International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V6I4P125
Eureka Vision Publication | Volume 6, Issue 4, 163-169, 2025

Original Article

Using Quantum Cryptography in Network Security Management

John Komarthi
San Jose, CA.

Received On: 10/11/2025 Revised On: 02/12/2025 Accepted On: 09/12/2025 Published On: 18/12/2025

Abstract - Quantum cryptography is an emerging methodology of classical cryptography. It secures communications with strong encryption and uplifts the principles of quantum mechanics. The encryption in quantum cryptography is stronger than that in classical cryptographic methods, making it unbreakable. Quantum Key Distribution (QKD) is a specific feature in quantum cryptography that checks for eavesdropping between two parties. Therefore, the present white paper aims to present the outline of quantum cryptography and its role in network security. The layout discusses limitations of present quantum cryptographic systems, like hardware requirements, distance restrictions, and challenges in integration. It also adds information on quantum computing threats, real-life influences with QKD deployment in industrial and government initiatives. It also covers the original case studies of QKD deployment, addressing adoption issues and alleviation procedures that use complementary strategies and technological advances. Above all, it explores hybrid methods to change quantum repeaters to global quantum, and provides insights for long-term protection in network security.

Keywords - Post-Quantum Security, Quantum Cryptography, Quantum Key Distribution (Qkd), Quantum Networks, Network Security, Secure Communications.

1. Introduction

The classical network security protocols depend on cryptographic algorithms of computational complexity. Quantum computers are the next innovative advancement after classical network security. It is visionary that quantum computers pose an existential threat to archetypal cryptosystems[1]. In polynomial time, Shor's quantum algorithms cracked public-key schemes (e.g., RSA, ECC). Thus, in this era, new approaches are required to secure communications without being dependent on mathematical difficulty[2]. Ergo, there are two strategies for network security systems. One is post-quantum cryptography (PQC), and the other is quantum cryptography. PQC uses classical resistant algorithms for security, whereas quantum cryptography uses laws of quantum physics to counter the attacks[2]. The National Institute of Standards and Technology (NIST) in America started standardizing PQC algorithms to ensure ready-made solutions[2], whereas quantum cryptography aims for information-theoretic security.

Quantum Key Distribution (QKD) is an essential key technique of quantum cryptography. It guarantees security with quantum mechanics. QKD allows the two parties of a communication to generate a secret security key. This makes the insecure channel a quantum channel, so the quantum state should not get disturbed. It gets disturbed if there is any eavesdropping. In such a case, QKD immediately alerts both parties about the interceptor's presence[4]. QKD provides involuntary security to the users. Even a quantum computer can't gain the key by being undetected. In 1984, the seminal protocol (BB84) demonstrated a security key with guaranteed security evidence[5]. It is because the encoding of qubits in photon polarizations initiates a security key. Subsequently, there has been a development of many QKD implementations and protocols. Single photons are disseminated through a free-space link or an optical fiber in a regular QKD environment. According to the Heisenberg uncertainty principle and the no-cloning theorem, interception of eavesdropping can be detected through anomalies in a QKD setup[10]. The secret key with standard symmetric encryption (e.g., AES) is used to encrypt the actual data. High-speed bulk encryption is managed by well-reviewed classical algorithms. This combined effect of classical and quantum cryptography establishes data confidentiality with quantum encryption keys.

Network security management benefits quantum cryptography by adding a layer of protection, and it doesn't need any dependence on computational assumptions. In particular, QKD reduces the threat "harvest-now, decrypt-later". This threat records present encrypted traffic and decrypts it when quantum computing is available[2]. Quantum-secured links can provide high-value protection to the data. Therefore, organizations make sure that the encrypted data and QKD sensitive links should not be decrypted by future attackers[1], [4] because of their need for long-term confidentiality in government and private limited companies. The Geneva elections in Switzerland are the best illustration of QKD security implementation. During elections in 2007, the Geneva government opted for QKD to avoid data tampering, to secure vote transmissions, and to maintain a confidential ballot. In increasing network security, quantum cryptography is moving from theory to practice. ID Quantique company in Switzerland commercialized the system by designing QKD in a production environment for over a decade, for utmost reliability[6]. The Geneva government is continuously using it to safeguard the election confidentiality and to maintain the integrity to boost trust in election processes[6].

