comparison Diagram*

Figure 6 depicts the theoretical SKR (QBER E2E) curves for the attack scenarios IR and PNS. These curves are generated by the simulation model assuming a secret fraction per sifted bits given by the ecquation (2). Another assumption is that about half of the bits survive sifting. The efficiency of the errors correction f_EC is fixed to 1.16. The IR curve decreases only by the error correction term f_EC·H_2 (QBER), there is no information leak. When QBER E2E increases (as a result of a probable IR attack), SKR decreases sharply and tends to 0 for QBER approaching 25%. The PNS curve is shifted downwards compared to the IR curve, even for the same QBER E2E. The PNS attack does not increase QBER but reduces SKR by information leakage (if decoy states are not used).

This QBER threshold (that is, 0.11-0.15 for the present case) defines the security limit: for values below it the network can be assumed to be secured and the generated key can be used, otherwise the key can no longer be considered secure. This threshold of 11% defines the theoretical security limit for the BB84 protocol under ideal conditions. The QBER values above 0.15-0.2 are labeled as network insecure because in practical QKD deployments with noisy multi-hop networks, the error correction and privacy amplification cannot completely compensate the noise level and potential eavesdropping information leakage.

In the context of simulations with QuNetSim (or any QN simulator), the appearance of an „infinity" (∞) latency in the results of the QKD network with 3 intermediate nodes indicates that the transmission or establishment of the quantum channel was never achieved for certain settings. The possible causes for ∞ latency in simulation are as follows: a) Inability to establish a route between nodes -either there is no valid path through the intermediate nodes (the topology is not connected), or the routing protocol did not find the path; b) Total losses per channel (loss probability = 1 or close to 1)- if the channel parameters are set such that every photon/qubit is lost, then the transmission never arrives and the effective time becomes infinite; c) Message delivery timeout - if a classical or quantum message has a maximum waiting time (timeout) that is exceeded, the simulator may mark the latency as ∞; d) Deadlock in the protocol - if the nodes are waiting for messages that never arrive, the simulator may consider the latency to be infinite; e) Synchronization issues / implementation bug - in some implementations of QuNetSim, ∞ latency can occur if a channel is not initialized correctly or if parameters are not properly set (e.g. channel length = 0 or invalid error rate). In a physical deployment, for a real multi-hop QKD experiment, ∞ latency would mean: 1) no secret bit is generated (unusable channel), 2) the network is completely blocked by noise or attacks, 3) the intermediate nodes cannot establish entanglement (in the case of entanglement-based protocols- E91).

The next case studies for multi-hop QKD networks will consider: different sources of noise, fix and variable noise, the effects of the quantum channels imperfections and quantum decoherence on the performance. This methodological framework (based on QuNetSim) will be applied for cases incorporating realistic noise sources, quantum channel imperfections, and eavesdropping attack scenarios. The future case studies will show the QBER per link increasing together with the distance, noise and decoherence. It will be interesting to find out through simulation the maximum distance and the number of hops that can be afforded for a certain multi-hop topology to ensure a reliable key generation process. The entanglement-based QKD protocols will be considered for the future case studies together with their implications for the Cyber Security. A more complex simulation model including specific attack scenarios against the QKD protocol will be considered. One can consider simulation scenarios to show the network behavior under typical attacks against the QKD protocol. The future simulation cases will consider active attacks scenarios such as Man-in-the-Middle or Denial-of-Service. The simulation cases with various types of attacks against the QKD protocols are important to show the Cyber Security implications of the multi-hop QKD networks development.

The main contribution of this work is the methodological framework for the QN/QKD network simulation, extending the authors' previous work for P2P QKD links (Soviany et al., 2024). Besides the simulation process, the present case study is focused on exploring the multi-hop QKD networks performance and their implication for Cyber Security. The basic BB84 protocol was considered for this simulation case.

QuNetSim is a reliable simulation tool for the QKD networks; it includes primitives that simulate the qubits transmission on multi-hop paths. It allows to define communication protocols and to make sniffing on nodes, ensuring a software framework to simulate eavesdropping on channels (QuNetSim Project, 2019).