Quantum cryptography provides highly encrypted security, but doesn't actually replace classical cryptography. Yet, quantum cryptography addresses some primary issues and provides solutions to some practical constraints. However, quantum cryptography blends with classical cryptography protocols and makes a hybrid system by using data encryption and authentication. Indeed, security agencies recommend using QKD with conventional resistance like Post-Quantum Cryptography instead of using it alone[2]. As we investigate, there are notable challenges like higher costs for infrastructure, standardized certification or protocols, and distance restrictions in executing QKD[9]. Hence, QKD is considered a complementary approach to the classical approach. As a consequence, it is necessary to explore its tangible benefits and hurdles to overcome in network security.

2. Real-Life Impact

Over the past two decades, Quantum's secured network development has been supported by public and private investments. In consequence, quantum cryptography has been in progress with a growing impact on communications organizations.

2.1. National Strategic Networks

To secure government and defense communications, many countries built committed quantum communication networks. Particularly, China owns the biggest quantum network in the world. It spans over 4,600 km, connecting many cities with quantum-encrypted links[5]. There exists a backbone fiber network that stretches to an extent of 2,000 km between Beijing and Shanghai. This fiber network has increased satellite QKD links that form a space-ground blended quantum network[4]. The next advancement is using a satellite. With the aid of the Micius satellite, China exhibited the first intercontinental quantum encrypted video call across thousands of kilometers [4] between Beijing and Vienna. Through the EuroQCI (European Quantum Communication Infrastructure) initiative, Europe is investing more in quantum networks to cover the infrastructure and government with quantum-secured links in the future [11]. Countries like Canada, Russia, South Korea, and Japan are using QKD-based fiber networks in their quantum communication projects to connect metropolitan cities and research institutions[5]. Globally, in securing national security, quantum cryptography became a strategic asset.

2.2. Infrastructure Protection

The use of applied QKD is extended to other critical sectors like trials and pilot projects in healthcare, power grid, and financial systems [1]. A financial sector illustration in the year of 2022 specifies a collaboration between JPMorgan Chase (U.S.) with Toshiba, and Ciena to check a quantum-secured network for blockchain technology applications. When the QKD key is exchanged on a metropolitan fiber link, around 800 Gbps encrypted data rates are achieved[8]. QKD can be incorporated into modern high-bandwidth networks to detect and thwart espionage attempts[8]. Another illustration of using QKD is in the power sector of European trials in Austria and Italy to secure communication between power-grid control centers, to prevent eavesdropping or sabotage on energy infrastructure [1]. Further illustration of the use of QKD cryptography in the healthcare industry is to secure sensitive medical cases transmitted data among the hospitals. While many QKD applications are pilot studies, they display the *real-life impacts* by addressing security issues, which cause severe consequences.

2.3. Commercial and Industry Adoption:

Companies like ID Quantique (Switzerland), Toshiba (Japan/UK), QNu Labs (India), and QuantumCTek (China) are selling QKD devices to telecom companies and data centers to incorporate them into networking products for quantum cryptographic solutions[2]. For instance, British Telecom (BT) and Toshiba trialled and tested QKD keys to secure data traffic between datacenters in London, and Orange S.A. Communications in France for telecom network encryption[2]. The development of quantum-ready network hardware is another notable exploration in this industry. The vendors of Network encryption devices offer "quantum-safe" models that accept QKD systems keys[6], e.g., high-speed optical encryptors of 10 Gbps and 100 Gbps links are being upgraded to incorporate QKD key supply.

Real-life impacts of quantum cryptography are, on the whole, boosting the security of risky and specialized communication channels. The present technology doesn't support the deployment of QKD across the daily internet, but its impact is growing in certain domains that need high levels of security. It has been used by some Governments and enterprises to add an extra layer of defense against quantum threats, as classical encryption itself is not sufficient for long-term security management.

3. Limitations

There exist some limitations that restrict the use of QKD in network security management. Some important limitations include distance & cost limitations, specialized hardware requirements, challenges in adaptability and incorporation, security expectations and susceptibility, and operational overhead.

3.1. Distance and Cost Limitations

Single-photon quantum signals have a limited range as they cannot be magnified. With present equipment, fiber-optic QKD is limited to 100–150 km. It makes the key exchange impossible before the losses affect it[2], [12]. Beyond that, one must either introduce trusted nodes or intermediate relays that receive the key physically and re-transmit it. It's still in the experimental stage, where the key breaks end-to-end protection or uses quantum repeaters[2]. Consequently, over long-haul networks, without creating a chain of secured nodes, it is challenging to use QKD. Moreover, normal data traffic costs a bit more when compared to QKD key generation rates. In controlled settings, when the researchers achieve higher rates, the QKD systems generate keys. This generation of kilobits is equal to megabits per second, and this is enough for periodical refresh keys[12]. It denotes that QKD is best suitable for link-after-link key exchange, but not for bulk data encryption at line rate.

3.2. Specialized Hardware Requirements

Execution of quantum cryptography needs intensive use of hardware. Committed quantum optical links, dark fiber, or sightline free-space optical paths are required by QKD systems as they cannot knock over the present infrastructure without any change[3]. In this process, photon transmitters and single-photon detectors should be downloaded by users. These are delicate and need careful environmental stabilization in temperature, vibrations, etc. QKD is technically a physical layer; hence, its execution and maintenance of fibers and equipment calibration are difficult. Furthermore, the contemporary QKD devices are like proprietary boxes that don’t operate between vendors.

Hardware for special purposes and committed channels costs more. It limits the use of QKD to certain standard organizations. Unlike typical network traffic, quantum channels can’t be rerouted or virtualized easily due to their inflexibility. The quantum channel is point-to-point and brittle; therefore, it requires careful planning in network design[3].

3.3. Challenges in adaptability and incorporation

Incorporating QKD into present network security architectures causes important challenges. The important task of QKD is to provide *key exchange*. It neither provides authentication of the communicating parties nor encrypts data on its own[2]. Therefore, QKD should be combined with archetypal cryptographic mechanisms. An initial authentication using pre-shared keys or public-key signatures is required to set up the QKD link. Then, the exchanged quantum keys are used within proportioned encryption algorithms, e.g., it means QKD doesn’t replace classical cryptography, but it adds a layer of protection to that. Managing this hybrid system is difficult due to key management, key storage, and encryption alignment devices. Scaling QKD to networks with many nodes is difficult on a large scale. Conventional network security uses public-key scalewell infrastructures for many participants. Conversely, QKD networks may require a mesh network of direct quantum links or a trusted node to connect to a number of parties that don’t scale well. Though it is possible to create network topologies rings, stars, etc., with QKD, experimental multi-node QKD networks, like the DARPA and SECOQ, C showed that the overhead and management difficulty increase easily with the number of nodes[5], [1]. Until quantum repeaters and entangled photon technologies turn practical, QKD is not a good match as a drop-in replacement to secure communications along the internet. It is restricted to network configurations that have more control.

3.4. Security Expectations and Susceptibility

Theoretically, the QKD is secure, whereas its security depends practically on the functioning of quantum devices. The QKD systems can be attacked when there are loopholes in implementation. Example quantum hackings are blind avalanche photodetector receivers, injecting bright light to manipulate detector behavior, hardware imperfections, allowing an eavesdropper to avoid detection, etc.[3]. The more the hardware and protocols are used, the stronger the security will be. As QKD assures confidentiality, large-scale testing and certification are needed. There is no automatic guarantee provided, whereas it should be protected by means of classical ways. QKD is sensitive to loss of signal and commotion. Breaking encryption is not just an adversary; interference or blocking the quantum channels is an adversary, for example, bending the fiber or shining noise into it. These adversaries can cause service denial by stopping the key exchange[3]. Improper handling may cause outages, which is what network operators call this weakness as fragility of QKD in high-availability systems.

3.5. Operational Overhead and Costs

Quantum optic hardware, QKD execution are expensive, and dedicated fiber or free-space links cost per bit. Also, ongoing operational charges for monitoring optics alignment and trusted nodes for limited distances. Trusted nodes are physical points of classical form with logical complexity that check security risk; they must be guarded against threats[3]. Many organizations meet expenditure for most sensitive applications, but the security measures expenditure and complexities are prohibitive. Post-quantum algorithms are a bit cheaper, as they are mostly software updates. Due to its expensive factor, many decision makers omit QKD and choose PQC or new PQC algorithms instead for broad use. In fact, many European cybersecurity agencies and the U.S. NSA believe that using quantum-resistant encryption is less cost-effective and easier to maintain than QKD.

4. Case Studies

One should go through the real-world experiences, case studies, and reviews of quantum-secure networks. It gives a comprehensive idea of the practical, potential challenges caused by it.