CONCLUSIONS

This work belongs to an ongoing research concerning the QKD applications, with focus on the multi-hop QKD networks. A simulation-based case study is presented, including the performance and Cyber Security implications. The methodology can be further applied to model the quantum channel impairments, various changes in the QKD network topology (the number of intermediate nodes and links) and even passive and active attacks, including eavesdropping and specific attacks against the QKD systems. The simulation outcomes provide a reliable insight into the multi-hop network operation and performance, allowing to find out the trade-offs between the hop count, key generation rate and the security level. This could support a reliable guidance to design future quantum-secured communications infrastructures for applications requiring high security against both passive and active attacks. The present research work could bridge the gap between theoretical QKD security guarantees and the working framework of the large-scale QN/QKD networks deployment in vulnerable environments with many and complex threats.

The simulation is a reliable approach to evaluate the systems performances and their behavior under different conditions. This is especially true when one should deal with large-scale QN (QKD networks) for which the performance trade-offs and security implications must be properly estimated before the implementation. The various simulations software tools for QN and particularly multi-hop QKD networks could provide a reliable insight into their operations. The resulted evaluations are useful to enhance the overall design, given the complexity and the deploying costs. The advantages of such simulations include the capability to perform the modelling of the quantum channel properties, the possibility to integrate realistic noise and loss parameters and to test several QN/QKD networks topologies under various conditions. Some tools and methodologies allow to embed cyber-attack models alongside physical-layer impairments. Their goal is to outcome a reliable view of performance and Cyber Security resilience, which are very important for applications based on multi-hop QKD networks.

ACKNOWLEDGEMENTS
The work presented in this paper is supported by the Core Program within the National Research Development and Innovation Plan 2022-2027, carried out with the support of MCID, project no. 23380601, "Advanced research in the Metaverse and emerging technologies for the digital transformation of society".

REFERENCE LIST

Al-Janabi, S. (2025). The Effect of QBER Estimation on the Efficiency and Security of Quantum Key Distribution. *Baghdad Science Journal*, 22(7), 26. https://doi.org/10.21123/2411-7986.5006

Alléaume, R., Branciard, C., Bouda, J., et al. (2014). Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science*, 560, pp. 62-81.

Alshowkan, M., et al. (2024). *Resilient entanglement distribution in a multihop quantum network*. arXiv preprint arXiv:2407.20443.

Ashkenazy, A., Idan, Y., Korn, D., Fixler, D., Dayan, B., Cohen, E. (2024). Photon Number Splitting Attack – Proposal and Analysis of an Experimental Scheme. *Adv Quantum Technol*. 7(2300437). https://doi.org/10.1002/qute.202300437

Bebrov, G. (2024). On the (relation between) efficiency and secret key rate of QKD. *Sci Rep*. 14, 3638. https://doi.org/10.1038/s41598-024-54246-y

Blanco-Romero, J., Otero García, P., Sobral-Blanco, D., Mendoza, F., Vilas, A. & Fernandez-Veiga, M. (2025) *Hybrid Quantum Security for IPsec*. arXiv preprint arXiv:2507.09288.

Brazaola-Vicario, A., Ruiz, A., Lage, O., Jacob, E. & Astorga. (2024) Quantum key distribution: a survey on current vulnerability trends and potential implementation risks. *Optics Continuum*, 3(8), pp. 1438-1460. https://doi.org/10.1364/OPTCON.530352

BT&Toshiba. (2020) *BT and Toshiba install UK's first quantum-secure industrial network between key UK smart production facilities*. [Online]. https://www.toshiba.eu/cambridge-research-laboratory/news/bt-and-toshiba-install-uks-first-quantum-secure-industrial-network-between-key-uk-smart-production-facilities/? [Accessed 20th August 2025].

BT&Toshiba (2022). *BT and Toshiba launch first commercial trial of quantum secured communication services.* [Online]. Disponibil la: https://www.global.toshiba/ww/news/corporate/2022/04/news-20220427-01.html? [Accessed 20th August 2025].

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X. & Hanzo, L. (2022) The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Surveys & Tutorials*, 24(2), pp. 839-894.

Chen, H.Z., Li, M.H., Wang, Y.Z., et al. (2025) Implementation of carrier-grade quantum communication networks over 10000 km. npj Quantum Inf, 11, 137. https://doi.org/10.1038/s41534-025-01089-8

Chen, J.P., Zhou, F., Zhang, C., Jiang, C., Chen, F.X., Huang, J., Li, H., You, L.X., Wang, X.B., Liu, Y., Zhang, Q., Pan, J.W. (2024) Twin-Field Quantum Key Distribution with Local Frequency Reference. *Phys Rev Lett.*, 132(26), 260802.