4.1. DARPA Quantum Network (USA, 2003–2007)

The DARPA-funded research project in Cambridge, Massachusetts, is the first quantum key distribution network[5]. This network connected 10 nodes at length in a prototypical form between Harvard and Boston Universities. Many QKD links are connected with trusted nodes in a topology and incorporated with IP networking management. The DARPA network demonstrated the QKD working environment and underlined challenges. QKD works well in a real urban fiber environment. The challenges include specialized hardware for each node, synchronization between link encryptors and QKD devices[5]. The DARPA quantum network successfully showed methods for key relay, the feasibility of a multi-node QKD network, and QKD network routing designs for Europe and Asia. Therefore, it can be summarized that quantum cryptography can provide security to limited-sized networks.

4.2. Geneva Election Security, Switzerland (2007–present)

Primarily, in October 2007, Geneva authorities collaborated with ID Quantique to use quantum cryptography to provide security to the vote counts from the ballot counting center to the central government data repository[6]. This point-to-point link supplies encryption keys constantly to a high-speed optical encryptor by using QKD. This assures that encryption keys don't allow eavesdropping or espionage of the data that is moving among the sites. Since then, the Geneva government has been using QKD by means of a government application in every election[6]. Despite the use of QKD by the Swiss government for a long period since 2007, the downtime was minimal. It has been a substantial protection of the democratic integrity. Further, protecting the election data from interception and tampering upheld the citizens' trust. The Geneva government example led the way for many organizations to use QKD to protect their sensitive data, which includes confidential information, inter-departmental transfers, diplomatic communications, etc. The Geneva case study also proves that QKD is not just a lab-grown curiosity, but it is a practical tool for certain real-life security needs[6].

4.3. China's Integrated Quantum Communication Network

Among all G1 countries, China is the best user of the quantum network. In 2016, the country built a fiber network of 2000 km. Between Beijing and Shanghai. This is called a quantum trunk that uses trusted intermediate nodes[4]. Later, China launched a satellite, Micius quantum, in 2016. By using Micius, China facilitated an encrypted video conference call between the Chinese Academy of Sciences, Beijing, and the Austrian Academy of Sciences, Vienna[4]. The satellite delivered keys to two ground stations that are 7600 km apart from each other. This act allowed global quantum key distribution of intercontinental capacity by overcoming the distance limitations of fiber. Currently, in China, there are dozens of domestic QKD links connecting cities, government offices, stock exchange centres, and there is a secure line between Beijing and Shanghai that works with encryption for diplomatic and financial data[4]. Making keys and the complexity of multiple trusted nodes are a security challenge. Yet, this is the largest quantum cryptography so far.

4.4. European Quantum Networks (OpenQKD and EuroQCI)

The QKD projects in Europe started in 2008 with the SECOQC project in Vienna, Austria, with bankers and government agencies as stakeholders. Lately, in 2019–2022, the OpenQKD initiative has collaborated with communication networks with QKD[14]. As part of the initiative, testbeds are established in Vienna, Madrid, Berlin, Cambridge, and Geneva. These testbeds secure cloud storage backups, hospital data transmissions, and voting systems using QKD. One notable pilot linked hospitals in Austria, ensuring medical data exchanged between them remained confidential with quantum keys. In a pilot project in Austria, hospitals proved that quantum keys maintained confidentiality in medical data.

In Germany, the QuNET initiative of Fraunhofer built a 600 km quantum link (the longest link in the EU) between Berlin and Frankfurt with QKD devices to connect government sites with secured fiber lines[7]. The novel techniques, like multiplexing quantum and classical channels, reduced costs. In early 2025, Fraunhofer displayed an airborne QKD that established a secure optical link of 10 km between an aircraft and a ground station[7]. Standardizing interfaces makes the vendors communicate for certified security proofs to satisfy government evaluators.

4.5. Financial Network Trials (USA and UK)

Financial industries require ultra-secure and low-latency communications. In the United States, the research non-profit Battelle executed a QKD link in 2013 between Columbus, Ohio, and a satellite office that is 80 km away. In the US, this is the first commercial QKD network to secure corporate communications[13]. In the United Kingdom, British Telecom (BT) conducted trials to secure data links with Toshiba in the London metropolitan area by transmitting financial trading data between two sites with quantum keys, ensuring secrecy while forwarding. In 2018, a UK pilot involving the National Health Service (NHS) and BT secured the transmission of genomic data with privacy. Sometimes, financial and commercial pilots pair QKD with modern encryption hardware like high-speed Ethernet, bringing the outcome that QKD can coexist with high-bandwidth channels[8]. This means quantum keys can be delivered without dedicating entirely separate fibers. The most sensitive data, like high-value transactions, market data, etc., of financial institutions is carried safely, marking the readiness of the technology.

5. Challenges & Solutions

Beyond the technical limitations, quantum cryptography encounters many challenges as well. Here are some of the challenges considered from a broader perspective, and what is being done to address them in integrating quantum cryptography into mainstream network security management.

5.1. Standardization and Interoperability

Lack of widely accepted standards is a major challenge in quantum cryptographic systems. QKD applications are from various vendors, so they may not be compatible. European Telecommunication Standards Institute ETSI and the ITU are on their way to define standard interfaces and protocols for QKD hardware, APIs, and collaboration with link encryptors[14]. Another is certification of QKD devices; it is still in its infancy. Many organizations hesitate to trust quantum cryptography from multiple vendors. Some national metrology institutes, like NIST (US), BSI (Germany) launched programs that validate QKD systems.

5.2. Trust and Policy Issues

Another important challenge is non-technical, i.e, building trust in quantum cryptography among stakeholders. Decades of experience behind network security, decision-makers view new quantum tech as risky and unproven. In 2022, the U.S. NSA stated operational limitations and recommended quantum-resistant algorithms as the best solution [2]. In 2024, joint cybersecurity agencies of France, the Netherlands, Sweden, and Germany concluded that QKD is usable only in niche cases, so that migration to PQC is a priority for many applications[2]. These stances influence policy and investment[9]. Continuous research to address QKD weaknesses is a preferable solution. In some regions of the EU, there is more institutional support to invest and evaluate. Quantum cryptography has to prove its worth by increasing security in a transparent way to convince regulators and standards bodies. This ties into compliance with how QKD fits into security frameworks like ISO 27001 is yet to be defined.

5.3. Integration with Existing Infrastructure

Integration of QKD devices into an operational environment causes challenges. New software is needed to link quantum and classical systems. For this, QKD key material should interface with key management systems (KMS). On demand, APIs allow QKD boxes to dispatch keys to applications. Irrespective of the absence of plug-and-play type of IPsec tunnels or TLS sessions, QKD can be continuously used to refresh keys in these sessions. Linking QKD across network hops is a specific integration challenge. In between two QKD end-nodes, if there is a switch or router, the intermediate node can be trusted. Finding a way to tunnel is possible with a direct quantum repeater or fiber continuity. Therefore, to accommodate QKD, the network topology should be reconstructed. Using QKD in a cloud environment is an integration challenge. There is ongoing research about software-defined quantum networking. It is too nascent that the quantum channels and classical channels are managed together to route keys as needed. For the foreseeable future, integration is likely to be customized engineering for each usage.

5.4. Scalability

Scaling quantum cryptography is not merely a few QKD links. Usually, each QKD link needs a separate fiber that works only for quantum signals. Researchers are investigating the coexistence of quantum channels with classical data channels on the same fiber by means of filtering and isolation[8]. It needs careful engineering to keep noise away from classical signals because not to overwhelm single-photon quantum signals. Key management is another challenge for scalability. Keeping track of which keys work for which link and their replacement, trust distribution constitutes complexity in a large network. The traditional key management system is internal, not seen by third parties. Therefore, the development of new architectures like quantum key management systems (QKMS) that automatically handle the QKD-generated keys. As QKMS is under development, organizations that deploy multiple QKD links may face a piecemeal management of software. In the near future, it is expected to get the first quantum networks will be established on a small scale, and gradually lead to growth.

5.5. Competing Solutions and Uncertain Roadmap

The last challenge is the evolving landscape of quantum cryptography itself. It does not exist in a vacuum. It is an approach for secure communications against threats. PQC algorithms are being standardized now and are not cost-effective. They can run on existing hardware and provide deployable solutions quickly, rather than QKD. Hence, many organizations might choose PQC instead of investing in QKD. Therefore, QKD needs to be simplified and low-priced, as it is hard to convince the budget holders when PQC updates are readily available. It is a huge challenge to the quantum cryptography sector. Using QKD along with PQC is another solution to opt for if one fails. Thus, whether QKD is going to be widespread or remains nominal is a challenge. Hence, it is to be analyzed that until QKD is cheaper and offers interoperability solutions, its adoptability remains limited.