Chen, T.Y., Jiang, X., Tang, SB., et al. (2021) Implementation of a 46-node quantum metropolitan area network. *npj Quantum Inf,* 7, 134. https://doi.org/10.1038/s41534-021-00474-3 https://www.nature.com/articles/s41534-021-00474-3

Chen Y. (2021) An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, pp. 214-219.

ENISA European Union Agency for Cybersecurity (2024) *2024 Report on the state of Cyber Security in the Union 2024.* [Online]. https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf?

ENISA (2021) *Post-Quantum Cryptography: Current state and quantum mitigation.* [Online]. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation?utm_source=chatgpt.com#contentList

Eriksson, T.A., Hirano, T., Puttnam, B.J., et al. (2019) Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun Phys*, 2, 9. https://doi.org/10.1038/s42005-018-0105-5

ETSI (2019) *ETSI GS QKD 014 V1.1.1 (2019-02) Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.* [Online]. Disponibil la: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf?

European Health and Digital Executive Agency (HaDEA) European Comission (n.d.). *Quantum communication infrastructure (EuroQCI).* [Online]. Disponibil la: https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about/quantum-communication-infrastructure-euroqci_en [Accessed 20th August 2025].

Gaur, V. & Aggarwal, A. (2020) Quantum Key Distribution: Attacks and Solutions. *3RD International Conference on Innovative Computing and Communication (ICICC-2020).* https://www.researchgate.net/publication/340232084_Quantum_Key_Distribution_Attacks_and_Solutions

Government of Canada (2025) *Quantum Encryption and Science Satellite (QEYSSat).* [Online]. https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp

GRNET & NKUA Report (2024) *GRNET-NKUA Scientific Paper QKD.* [Online]. https://grnet.gr/en/2024/07/11/grnet-nkua-scientificpaper_qkd/

HellasQCI Project (n.d.) *HellasQCI Project.* [Online]. Disponibil la: https://hellasqci.eu

Ikken, N., Kumar, P., Slaoui, A., Kar, B., Laamara, R. A., Almousa, M., & El-Latif, A. (2025) *Optimizing Multi-Hop Quantum Communication using Bidirectional Quantum Teleportation Protocol.* arXiv preprint arXiv:2504.07320. https://arxiv.org/abs/2504.07320

Industrial Cyber (2024) *ENISA's 2024 report on state of the cybersecurity focuses on fortifying digital frontier, provides recommendations.* [Online]. https://industrialcyber.co/reports/enisas-2024-report-on-state-of-the-cybersecurity-focuses-on-fortifying-digital-frontier-provides-recommendations/?utm_source=chatgpt.com

ITU-T (2019) *Recommendation ITU-T Y.3800 Overview on networks supporting quantum key distribution. (SERIES Y).* [Online]. https://www.itu.int/rec/dologin_pub.asp?id=T-REC-Y.3800-201910-I%21%21PDF-E&lang=e&type=items&

Kuhn, R. (2003) *Vulnerabilities in Quantum Key Distribution Protocols. National Institute of Standards and Technology.* [Online]. https://nvlpubs.nist.gov/nistpubs/ir/2003/ir6977.pdf

Kumar, P. & Kundu, N. K. & Kar, B. (2024) *Quantum Key Distribution Routing Protocol in Quantum Networks: Overview and Challenges*. arXiv preprint arXiv:2407.13156. https://www.researchgate.net/publication/382363418_Quantum_Key_Distribution_Routing_Protocol_in_Quantum_Networks_Overview_and_Challenges

Liao, S.-K. et al. (2017) Satellite-to-ground quantum key distribution. *Nature*, 549, pp. 43–47.

Liao, S.-K. et al. (2017) Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab. Chin. *Phys. Lett.*, 34, 090302.

Liu, Y., Zhang, W.-J., Jiang, C., Chen, J.-P., Zhang, C., Pan, W.-X., Ma, D., Dong, H., Xiong, J.-M., Zhang, C.-J., Li, H., Wang, R.-C., Wu, J., Chen, T., You, L., Wang, X.-B., Zhang, Q. & Pan, J.-W. (2023) Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance. arXiv preprint arXiv:2303.15795. https://www.researchgate.net/publication/369592659_Experimental_TwinField_Quantum_Key_Distribution_Over_1000_km_Fiber_Distance

Lopez, D. (2021). Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks. *Optical Fiber Communications Conference and Exhibition*, San Francisco, 2021.

Luo, Y., Cheng, X., Mao, H.-K., & Li, Q. (2024). An Overview of Postprocessing in Quantum Key Distribution. Mathematics, 12(14), 2243.