6. Future Directions:

The quantum cryptography sector is rapidly expanding, and several efforts are on the way to extend capabilities, minimize limitations, and enhance practicality for network security management.

6.1. Advancements in Distance Restrictions and Network Scaling

The primary research goal of QKD is the distance barrier. The development of quantum repeaters extends long distances by overcoming loss and decoherence[2]. Quantum repeaters are like the quantum analog of signal repeaters, and the research is at the experimental stage. In the quantum internet, entangled qubits can be distributed universally[2]. Satellite-based QKD in China led by Micius. Europe has planned its Eagle-1 satellite for launch around 2024–2025 to collaborate with the EuroQCI network[15]. A constellation of quantum satellites is expected in the near future for global QKD services. Potentially, it rates a space-based protective key supply layer for the planet for secure communications between any two points on Earth. When these technologies grow, distance limitations will be automatically removed.

6.2. Improved Hardware and Integration

The future trend is photonic integration that moves from bulk optics to chip-based photonic circuits for QKD transmitters and receivers. It drastically reduces the size and cost of QKD devices, and enhances their stability[7]. In a few years, we may see QKD devices of router size and executed at data centres. This size reduction goes hand-in-hand with improving key rates and fast network speed. A recent demonstration is the free-space aircraft-ground QKD link[7] for mobile and wireless. Free-space optics improved quantum encryption for planes, drones, or satellite-to-ground. The quantum links might extend quantum security to moving platforms such as military communications, ships, and aircraft that cannot be connected by fiber, by providing easy integration.

6.3. Protocol Innovations and Security Improvements

On the protocol side, researchers are working on quantum digital signatures and quantum authentication schemes. Another protocol innovation is Measurement-Device-Independent QKD (MDI-QKD). It alters the QKD setup so that the two users can send quantum states to an untrusted intermediary for measurement by making modifications at the user end. MDI-QKD has been experimentally shown to work over metropolitan distances because it neutralizes many detector side-channel attacks. Device-Independent QKD (DI-QKD) is the ultimate long-term goal. This protocol guarantees security by depending solely on observed data. PQC and QKD develop hybrid protocols to hedge bets. In the future, expected security will evolve into multiple layers of cryptography with a combined approach.

6.4. Network Architecture and Management

The most expected future direction is the concept of Quantum Access Networks. Here, the end-users can connect to a quantum network service through a telecom operator. Maybe there won’t be any fiber for QKD, but the telecom providers offer quantum security keys as services. There are research projects on Software Defined Networking (SDN) for QKD and key management virtualization. In view of management, automation and orchestration tools can handle quantum keys, such as auto-renewal of QKD appliances, checking quantum health channel, VPN backup channel, etc.

6.5. Integration with Post-Quantum Cryptography

An essential future direction is the coexistence and integration of PQ algorithms with QC, a hybrid cryptographic mode. For example, a VPN tunnel derives its encryption key from the PQ key algorithm and QKD. The attackers need to break two encryptions to peep into the communication. A researcher's demonstration in 2024 revealed that both systems negotiate before delivering a final key[2]. In a decade or more, the two parties get a quantum key from the network or from PQC; everything works under one umbrella without user mediation.

6.6. Economic and Security Ecosystem Developments

The last future directions include the broader ecosystem. Markets and services grow, and the cost curve improves with the augmenting maturity of quantum cryptography. In view of the security, insurance, and risk management might account for quantum security where companies could get lower cybersecurity insurance premiums. Government incentives and public-private subsidies may rise. International global cooperation may increase for secured communication, eg, Euro-Asia satellite call. Quantum consortia and academic collaborations initiate these developments. It is expected that in the future, the QC is going to be strengthened, user-friendly, and more integrated. If all the research milestones are reached, current limitations like distance, cost, etc. It will be reduced in a decade.

7. Conclusion

Quantum cryptography made a great shift in communication security by using physical laws instead of computational complexity. The protection of quantum cryptography is promising in providing security with a high degree of encryption. In addition, this high-level encryption works better against future quantum computers. QKD has a proven record of its deployment, safeguarding multiple data, such as Geneva elections data, securing links for financial organizations, intercontinental links between research institutions, etc. It can augment classical cryptography and ensure critical communications. If classical cryptography encounters a threat from quantum computing in the future, QKD can be future-proof for the data through encryption keys, so that no one can spy on or steal it. However, it's not a one-size-fits-all solution for all. Quantum cryptography is not a replacement for classical cryptography, but it assures maximum security for confidential and sensitive data. e.g., data of government, medical, defense, critical infrastructure, financial, etc.