Marquardt, C., Seyfarth, U., et al. (2023) Implementation Attacks against QKD Systems. *Federal Office for Information Security.* [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.pdf?__blob=publicationFile&v=3

Martin, V. (2019) The Madrid SDN Quantum Network. *ITU Workshop on Quantum Information Technology for Networks*, Shanghai, 2019.

Networkx.org (n.d.) *NetworkX. Network analysis in Python.* [Online]. https://networkx.org/

NICT press release. (2021) *Beginning Joint Verification Tests on quantum cryptography technology to enhance cybersecurity in the financial sector.* [Online]. https://www.nict.go.jp/en/press/ 2021/01/18-1.html

NIST - National Institute for Standards and Technology-Information Technology Laboratory. (2025) Post-Quantum Cryptography PQC/Projects. [Online]. https://csrc.nist.gov/projects/post-quantum-cryptography [Accessed 19th August 2025].

Nosouhi, M.R., et al. (2024) Towards quantum-secure software defined networks. *IET Quant. Comm.*, 5(1), pp. 66–71. https://doi.org/10.1049/qtc2.12073

Pantoja, J.J., Bucheli, V.A. & Donaldson, R. (2024) Electromagnetic side-channel attack risk assessment on a practical quantum-key-distribution receiver based on multi-class classification. *EPJ Quantum Technol.*, 11, 78.

Podmore, H. (2021) QKD terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat). *Proc. SPIE 11852, International Conference on Space Optics*, Iunie 2021. https://doi.org/10.1140/epjqt/s40507-024-00290-6

Qiu, K.; Haw, J. Y.; Qin, H.; Ng, N. H. Y.; Kasper, M.; Ling, A. (2024) Quantum-Secured Data Centre Interconnect in a field environment. *J. Surveill. Secur. Saf.*, 5, pp. 184-97.

QuNET Berlin (2025) Key experiment of the QuNET initiative. [Online]. https://berlinquantum.de/en/blog/article/key-experiment-of-the-qunet-initiative/

QuNetSim Project (2019) *QuNetSim: A Software Framework for Quantum Networks.* [Online]. Disponibil la: https://tqsd.github.io/QuNetSim/

Sabani, M., Savvas, I., Poulakis, D. and Makris, G. (2022) Quantum Key Distribution: Basic Protocols and Threats. *26th Pan-Hellenic Conference on Informatics (PCI 2022),* 25–27 noiembrie 2022, Atena, Grecia. ACM. https://doi.org/10.1145/3575879.3576022

Soviany, S., Gheorghe, C.-G., Gheorghe-Moisii, M. (2024) Quantum Networks and Cyber Security. A Simulation Case Study for Point-to-Point QKD Links. *Romanian Cyber Security Journal*, 6(2), pp. 27-43. https://doi.org/10.54851/v6i2y202403

Stanley, M., Dynes, J. F., Lucamarini, M., Sharpe, A. W., Yuan, Z. L., & Shields, A. J. (2022) Recent progress in quantum key distribution network deployments and standards. *Journal of Physics: Conference Series*, 2416 (1), 012001.

Tessinari, R.S., Woodward, R.I. and Shields, A.J. (2023). Software-defined quantum network using a QKD-secured SDN controller and encrypted messages. În: Optical Fiber Communication Conference, Martie 2023, pp. W2A-38. Optica Publishing Group.

Toshiba Digital solution press release (2022). T*oshiba Group and KT Collaborate on Quantum Key Distribution Pilot Projects in South Korea.* [Online]. https://www.global.toshiba/ww/company/digitalsolution/news/2022/0328.html#id03

Toshiba Europe Ltd & Orange. (2024) *Toshiba Europe and Orange successfully evaluated quantum-secure solutions suitable for today's telecoms networks.* [Online]. https://www.toshiba.eu/quantum/news/toshiba-europe-and-orange-successfully-evaluated-quantum-secure-solutions-suitable-for-todays-telecoms-networks

Tsai, C.-W.; Yang, C.-W.; Lin, J.; Chang, Y.-C.; Chang, R.-S. (2021) Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. *Appl. Sci.*, 11, 3767.

University of Chicago press release. (2022) *Chicago expands and activates quantum network, taking steps toward a secure quantum internet*. [Online].

Valls, V. & Promponas, P. & Tassiulas, L. (2024) *A Brief Introduction to Quantum Network Control.* arXiv preprint arXiv:2407.19899.