Quantum repeaters, improved hardware, and satellite QKD extend the reach of QKD and hybrid crypto approaches expect to integrate quantum methods seamlessly into the cybersecurity ecosystem. It is reasonable to expect that in a decade that quantum cryptography will be more accessible and organizations might opt for quantum-security services from their telecom providers. In that future, network security management involves quantum keys regularly, like classical keys.

Ultimately, quantum cryptography illustrates how advances in science are directly proportional to enhancing cybersecurity. It converts the theoretical single photons into practical protection tools. The progress in this field is likely essential as the threats are new and increasing in order. With diligence and intelligence, if quantum cryptography is placed in its value, building networks with strong protection against threats is possible. This quantum-resilient communications infrastructure networks secure data from future adversaries.

References

[1] M. Stanley *et al.*, “Recent Progress in Quantum Key Distribution Network Deployments and Standards,” *Journal of Physics: Conference Series*, vol. 2416, p. 012001, 2022. (Open Access) DOI: 10.1088/1742-6596/2416/1/012001

[2] N. Aquina *et al.*, “A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography,” *EPJ Quantum Technology*, vol. 12, Article no. 51, May 2025. [Online]. Available: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-025-00350-5

[3] National Security Agency (NSA), Quantum Key Distribution (QKD) and Quantum Cryptography (Cybersecurity Advisory), Sep. 2022. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[4] A. Nordrum, “China Demonstrates Quantum Encryption By Hosting a Video Call,” *IEEE Spectrum*, 03 Oct 2017. [Online]. Available: https://spectrum.ieee.org/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call

[5] Aliro Quantum, Real World Quantum Network Deployments (White Paper), Aliro Technologies, 2022. [Online]. Available: https://www.aliroquantum.com/real-world-quantum-network-deployments-white-paper

[6] ID Quantique, IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation, Press Release, 23 Nov 2017. [Online]. Available: https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

[7] Fraunhofer HHI, QKD in Action: Fraunhofer HHI Brings Quantum Communication into Real-World Infrastructures, News Article, Apr 2025. [Online]. Available: https://www.hhi.fraunhofer.de/en/press/news/2025/qkd-in-action-fraunhofer-hhi-brings-quantum-communication-into-real-world-infrastructures.html

[8] JPMorgan Chase, JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application, Press Release, 17 Feb 2022. [Online]. Available: https://www.jpmorganchase.com/newsroom/press-releases/2022/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network

[9] ANSSI, BSI, NLNCSA, and SANS (Sweden), Position Paper on Quantum Key Distribution, Joint Cybersecurity Agencies' paper, Jan 2024. [Online]. Available: https://open.overheid.nl/documenten/797c7e8e-9c70-4a98-bfb4-11cb5f19515f/file

[10] J. Schneider and I. Smalley, "What Is Quantum Cryptography?", IBM Think, 2024.[11] European Commission, "European Quantum Communication Infrastructure - EuroQCI," Digital Strategy – European Commission, 2025. [Online]. Available: https://qt.eu/ecosystem/quantum-communication-infrastructure#:~:text=Europe's%20Quantum%20Communication%20Infrastructure%20initiative,EuroQCI.

[11] ID Quantique, "Quantum Key Distribution," Quantum-Safe Security – ID Quantique. [Online]. Available: https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/#:~:text=These%20solutions%20work%20up%20to,corporate%20campuses%20or%20datacentre%20interconnects.

[12] L. Greenemeier, "Election fix? Switzerland tests quantum cryptography," *Scientific American*, Oct. 19 2007. [Online]. Available: https://www.scientificamerican.com/article/swiss-test-quantum-cryptography/#:~:text=That%20is%20where%20the%20100%2C000,speed%20of%20one%20gigabit. (scientificamerican.com)

[13] AIT Austrian Institute of Technology, "Open QKD – Open European Quantum Key Distribution Testbed," AIT, [Online]. Available: https://www.ait.ac.at/en/research-topics/cyber-security/projects/open-qkd#:~:text=Important%20advances%20have%20been%20made,Additionally%2C%20in%20order%20to.

[14] European Space Agency and European Commission, "ESA and European Commission to build quantum-secure space communications network," 30 Jan 2025. [Online].Available: