*cryptography*

*Article*

# On the Security of Quantum Key Distribution Networks

**Eufemia Lella [1,*], Giovanni Schmid [2,†]**

[1] Innovation & Technology-Innovation Lab, EXPRIVIA S.p.A, 70056 Molfetta, Italy
[2] Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni, 80131 Naples, Italy
[*] Correspondence: eufemia.lella@exprivia.com
[†] Deceased author.

**Abstract:** The main purpose of a quantum key distribution network is to provide secret keys to any users or applications requiring a high level of security, ideally such as to offer the best protection against any computational attack, even of a quantum nature. The keys shared through a point-to-point link between a source and a detector using a quantum key distribution protocol can be proven information-theoretically secure based on the quantum information theory. However, evaluating the security of a quantum key distribution network, especially if it is based on relay nodes, goes far beyond the quantum security of its single quantum links, involving aspects of conventional security for devices and their communication channels. In this contribution, we perform a rigorous threat analysis based on the most recent recommendations and practical network deployment security issues. We show that, at least in the current state of our understanding of quantum cryptography, quantum key distribution networks can only offer computational security and that their security in practical implementations in the shorter term requires resorting to post-quantum cryptography.

**Keywords:** quantum key distribution; unconditional secrecy; threat analysis; security controls; post-quantum cryptography

check for updates

**Citation:** Lella, E.; Schmid, G. On the Security of Quantum Key Distribution Networks. *Cryptography* **2023**, *7*, 53. https://doi.org/10.3390/cryptography7040053

Academic Editors: Josef Pieprzyk, Leonie Ruth Simpson and Mir Ali Rezazadeh Baee

Received: 14 July 2023
Revised: 12 October 2023
Accepted: 17 October 2023
Published: 20 October 2023

## 1. Introduction

Quantum key distribution (QKD) is a symmetric secret key negotiation protocol that provides unconditional secrecy based on the laws of quantum mechanics [1]. It is an area of quantum information science that is growing very rapidly as shown by recent developments and advances, both theoretically and experimentally [2]. Numerous QKD protocols and devices have been developed to enhance the performance of QKD systems, which is typically measured in terms of secret-key rate, distance, and security. Consequently, QKD systems are now readily accessible in the commercial market. Whereas previous studies on QKD were only concerned with academic research, preliminary applications have been developing recently [3]. For this reason, the construction and the management of QKD networks (QKDNs) is currently an important foundation for the widespread use of quantum keys [4–6]. A QKD network comprises two or more QKD nodes interconnected by an optical fiber or free space links. Experimental studies on the design, implementation, management, and security of a QKDN constitute an important driving force for applying this promising information security technology [7]. The interest in this kind of technology starts from the observation that recent advances in quantum computing and quantum information theory constitute a severe threat to the current mechanisms protecting data integrity and confidentiality. Indeed the current state-of-the-art of data protection relies on the computational hardness of some mathematical problems which are susceptible to quantum cryptanalysis [8]. For example, the most widely used public-key cryptographic techniques, the encryption/signature RSA algorithm [9] and the Diffie–Hellman key-agreement protocol [10], based on the prime factorization and discrete logarithm problem, respectively, have sub-exponential time complexity if solved with the best algorithm for conventional computers but only polynomial time complexity if solved with the Shor algorithm [11] on quantum computers. Similar observations can be extended to other public-key cryptographic schemes, such as those based on elliptic curve cryptography (ECC) [12]. In addition, it is worth considering that symmetric-key schemes for data encryption (e.g., AES [13]) and data authentication (e.g., HMAC [14]) require substantial modifications of their security parameters to remain safe (for example, doubling the length of the AES encryption key). Indeed, they can be broken with "brute force" by search algorithms, for which their quantum versions offer a quadratic speedup (e.g., the Grover algorithm [15]).

### *1.1. QKDN Security Assessment*

In this scenario, the interest in studying the security of QKDNs has become increasingly great both in terms of enabling technologies and standardization procedures. The QKDNs should provide, at the application level, the secret-key bits obtained from the QKD protocol with good usability but without compromising its theoretical security. However, this has proved to be a challenging task. First and foremost, the unconditional security of a QKD protocol, as deduced from the laws of physics, has to withstand concrete implementations and operational practices. Realistic devices always have imperfections, which might not conform to idealized theoretical models used in security analysis by theorists. Two decades of studies on QKD protocols and device imperfections in practical systems have shown that a QKD protocol may have a stronger theoretical security than another, yet this can provide stronger security in the operational practice. This is because QKD protocols can only be operated below a certain implementation complexity level that arose by engineering thresholds. Over time, new QKD protocols have been proposed to address the issues posed by device imperfections [16–18]. The decoy-state protocol [19] allows secure QKD with weak coherent pulses. The measurement-device-independent (MDI) protocol [20] removes all detector side channels from QKD implementations (i.e., attacks based on extra information that can be gathered or injected because of the way detectors operate). The device-independent QKD [21] can enable QKD with uncharacterized devices (i.e., devices for which a model or their behavior is lacking or unknown).

Overall, we currently have protocols and technologies that make it possible to transmit and share quantum keys in a very secure way, at least for specific use cases and appropriate network topologies. This circumstance has been tested and improved through several field-test QKDNs realized in diverse countries. The world's first metropolitan QKD network was deployed in Boston (DARPA project [4]), followed by metropolitan QKDN implementations in other places like Vienna (SECOQC project [22]), Geneva (SwissQuantum QKD network [23]), Tokyo [24], Madrid [25], Shanghai [26], Cambridge [6], and Bristol [27]. With the advances in QKDN technology, long-haul QKD networks have been implemented in practice, in addition to the point-to-point link. For example, the space–ground integrated quantum network deployed in 2020 in China [5] depends on several key relay nodes that must be assumed fully trusted. From a security viewpoint, fully trusted nodes are problematic since they process quantum key bits in the clear. The Chinese large-scale QKDN exposes fully trusted nodes both in the context of metropolitan area networks and the backbone network connecting them. Some of the relay nodes in metropolitan networks could be converted into less critical nodes since they represent centers of star-type sub-networks, and MDI-QKD is particularly well suited to construct a star-type QKD network with untrusted centric detectors for key relay. However, intermediate relays throughout the backbone network, as well as some key relays in metropolitan networks (especially in the Beijing area), must remain fully trusted since they are constrained in performing key bit forwarding. This state of affairs will last as long as reliable quantum memories are unavailable.

In addition to threats concerning quantum key bit emission, transmission, and detection, QKDNs are complex network architectures whose security depends on many other factors, devices, interfaces, and functions other than those directly involved in QKD. Indeed, QKDNs require administration and monitoring through suitable interfaces and software, authentication plus access control for people in charge of their management, and secure links to distribute quantum key bits to cryptographic applications in the user network. Therefore, as dictated by well-known principles in cyber security [28], a proper security assessment must consider the entire system consisting of the QKDN and its connections with the application network it serves, with all the components, modules, interfaces, and players involved.

As is good general practice in information security, the security analysis of a QKDN must first identify its attack surface, i.e., the network functional elements that are susceptible to threat, including their interconnection channels. It is useful to stress in this respect that the attack surface for a QKDN does not include QKD modules and protocols; these constitute the "primitives" deployed through the network and, given their quantum physics nature, they require a separate security analysis by quantum cryptanalysts rather than network security experts. After defining the attack surface, the threats that may compromise the proper functioning of a QKDN must be classified by type and severity and associated with each element in the attack surface. In this way, it will be possible to determine the system components at risk, the related countermeasures, and their priority according to the severity of the threats. The last is a crucial aspect of a threat analysis, as it allows tailoring the security intervention according to the available resources.

In the case of a QKDN, the severity of a threat is related to the impact its occurrence may have on the confidentiality, integrity, and availability of one or more quantum keys. An accurate specification, which unfortunately is not always feasible in practice, would involve quantifying the risk of a threat based on appropriate metrics that take into account its probability of occurrence and cost. The probability of occurrence should also be assessed with the MOM (method, opportunity, motive) paradigm [28]. Moreover, business interests, relationships, and contractual and legislative constraints between operators, users, and third parties should be considered when assessing costs.

Once the threats have been identified and classified in relation to the attack surface, with their priority level, the security requirements for each of the components of the QKDN must be defined. Finally, the controls to be implemented in order to meet these requirements must be identified.

### *1.2. Scope and Contribution of Our Work*

Although much progress has been made on the security of the QKD primitive, thanks to the devising of new quantum protocols and procedures, the studies on the overall practical security of pervasive or large-scale networks for the deployment of QKD in the field are still immature both in theory and practice. Evaluating the security of a QKDN, especially if it is based on trusted relays, goes far beyond the quantum security of single QKD links, involving aspects of conventional security for devices and their communication channels. Only recently, test benches have been set up on QKD networks of a certain complexity, which is a necessary condition for carrying out adequate assessments of the overall security of these networks. Existing experiments and studies in the literature have provided valuable results in terms of the network framework, key generation rate, communication distance, and routing protocol. However, there are still some challenges and issues that must be overcome in the field of QKDN security, in particular, as underlined in other recent works on QKDN security [29], the existence of no suitable security interface between the classical end users/application and the quantum nodes. Addressing this issue is essential to enable classical end users/applications to securely access the key distribution service of QKD networks within the quantum computing environment. Furthermore, QKDNs necessitate the presence of appropriate interfaces and software for administration and monitoring, authentication and access control mechanisms, and secure links for distributing quantum key bits to cryptographic applications within the user network. This paper aims to consider these aspects and to identify possible measures to protect a QKDN as a whole, including its interface with the application layer.

On the other hand, QKDN security standards and recommendations have only been introduced in the last two years (see Table 1). Although these documents constitute a significant and decisive contribution to the secure use of the QKD primitive in practice, they are often based on ideal models whose concrete implementations, at this current stage, can lead to a high degradation of the security of the network. Several documents propose using the one-time pad (OTP) encryption scheme [30] for transmitting quantum key bits between the nodes of a QKDN with perfect secrecy, assuming the nodes themselves are trusted, i.e., immune to security threats. However, they do not address how to realize such trustiness in practice and how its implementation affects the overall confidentiality of quantum key bits or, more generally, the security of a QKDN. This approach conflicts with the basic principles of cyber security, stating that security is a holistic property of a system: the security assessment of a system and the design of controls aimed at reaching an adequate security threshold for its functional purposes must be carried out on the system as a whole.

**Table 1.** Documents and recommendations produced by standardization bodies and related to the present work.

| Label | Title | Description | Version |
|---|---|---|---|
| ETSI GS QKD 005 | Quantum Key Distribution (QKD); Security Proofs | A specification that precises the nature of the security claim, listing meaningful restrictions of adversarial action and clarifying the difference between the security claim of a QKD protocol based on models and the security claim of its implementation | 1.1.1 (2010-12) |
| ETSI GS QKD 008 | Quantum Key Distribution (QKD); QKD Module Security Specification | A specification for establishing the necessary requirements for a QKD module to have a high probability of detecting and responding precisely and timely to attempts of direct physical access and use or modification of modules inside | 1.1.1 (2010-12) |
| ETSI WP n. 27 | Implementation Security of Quantum Cryptography | A white paper for a general audience summarizing the status of quantum cryptography implementation security and outlining the understanding of the best practice related to it | 1st ed (2018) |
| ETSI TR 103 616 | CYBER; Quantum-Safe Signatures | A technical report providing descriptions of the digital signature schemes submitted to the National Institute of Standards and Technology (NIST) for the third round of their post-quantum cryptography (PQC) standardization process | 1.1.1 (2021-09) |
| ETSI TR 103 823 | CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation | A document providing technical descriptions of the public-key encryption (PKE) and key encapsulation mechanisms (KEMs) submitted to NIST for the third round of their PQC standardization process | 1.1.2 (2021-10) |
| ITU-T XSTR-SEC-QKD | Security Considerations for Quantum Key Distribution Network | A technical report providing security considerations for QKD networks, standardization issues, and suggestions for future work | 1.0 (2020-03) |
| ITU-T X.1710 | Quantum Communication–Framework of QKDN Security | A recommendation that specifies a simplified QKDN structure for the analysis of the relevant security threats. Security requirements and corresponding security measures are then specified on that basis | 1.0 (2020-10) |
| ITU-T X.1712 | Security Requirements and Measures for Quantum Key Distribution Networks—Key Management | A recommendation specifying security threats and security requirements for key management in QKDNs, and security measures of key management to meet the security requirements | 1.1 (2022-02) |
| ITU-T X.1714 | Key Combination and Confidential Key Supply for Quantum Key Distribution networks | A recommendation that describes key combination methods for QKDN and specifies security requirements for both the key combination and the key supply from QKDN to cryptographic applications | 1.0 (2020-10) |

This work aims to use the methodology described in the previous section to identify the security risks to which a QKDN may be subject and the related preventive controls. The analysis starts from the functional diagram of a QKDN performing key relay taken from the ITU-T standards documentation and provides a detailed threat analysis for a QKDN. Through the definition of the attack surface and the characterization of the possible threat for a QKDN, we will show that the unconditional secrecy for key bits is actually possible only for the simplest and idealized usage scenarios, whereas practical use cases require, at the current state, a strict integration of QKD and conventional security controls, in particular post-quantum cryptography. Then, we will discuss how to achieve security for QKDN nodes and communications among them, especially for key relay functions, and communications between the QKDN and cryptographic applications. Also in this case, we will start from the schemes for bit forwarding defined by the ITU-T and we will propose some variants combining simpler management of key forwarding and a high level of security. It is worth specifying that this paper focuses on the case of point-to-point trusted node QKD networks. Recently, multi-user scenarios have become research hotspots, in particular multi-user QKDN based on entangled states which are in the testing phase [31,32].

The rest of the paper is organized as follows. Section 2 discusses related work. After defining in Section 3 the attack surface of a QKDN, Section 4 introduces the criteria for classifying the threats that may afflict a QKDN in terms of their type and severity. Based on these criteria, the focus in Section 5 moves to an analytical description of the threats in relation to the attack surface. Section 6 represents the core contribution of this paper. It discusses a set of controls for ensuring the security of a QKDN versus its attack surface, providing insights into the security requirements for a trusted node and how they can be implemented through a security perimeter. Section 7 concludes the work.

## 2. Related Work

The present paper concerns preventive measures aimed at the security of QKDNs, mainly dealing with analyzing network threats and cryptographic protection mechanisms. Both cannot be addressed without reference to common practices, recommendations, and standards. Actually, the development of industry standards is essential to support the strategic goals of QKDNs and, more generally, quantum-safe cryptography. Standards promote hardware and software interoperability from various vendors, enabling the integration of quantum-safe products into telecommunication networks and facilitating the creation of a supply chain thanks to interfaces and specifications for components and modules. Standards help obtain on-market fit-for-purpose quantum-safe products and reduce the security risks arising from design flaws and implementation bugs. Based on standards, it is also possible to certify the products by laboratories and independent organizations.

Our work was mainly influenced by the recent outcomes of the post-quantum cryptography standardization process carried out by NIST [33] and the recommendations produced by the two ITU-T working groups SG13 [34] and SG17 [35] dedicated to the development of standards for next-generation networks and telecommunication security. Less influential have been the specifications produced within ISO-IEC [36] and ETSI [37], given that these standardization bodies in recent years have concentrated their efforts mainly on the security requirements of the QKD modules and on the methodologies and metrics to ensure that these requirements are satisfied in the implementations. Instead, relevant is the work of these organizations in the more general context of quantum-safe cryptography, which resulted in a series of technical documents [38]. A list of documents and recommendations produced by standardization bodies and related to our work is presented in Table 1.

## 3. Attack Surface of a QKDN

In a QKDN architecture, different functions are performed by different modules and protocols, some of which operate in overlapping layers. Overall, the following six layers can be distinguished [39]; the first four are specific to the QKDN, while the last two concern its relationship with the application-level network (see Table 2): Quantum, Key Management (KM), Quantum Network Control (QKDN Control), Quantum Network Management (QKDN Management), Service, User Network Management (UN Management).

The quantum layer represents the lowest layer of a QKD node: it is in charge of the physical transmission of quantum information and is the analog of the physical layer in the OSI model. Superimposed on it are, in order, the key management (KM), network control, and service layers, the latter being the analog of the application layer in the OSI model. In addition to these layers defining the protocol stack for a QKD node, there are two management layers, one for the quantum network and the other for the user network, that constitute a layer structure parallel to the previous one, related to the nodes for the management of the QKDN [39].

**Table 2.** The six functional layers of a quantum key distribution network.

| **QKDN Layer** | **Description** |
|---|---|
| Quantum | A set of hardware and software components that implements QKD protocols, synchronization, and distillation for sharing quantum key bits between two parties. |
| Key Management | Functional elements for performing all the activities required on keys during their life cycle. The key management agent (KMA) resizes, formats, and stores keys received from one or more QKD modules; it also relays keys to other KMAs. The key supply agent (KSA) synchronizes keys and verifies their integrity via a KSA link before supplying them to the cryptographic application. |
| QKDN Control | Functional elements to control QKDN resources, ensuring secure, stable, efficient, and robust operations of a QKDN. Controlled operations include configuration, access, session establishment, and routing. |
| QKDN Management | Functional elements to manage fault, configuration, accounting, performance, and security (FCAPS) aspects of a QKDN as a whole, and support user network management. |
| Service | A network in which cryptographic applications consume keys supplied by a QKDN. |
| UN Management | Performs FCAPS management features of a user network. |

Based on this architecture, the attack surface of a QKDN can be deduced. It consists of the input and output ports of its network nodes and management modules, as well as the interfaces and connections between them and the application layer modules to which the QKDN offers its services. We will assume that the QKDN is able to provide quantum key bit routing operations (key relay) through the interposition of nodes between the sender and the receiver. These are known as type I and type III QKDNs [40] and are more demanding in terms of security than type II QKDNs, where nodes do not perform routing operations and therefore have a simpler protocol stack. Under this assumption, according to ITU-T recommendation [41], the attack surface of a QKDN composes of the following elements (see Figure 1):

- The QKD *classical channel*, as it deals with the authentication of QKD devices and the communication of parameters required for the QKD protocol functioning;
- The *KMA* and *KSA links* between the homonymous key management modules on distinct nodes, through which the bits of quantum keys and information for their management across the network;
- The *control links* between the control modules (QKDN controllers) of designated nodes and the KM and QKD modules of the other nodes afferent to the network, where information and instructions are transmitted for the control of nodes operations;
- The *management links* between the network management modules (QKDN manager) and the KM and QKD modules of the nodes, where information and instructions for network management are transmitted;
- The *key supply links* among the QKD and KM modules on the nodes and the cryptographic applications, along which the quantum key bits are transferred to protect communications at the application level;
- The *QKDNM-NM links* between the network management modules (QKDN manager) and the corresponding application-level modules (network manager), where travel information and instructions relating to the coordination between the QKDN and the network at the application level;
- All the *physical ports* and *logical interfaces* relating to the aforementioned links, both those on each network node and those on the management modules. The former constitutes the attack surface of a trusted node. It also affects the security of the KM modules and related links belonging to the same node, deputed to transmit and store the quantum keys produced by the QKD module.

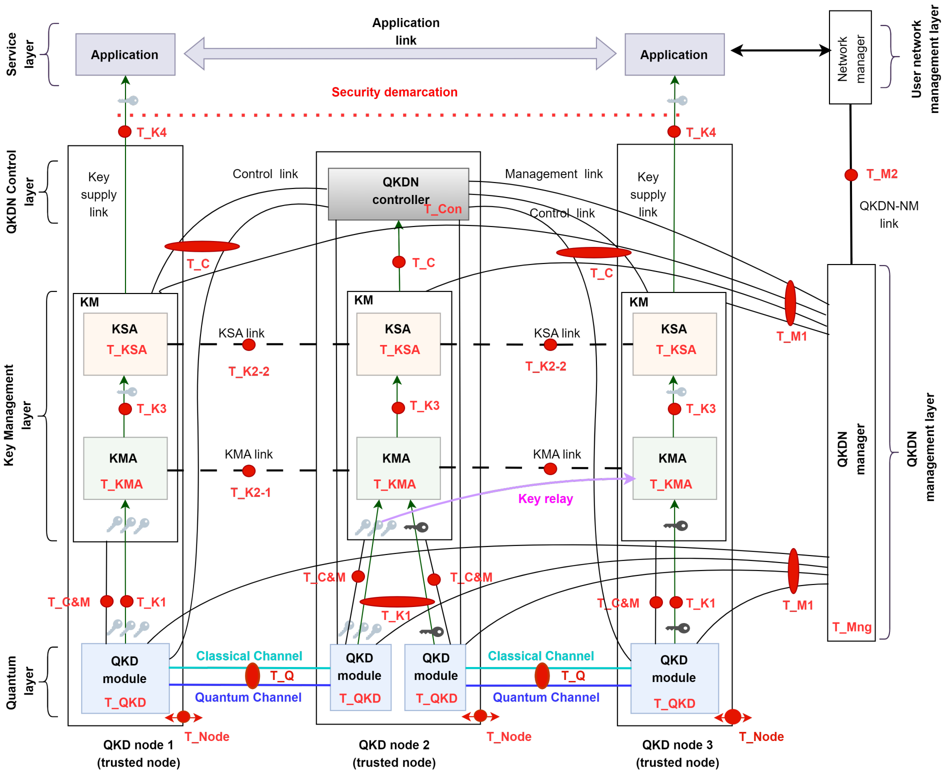

**Figure 1.** The functional diagram of a QKDN performing key relay, in which the elements belonging to the attack surface and their threats are highlighted in red (adapted from [41,42]). Dotted black lines represent KSA and KMA links. Blue and light blue lines depict, resepectively, quantum and classical channel. Quantum key bits provided to applications are shown in grey, whereas black keys denote quantum key bits used for key relay.

It is worth noting that in the context of a QKDN, the term "trusted node" indicates a protected and monitored area where the devices necessary for the functionality of the quantum, key management, control, and (optionally) application layers are located. Typically, this is a laboratory equipped with physical barriers, logical barriers, and instrumentation to control and monitor both physical access to the equipment and side channels (quantum and non-quantum) [43]. QKD devices are indeed very exposed to those threats because of the physical nature of the QKD protocol. For example, side-channel attacks cannot be prevented or reduced through attentive programming practices as they can for conventional cryptographic systems. The emergence of compact equipment integrating multiple layers (e.g., ID Quantique XG Series [44], Toshiba QKD systems [45]) can mitigate the risks of side-channel attacks but not those deriving from weak access control or vulnerabilities in QKD and QKDN management software. While these last aspects fall within the security domain of a QKDN, the mitigation of side-channel attacks is highly dependent on the protocol and devices used for transmitting quantum keys and it is, therefore, specific to QKD module security [46–48]. Regarding recommendations or implementation specifications concerning QKD modules, only the two standards GS QKD 005 [49] and GS QKD 008 [50] defined by ETSI more than ten years ago are currently available, while a new version of GS QKD 005 and the outcomes of the WG3 of ISO/IEC JTC 1/SC 27 are expected soon.

## 4. QKDN Threats and Their Severity

Cyber threats are generally specified with respect to the well-known CIA (confidentiality, integrity, availability) classification, which refers to basic information security properties. However, in the case of threats to QKDNs, it is more appropriate to consider an alternative classification that allows further or complementary details to be specified. A suitable choice could be the STRIDE classification [51], which is widely used to categorize threats in the context of software application development. In the security analysis of QKDNs, we will use STRIDE because it allows us to classify threats relating to the alteration of data or information flows more precisely than CIA, distinguishing between a violation of authentication, authorization, or data integrity.

According to STRIDE, threats can be classified as follows:

1. *Spoofing of identity (S)*: The act of usurping the identity of a party authorized to access a system or service. The violated property is entity authentication.
2. *Tampering with data (T)*: The act of modifying information, data, and documents in violation of the intentions of those who are delegated to the processing and storage. The violated property is data integrity.
3. *Repudiation (R)*: The possibility for an entity to repudiate data or actions previously attributed to it. The violated property is non-repudiation.
4. *Information disclosure (I)*: The release of information, data or documents to third parties in violation of the creators' intentions. The violated property is confidentiality. Denial of service (D): The total or partial impossibility of accessing data and services as required by the modes of provision and operation that may be established by a contract. The violated property is availability.
5. *Elevation of privilege (E)*: The ability of an entity to increase its privileges in the use of a resource or service. The violated property is authorization.

We stress that the STRIDE classification concerns only attack goals, not attack patterns, i.e., strategies and techniques for deploying them. For example, identity spoofing could happen because of weak user credentials or a bug in the authentication module.

Concerning threats prioritization, a standard semi-qualitative scale for attack rating could be deduced from the Common Criteria (CC) [52], which grades the five factors described in Table 3. However, the CC methodology makes full sense when you have a target for which all the design aspects and implementation details are known, as in the case of the experimental prototype evaluated in [48]. Without such specifications, it is impossible to obtain a prioritization that is not purely qualitative.

**Table 3.** The Common Criteria (CC) factors for attributing a numeric value to the total effort required to successfully mount an attack (*attack potential*).

| **CC factor** | **Description** |
|---|---|
| Expertise | The level of technical expertise required to successfully perform the attack. |
| Knowledge of the target | The amount of knowledge of the target design and operation required. |
| Opportunity window | The ease and frequency with which the attacker can access the target. |
| Equipment | The level of sophistication of the equipment used in the attack. |
| Elapsed time | The time to identify a certain vulnerability and to successfully mount the attack. |

In accordance with the ITU-T [41] recommendation, it is possible to consider three levels of severity that, independently of the notion of risk and its quantification, make it feasible to qualitatively assess the impact on the service offered by a QKDN, whose primary objective is to provide secret keys to pairs of nodes at the application level.

- Fatal (F): a threat of this level is fatal to the quality of service offered by a QKDN, as it involves the violation of the confidentiality of one or more quantum keys;
- Grave (G): a threat of this level can seriously compromise the reliability of the service offered by a QKDN, as it can alter actions or controls during the key or network management phases;
- Medium (M): this type of threat does not affect the confidentiality or quality of the generated keys but seriously undermines the availability or usability of a QKDN.

The following applies to the severity levels of the STRIDE scheme. Information disclosure (I) threats must be considered fatal or grave, depending on whether the attack involves access to secret-key bits or QKDN management and control information (e.g., metadata associated with keys). Tampering with data (T) is grave since its occurrence involves altering actions or controls deputed to the proper functioning of the network. Denial-of-service (D) threats are of medium severity, as their occurrence negatively affects the availability of keys but does not compromise their confidentiality and quality. Threats of the repudiation (R) type are also to be considered of medium severity since their occurrence is limited to affect the quality of the controls implemented in the QKDN concerning accesses and authorizations. Finally, a more nuanced assessment is needed for spoofing of identity (S) and elevation of privilege (E), as these threats are not directly related to ITU-T severity levels. Actually, their severity depends on the impact they have on the QKDN functioning that, according to the classification previously given, can range from medium to fatal. For example, if a spoofing of identity allows the attacker to read quantum key bits, then it must be graded as fatal; otherwise, if it results in a denial of service, then it will be graded as medium.

## 5. Threat Analysis of a QKDN

Based on the attack surface and the threat classification defined in the previous sections, we can now carry out the threat analysis for a QKDN. Our analysis follows that provided in [41] but with some modifications for better conformance to the STRIDE classification. In the following, threat type and severity are denoted with labels like $\mathbf{T}S[-S_U]$, where **T** is the STRIDE type, while $S$ and the optional $S_U$ are the lower and upper severity levels, respectively.

The various elements constituting the attack surface of a QKDN are subjected to the following threats (see Figure 1):

- **T_Node—**attacks to the physical perimeter of a trusted node to get access to its modules and the links connecting them (see Section 3):
  - **S*M-F***: an attacker impersonates an authorized entity and gains physical access to one or more of the trusted node's components;
  - **E*M-F***: an attacker performs privilege escalation and gains physical access to one or more of the trusted node's components.
- **T_QKD—**attacks to the QKD module through its logical boundary (e.g., one or more of its listening ports) to gain its command or to disclose or alter key data:
  - **S*M-F***: an external attacker impersonates the administrator of the QKD module, gaining access to one or more of its components or services;
  - **E*M-F***: an internal attacker performs a privilege escalation and gains access as the administrator of the QKD module to one or more of its components or services;
  - **R*M***: an authorized user performs QKD functions and subsequently denies that fact.
- **T_KSA, T_KMA—**attacks to the KSA or KMA key management modules through their logical boundaries (e.g., the KSA service port or the login service) to gain their control or to disclose or alter key data or metadata:
  - **S*M-F***: an external attacker impersonates the administrator of the KM layer, gaining access to one or more of its components or services;
  - **E*M-F***: an internal attacker performs a privilege escalation and gains access as the administrator of the KM layer to one or more of its components or services;
  - **R*M***: an authorized user performs key management functions and subsequently denies that fact.
- **T_Con—**attacks to the logical boundary (e.g., the control port or the management port) of a QKDN controller to gain its command or to disclose or alter control instructions:
  - **S*M-G***: an external attacker impersonates the administrator of the QKDN controller, gaining access to one or more of its components or services;

  - **E***M-G*: an internal attacker performs a privilege escalation and gains access as the administrator of the QKDN controller to one or more of its components or services;
  - **R***M*: an authorized user performs node control functions and subsequently denies that fact.
- **T_Mng—**attacks on the logical perimeter (i.e., the listening ports) of a QKDN management node to gain its control or to acquire or alter network management instructions:
  - **S***M-G*: an external attacker impersonates the administrator of the QKDN management node, gaining access to one or more of its components or services;
  - **E***M-G*: an internal attacker performs a privilege escalation and gains access as the administrator of the QKDN management node to one or more of its components or services;
  - **R***M*: an authorized user performs node management functions and subsequently denies that fact.
- **T_Q—**attacks to the classical channel of a QKD link:
  - **S***F*: impersonation of one of the two communicating parties to get access to quantum key bits;
  - **T***G*: partial or total alteration of the parameters for the correct generation of the quantum key;
  - **D***M*: overload or disturbance of the channel to reduce or zero its transmission capacity.
- **T_K1, T_K2-1, T_K3, T_K4—**attacks to one of the key supply links:
  - **I***F*: partial or total reading of quantum key bits;
  - **T***G*: partial or total alteration of quantum key bits;
  - **D***M*: overloading or disturbing the channel to reduce or zero its transmission capacity.
- **T_C&M, T_K2-2—**attacks to one of the key supply control links:
  - **I***M*: partial or total reading of metadata related to quantum key bit management;
  - **T***G*: partial or total alteration of metadata related to quantum key bit management;
  - **D***M*: overloading or disturbing the channel to reduce or zero its transmission capacity.
- **T_C—**attacks to the control channels:
  - **I***M*: reading data and instructions related to the control of the QKDN;
  - **T***G*: partial or total alteration of data and instructions related to the control of the QKDN;
  - **D***M*: overload or disturbance of the channel to reduce or zero its transmission capacity.
- **T_M1, T_M2—**attacks to the management links:
  - **I***M*: reading data and instructions related to the management of the QKDN;
  - **T***G*: alteration of data and instructions related to the management of the QKDN;
  - **D***M*: overload or disturbance of the channel to reduce or zero its transmission capacity.

From this analysis, it follows that the most severe attacks for a QKDN can belong to the two subsequent categories:

1. Authentication or access control violations at the level of the physical or logical perimeter of a node or at the classical channel that acts as a link between two QKD modules, resulting in breaches of confidentiality or integrity for the secret-key bits;
2. Confidentiality or data integrity violations for links between QKD and KM modules on the same node, between two KM modules on separate nodes, and between a KM module and a cryptographic application.

Accordingly, controls of a preventive nature must consist of:

- Access control policies implemented through appropriate entity authentication and authorization mechanisms;
- Mechanisms for the confidentiality and integrity of data and metadata related to quantum keys, as well as mechanisms to ensure the integrity of data and instructions for controlling the QKDN.

It should be clear that entity authentication, data confidentiality, and data integrity are all based on cryptographic techniques: they should be quantum-safe to avoid a general regression of the security offered by QKDNs, rendering their function useless. We wish also to stress that confidentiality protection should always be coupled with data integrity protection mechanisms; otherwise, confidential data could become useless or, in the worst case, disclosed [53,54]. For example, an active attacker could modify the key bits provided by one of the terminal KSAs to the corresponding application module, thus preventing encrypted communication between the two endpoints.

Access control policies and related mechanisms serve to protect both the perimeter of nodes and devices composing or interfacing with the network and the access to the communication channels between those nodes, with the QKDN management devices, and with the network at the application level. Given the characteristics of a trusted node, authentication mechanisms should allow for implementing a multi-layered defense by combining physical and logical protections, for example, by combining physical access control and monitoring with login procedures for the devices implementing each of the QKDN nodes (or modules). On the other hand, data integrity and confidentiality mechanisms primarily protect the various communication channels through which quantum key bits control information to adequately manage such keys travel, including communication channels between different modules located on the same node. If pre-computation of quantum keys and their storage is required, then it will be necessary to provide suitable mechanisms for storing such data in encrypted form on disk. Figure 2 illustrates the most critical subset of a QKDN. These are the components dedicated to quantum key bit management, through which the key bits or their metadata are processed, transferred, and stored. Some of these components solely require authentication mechanisms (orange lines), whereas others require integrity and confidentiality (red lines).

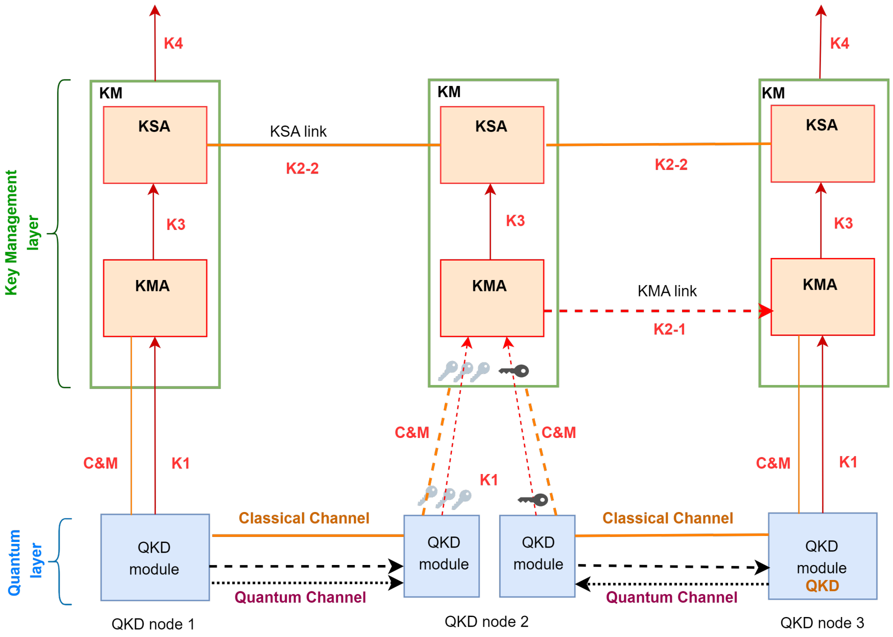

**Figure 2.** The links conveying quantum-key-related data depend on the two communication setting for the QKD end-point modules: sender–receiver (dashed black arrows) and sender–sender (dotted black arrows). Red and orange links denote communication paths for key bits and related control data, respectively. Dashed links are required only in the sender–receiver setting.

## 6. QKDN Security Controls

This section discusses measures to protect a QKDN as a whole, including its interface with the application layer. As we are going to show in the following, a QKDN requires a strict integration between the QKD quantum security primitive and a series of conventional preventive mechanisms (in some cases of the latest generation) to guarantee security and reliability adequate to its purpose. When defining the security mechanisms for a QKDN, other factors, apart from the primary one of protecting quantum keys, must be considered. Indeed, neglecting aspects such as performance, the way of using quantum keys, and the network topology could undermine the usability and robustness of the network or even its proper operation.

Two of the crucial parameters for a QKDN are the (average) speed of quantum key generation by its point-to-point QKD links and the maximum length of such links. Significant progress has been made for both over the last twenty years, thanks to more efficient post-processing algorithms and the advances in optical and electronic components, especially for transmission media and receiving devices. However, current quantum key generation rates are tens or hundreds of kilo bits, which are too low if we assume the key stream is used directly for application-level encryption with OTP, except for those specific use cases characterized by such transmission bandwidth values. For instance, recent measurements show that the conventional TLS protocol affects the average throughput and latency of communications by less than 5 percent and 15 percent, respectively, with many Internet communications having speeds above 250 Mbps [55]. As for the maximum length of a point-to-point link, it greatly varies in function of the communication media and QKD protocol type. For wired connections, experiments in the MDI setting broke the limit of 500 km [56,57], but devices on the market currently allow a maximum length of the quantum channel of about one hundred km (e.g., [44,45]).

Another important factor influencing the performance of a QKDN is how the quantum key bits are used. Ideally, we would like to ensure perfect secrecy for all links that transmit secret-key bits and application-level linking (see Figure 2). Indeed, this is the only way to "expand" the security of the QKD protocol to the whole system consisting of the QKDN and the application layer. Since OTP is the most efficient scheme offering perfect secrecy [30], that turns out in encrypting with OTP both the data flow at the application level and those related to quantum key bit transfers between the different components of the QKDN.

As indicated by the red lines in Figure 2, not only the links K2-1 for key delivery (KMA link between two repeaters or between a repeater and the destination node) should be encrypted with OTPs but also the K4 links for the delivery of key bits at the application level and the K1, K3 links for the transfer of key bits between the quantum and key management levels within the same node. This approach would reduce the number of quantum key bits available at the application level by at least one-half, with a considerable degradation in performance. Indeed, half of the bits produced by the QKD module should be considered an OTP key to be put in eXclusive OR (XOR) with the remaining half of the bits that constitute the secret key to be used at the application level. A sketch of this approach in the simplest key relay deployment is illustrated in Figure 3, under the assumption that all the key management operations can be performed on OTP encrypted key bits.

However, the main problem with this solution is not efficiency but security since it poses the following two issues:

1. How to protect the confidentiality of the quantum key bits at their sources, i.e., in the QKD modules;
2. How to keep the OTP keys of the sender and receiver confidential but shareable with their corresponding application layers.

The only plausible solution to the first issue is to imagine a security perimeter enclosing the QKD modules on each node. A "security perimeter" is a physical or logical (or both) splitting of some components, functions, and devices from the "outside world" thanks to access control technologies. It should be clear that a security perimeter allows the "black box" notion of trusted node, as introduced and used in some recommendations, to be translated into concrete implementations.

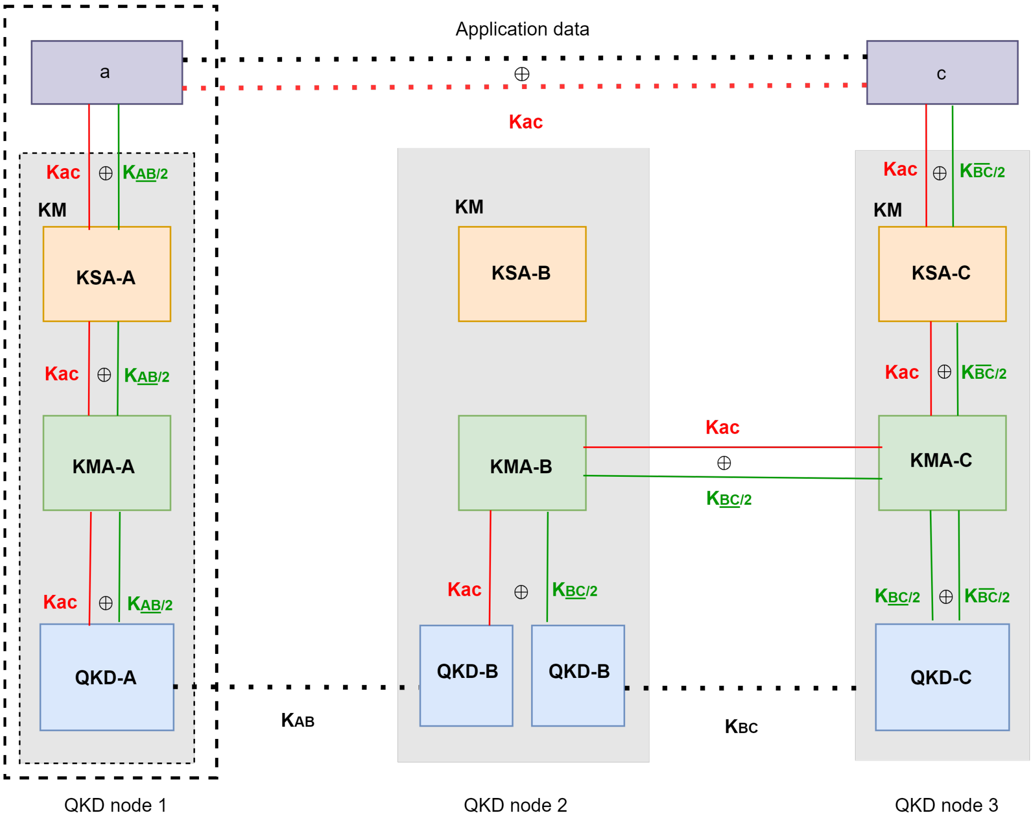

**Figure 3.** A simple example of encrypting all the key bit transmissions with OTP, where $K_{\overline{XY}/2}$ and $K_{\underline{XY}/2}$ denote the first and second half quantum key bits produced by $X$ and $Y$, respectively, and $K_{ac} = K_{\overline{AB}/2}$. The dotted and dashed rectangles enclosing node 1 represent the two kinds of security perimeter assumed for any QKD node in recent recommendations.

The second issue could be solved with an asymmetric key encapsulation mechanism (KEM) [58] between the KSA module and its corresponding application module. However, at present, there are no known asymmetric schemes that offer unconditional security.

An alternative given in recent recommendations by standardization bodies (e.g., [41,42]) is to assume that the QKD, KMA, and KSA modules belong to a single security perimeter and that this perimeter could also include either an application module or a QKDN control module, depending on whether it is a terminal or repeater node. In any case, the fundamental problem of guaranteeing perfect secrecy for quantum key bits remains challenging. Indeed, as we are going to show in the following sections, while the confidentiality and authenticity of the quantum key forwarding process can be guaranteed with unconditional security (cf. Section 6.1), for the establishment of authentication for QKDN devices and users, there are no known approaches that allow this level of security. It follows that, as far as is known from the current state of the art of quantum cryptography, it is only possible to realize QKDN networks that offer conditional (i.e., computational) resistance to quantum cryptanalysis by using post-quantum cryptographic algorithms.

## 6.1. Confidentiality of Quantum Key Relaying

Quantum key relaying is a critical feature for the practical realization of QKDNs. The quantum key bits generated through a QKS link may need to be transmitted to destination nodes not directly linked to the source node or along distances beyond the physical limits imposed by the communication medium and the QKD protocol. Key relaying in QKDNs can be realized in the traditional sender–receiver or sender–sender settings (see

Figure 2). The last is the setting exploited by the MDI protocol and derivatives to avoid trustiness in the relay since, in these protocols, the relay's honesty can be checked through a Bell-state measurement for entanglement swapping [46]. The sender–sender setting allows doubling the maximum distance between two end-points but no more; moreover, it cannot accomplish this for most network topologies. For large-scale QKDNs or multiple hops between communicating nodes, the only possible alternative is the sender–receiver setting, where MDI protocols cannot be adopted, and the relay must have some level of trust. In the following, we will therefore limit our discussion to the confidentiality of quantum key bit transmission in the sender–receiver scenario, using the terms "(quantum) key forwarding" and "repeater (node)" for this specific type of key relaying. We start from the assumption that QKD modules are secure because of their security perimeter (see the previous section), discussing concrete attacks to the key management layer to determine the most appropriate key forwarding scheme without the substantial degradation in throughput of the scheme in Figure 3. Our analysis, based on recent recommendation [42], also serves to understand how much it is necessary to use the notion of security perimeter to obtain a network with adequate levels of security and performance.

A naive approach to the confidentiality of quantum key forwarding is illustrated in Figure 4 (see Figure 6 of [59] for an essentially similar approach in terms of security, but computationally more onerous). The problem, in this case, is that each repeater node must be *fully trusted*, meaning that single read-only access to the node by an adversary may result in the total break of the secret key to be shared between the two end nodes. Indeed, an adversary with read-only access to any of the nodes afferent to one of the forwarding paths can retrieve all the bits of the secret key through an appropriate XOR operation. If, for example, an adversary were able to gain read access to node C of Figure 4, he could infer the bits of key $\boldsymbol{K_{AB}}$ by performing XOR between the bit strings $\boldsymbol{K_{AB}} \oplus \boldsymbol{K_{BC}}$ and $\boldsymbol{K_{BC}} \oplus \boldsymbol{K_{CD}}$, available in C's KMA-C module, and the bit string $\boldsymbol{K_{CD}}$ related to the quantum key that C shares with D. Ideally, an adversary should be able to access the secret bits to be shared between nodes A and D only following direct access to those nodes, whereas in this scheme it can do this by accessing any of the repeaters interposed between A and D. In this case, the risk of the fatal threat of one or more secret keys being acquired by unauthorized third parties, i.e., other than Application A and D, is greater the greater the number of repeaters between A and D. Given the passive nature of the attacks, which makes them difficult to detect, and given the possibility of attacks even from insiders (i.e., authorized personnel) at repeaters, the level of risk is particularly high and not permissible in any of the use cases of a QKDN involving repeater nodes.

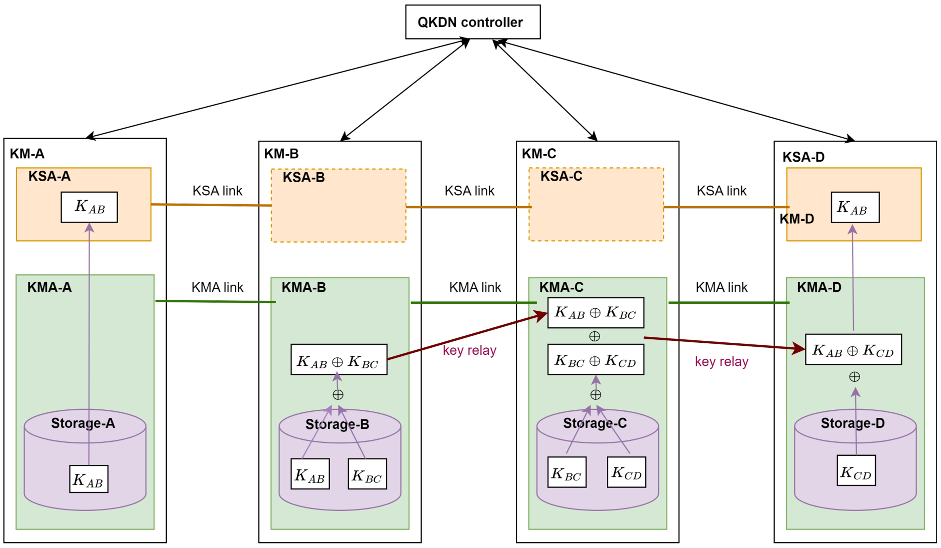

**Figure 4.** A naive approach to quantum key bit forwarding.

A better approach is that illustrated in Figure 5. In this case, the only repeater through which the shared secret key $K_{AB}$ can be inferred is node B succeeding the source node A. In fact, the forwarding path of $K_{AB}$ now involves a direct passage from B to D without the involvement of C (and any other repeaters that may be present between C and D). Therefore, the only nodes to be assumed as fully trusted in the key forwarding path are the source, the destination, and, if present, the first repeater after the source. We should note, however, that the number of fully trusted repeaters may increase if the forwarding between a source and a destination involves alternative paths, which, on the other hand, is a good practice for resilience to failures and mitigation of DoS attacks for QKDNs.

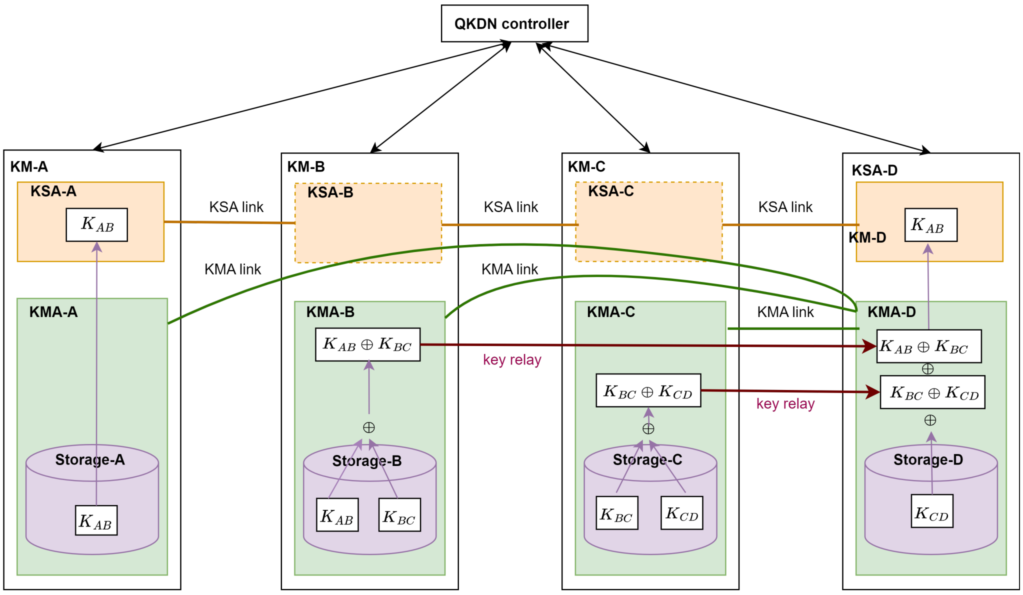

**Figure 5.** Quantum-key bit forwarding through a direct link between the first repeater node and the destination node.

An even better result can be achieved if the topology of the QKDN is changed to provide a centralized key management (KMA) layer expressly dedicated to forwarding operations, as illustrated in Figure 6.

In contrast to the forwarding mechanism proposed in [59], the variant illustrated in Figure 6 is optimal as it requires only the trustiness of the source and destination nodes to access the shared secret, which is evidently the lowest possible level of trust. This approach consists of the following:

- The source A uses a (quantum) random bit generator (RBG) to generate the secret key $K_{RBG}$ to be shared with the destination node D;
- A sends the binary string $K_{RBG} \oplus K_{AB}$ to the centralized KMA; meanwhile, B and C will send, respectively, $K_{AB} \oplus K_{BC}$ and $K_{BC} \oplus K_{CD}$, so that the forwarding KMA can send the binary string $K_{RBG} \oplus K_{CD}$ to the destination D;
- D recovers the secret key $K_{RBG}$ thanks to the operation $K_{RBG} \oplus K_{CD} \oplus K_{CD}$.

With this scheme, an adversary that managed to gain read-only access to one or more of the repeater nodes related to a key forwarding $K_{RBG}$ between A and D would still not be able to gain access to the key. Compared to the previous scheme, the latter also offers simpler management of key forwarding due to the possibility of centrally defining routing paths, although at the price of having to guarantee high levels of integrity and availability for the centralized KMA. It should be noted that the centralized KMA does not have to be a fully trusted node, as read access to the key bit strings managed by it does not allow $K_{RBG}$ to be obtained.

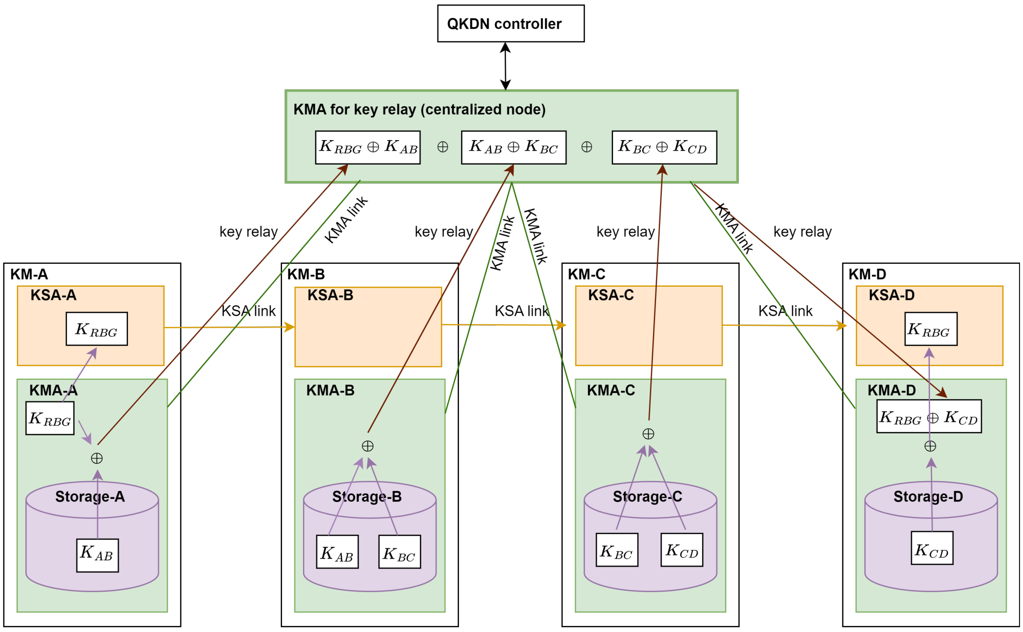

**Figure 6.** An optimal approach for forwarding quantum key bits by using a centralized controller.

Even with this approach, however, the overall level of confidence in the nodes which compose QKDN can be very high, depending on the use cases to which the network is destined. In particular, all the nodes that make up the QKDN must be considered fully trusted if the sharing of secret keys can take place between arbitrary pairs of nodes in the QKDN. More generally, in the context of the use cases provided for the QKDN, at least the nodes where the sharing of secret keys may occur must be fully trusted.

A fully trusted node requires implementing both physical and logical access control mechanisms so to realize a control perimeter able to guarantee that only authorized entities can access, locally or remotely, a particular node and exercise its functions. Clearly, implementing any access control policy will first require appropriate party authentication protocols to get corroborating evidence of the identity of the individuals, devices, or processes requesting access or the execution of an action.

### *6.2. Access Control to the QKDN Nodes*

Access control and authentication procedures are required not only for the fully trusted nodes mentioned in the previous subsection, but also repeater nodes, whose secret-key bit stream is protected by the scheme of Figure 6, should be protected by similar mechanisms. In practice, as we will show in the following, all the nodes of a QKDN must be accessible only by authorized parties, thanks to the creation of an appropriate security perimeter for each of them, whether they are control nodes of the QKDN or nodes involved in the various paths for sharing secret keys.

In a conservative approach to the security of a QKDN, it is appropriate to consider the Dolev–Yao model [60], in which an adversary $\boldsymbol{E}$ can gain complete control of the network: $\boldsymbol{E}$ can listen, intercept, and alter any message and can be limited only by the constraints imposed by the cryptographic methods used for the communication protocols. In such a context, in the absence of an appropriate access control procedure for one of the nodes involved in a secret-key share, $\boldsymbol{E}$ can access the contents of those keys. For example (see Figure 6), $\boldsymbol{E}$ could acquire $\boldsymbol{K_{RBG}}$ by accessing node C and simultaneously observing the communication channels between nodes A and B and the centralized KMA. Indeed, by observing the two channels, $\boldsymbol{E}$ can acquire $\boldsymbol{K_{RBG}} \oplus \boldsymbol{K_{AB}}$ and $\boldsymbol{K_{AB}} \oplus \boldsymbol{K_{BC}}$, while accessing C can allow $\boldsymbol{E}$ to acquire $\boldsymbol{K_{BC}}$, so that $\boldsymbol{E}$ can obtain $\boldsymbol{K_{RBG}}$ by combining the three previous binary strings in XOR.

Storing the keys $\boldsymbol{K_{BC}}$ and $\boldsymbol{K_{CD}}$ in the KMA of C in the form of the cryptogram $\boldsymbol{K_{BC}} \oplus \boldsymbol{K_{CD}}$ reduces both the surface area and the time window of vulnerability of $\boldsymbol{K_{RBG}}$ at the cost of increased complexity in handling key bit streams. However, this does not eliminate the need for a security perimeter on C. Indeed, $\boldsymbol{E}$ could acquire $\boldsymbol{K_{BC}}$ by observing the communication channel on C between the QKD and KMA modules.

In the scheme of Figure 6, as well as in any other key forwarding scheme, the absence of adequate security perimeters on the repeater nodes may result in the reading of secret keys by an adversary $\boldsymbol{E}$ even without listening to any of the network links. Indeed, $\boldsymbol{E}$ can infer $\boldsymbol{K_{RBG}}$ by accessing either the centralized KMA or any of the repeater nodes X between the source and the destination, operating as follows:

- $\boldsymbol{E}$ reads on node X the quantum key shared with the previous repeater;
- $\boldsymbol{E}$ reads on the centralized KMA all the bit strings received from the source node and the repeater nodes which precede X in the path from source to destination;
- $\boldsymbol{E}$ performs the XOR operation between the key acquired on node X and all the bit strings acquired on the centralized KMA.

Thus, implementing access control through a security perimeter on the nodes involved in quantum key bit forwarding is an essential condition to protect the secrecy of keys shared between pairs of nodes in the network. A violation of this type would constitute a vulnerability of grade fatal because it defeats the very purpose of the QKDN.

Ultimately, since an attacker could always read quantum key bits at their sources (i.e., in the QKD modules), our previous analysis shows that the security perimeter of a QKDN node has to enclose at least their QKD, KMA, and KSA modules.

A security perimeter with associated access control is also necessary for all those nodes that are only dedicated to the management of the QKDN, i.e., that exclusively implement control or management modules (QKDN controller, QKDN manager). Access by an $\boldsymbol{E}$ adversary to such a node could indeed lead, as described in Section 4, to serious violations of the quality and continuity of service of the QKDN.

In the next part of this section, we will omit the discussion of physical protection mechanisms since they are beyond the scope of this work, while we will briefly focus on the critical issues related to the implementation of a logical security perimeter for the nodes of a QKDN, i.e., confinement with controlled access for a node's resources and processes through the exclusive use of information technologies. However, it is important to emphasize the need for a kind of multi-level protection in which diverse security controls operate in a complementary and synergic manner to achieve the level of dependability required by critical networks such as QKDNs.

In general, a logical security perimeter makes it possible to regulate and monitor under which circumstances and which entities (persons, processes, devices) may certain actions (read, write, execute, etc.) be exercised on the set of resources inside the perimeter. The creation of a logical perimeter thus provides for the specification of one or more access rules, which constitute the access policy to be enforced. It also requires the implementation of two software modules necessary to exercise that policy: an authentication module and a control module (reference monitor). The authentication module determines the identity of the entity requesting access, while the control module imposes that the (authenticated) entity may only exercise the actions provided by the access policy [28].

Depending on the security perimeter, the control module's implementation occurs at a single host or one or more network devices (e.g., a router acting as security gateway [61]) through an appropriate software interface provided at the application or operating system level. It uses isolation and confinement technologies implemented through appropriate APIs (application programming interfaces), kernel protection [28] features (e.g., process permissions, packet filtering) , and possibly special hardware, whose security is not affected by cryptanalytic techniques. On the other hand, to implement the authentication module, it is necessary to use one or more entity authentication protocols that are susceptible to cryptanalytic attacks as they employ cryptographic mechanisms. This applies in particular to remote login protocols, which exploit authentication procedures based on public key cryptographic schemes. A relevant example of such a protocol is secure shell (SSH), while the transport layer security (TLS) protocol is generally exploited to realize remote login services via web interfaces and web services. The proper functioning of these protocols may also require the support of a public key certificate infrastructure, which will be discussed in more detail in the following.

### *6.3. Mutual Authentication of QKDN Nodes*

The literature on QKDNs often discusses authentication issues just for the classical communication channel between the QKD modules. However, it is essential to emphasize that all the communication channels on which travel the secret-key bits and the control and management information require authentication. Otherwise, it would be hard to readily detect data manipulations by adversaries, resulting in potentially serious anomalies or service disruptions for the QKDN.

The connections between two nodes of a QKDN can be authenticated using a Wegman–Carter-type [62–64] scheme. This solution is often proposed in the literature for authenticating the classical channel between couples of QKD modules; however, it could also be extended to the KMA and KSA links. Message authentication schemes of this type offer unconditional security by using sets of functions with particular properties. However, they require sharing an initial secret key between the two connected nodes. This initial shared secret represents the outcome of a node-to-node authentication process, which is a prerequisite of any cryptographic scheme to protect the communication links between them.

In a static QKDN (i.e., where nodes, links, and key forwarding routing paths are defined once and for all in an initial configuration phase), one can imagine authenticating all links by sharing a secret key through a secure channel external to the QKDN, for each pair of nodes to be connected. For instance, a certified courier service or a secret sharing scheme and some external channels (email, mail, SMS, FTP, etc.) could be used to deliver the key. In these cases, the entity authentication, necessary to identify with proven certainty the two nodes to be connected, is implemented through not (completely) digital procedures that do not require the use of asymmetric cryptographic schemes but for which it is often difficult to accurately quantify the level of security and reliability, as they require at least partial human intervention.

A more scalable and usable approach, suitable for all those use cases where the QKDN may have a variation of nodes or key forwarding paths, is to recur to the core target of public-key cryptography, i.e., entity authentication protocols. Before dwelling on details, it is important to point out that entity authentication cannot be made unconditionally secure, unlike OTP encryption and the message authentication schemes discussed previously. Indeed, no known asymmetrical schemes offer information-theoretic security, neither on a quantum nor a classical basis.

In the following, we will use the term “node authentication” to refer to the “unitary” authentication management for all the communication links related to a QKDN node (i.e., classical channel, KMA, KSA, and application links, plus any channel for logging into the node). While using different protocols and, presumably, different communication ports and supports, these links could be seen as belonging to the same node by exploiting the security perimeter concept discussed in the previous section, for example, by imposing that all their data flows pass through the same security gateway.

The mutual authentication of the nodes of a QKDN is necessary to avoid spoofing attacks [65] in which an unauthorized entity ***E*** interposes itself in the communications between a source and a destination, disguising itself as an authorized party. Referring to Figure 6, ***E*** could, for instance, impersonate the centralized KMA towards one or more QKD nodes, impersonate the destination node D, or impersonate B with A and C simultaneously. Usually, a strategy called “man in the middle” (MiM) [66] is used to carry out a spoofing attack, as it reduces the possibility of discovering the attack. In fact, when performing a spoofing attack, there is always the possibility that the node involved in the identity exchange may encounter interruptions or other anomalies in its communication with the adversary, thus detecting the attack. In the MiM technique, the adversary ***E*** impersonates the counterpart with each of the two nodes in communication so that each believes in communicating with the authorized counterpart. For example, to impersonate the centralized KMA to A, ***E*** can simulate being the KMA with A and being A with the KMA so that both A and the KMA believe they are communicating with the correct counterpart. In the context of QKDN networks, spoofing attacks can be used to obtain access or alter the data flows on network links or to disguise the access control system on network nodes.

### *6.4. QKDN and the Application Layer*

The interactions between the QKDN and the application layer serve to provide the secret quantum key bits and related control information to the applications that need to communicate securely. Two scenarios are possible in this context, depending on whether the security perimeter of a node includes the application stack or not. In the first case (see Figure 3), the confidentiality and integrity of these connections pass on the security perimeter and its access control system. If, on the other hand, the perimeter does not include the application stack, the protection for the aforementioned connections will stem from an entity authentication protocol between the KMA and the cryptographic applications. The requirements and actual implementation for the authentication protocol depends on the QKDN use case; however, as for the authentication between couples of QKDN nodes, we of course have to resort to quantum-safe mechanisms which, at the current state of knowledge, must relay on a (conventional) computational problem supposed to be hard for both conventional and quantum computers.

A concrete implementation when the security perimeter includes the application stack can be achieved thanks to networking devices capable of coordinating key sharing with the KSA. In this respect, Cisco Systems has recently built a protocol called Secure Key Integration Protocol (SKIP) that enables any router supporting encryption to use keys provided by a quantum distribution system (https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html, accessed on 18 October 2023). Using such a router as a security gateway could enforce the security perimeter for a QKDN node and, at the same time, provide security (e.g., access control, packet filtering, cryptographic services) for a co-located network. Furthermore, the router can securely exchange data traffic with other routers by relying on the underlying QKDN, thus realizing quantum-safe routing for the network at the application layer. Depending on the traffic load, data exchanges between the routers can be made unconditionally secure thanks to OTP encryption and Wegman–Carter message authentication. In this case, mutual authentication for the routers is "hard-coded" into the underlying QKDN topology, except at most during network startup, for which an asymmetric scheme may be appropriate. However, it is unrealistic to expect that the quantum key bits provided by the QKDN could be used to unconditionally secure communications between the devices in the network co-located to a router. Even in the hypothesis of having a sufficient number of quantum key bits, the need to secretly distribute these bits between the router and the devices would impose the use of asymmetric schemes.

The use of asymmetric schemes is even more necessary when the security perimeter does not include the application stack. In this case, the KSA will also have to establish mutual authentication with the cryptographic applications. The only case in which we can achieve unconditional security for the communication paths of the application layer network is when each application node falls within the security perimeter of a corresponding node of the QKDN. Provided that physical and logical controls are in place to prevent access to quantum key bits even to the QKDN management personnel, it might also be possible to guarantee perfect secrecy for quantum key bits from source QKD modules up to consumer applications. Even in this case, however, it will be necessary to use quantum-safe asymmetric schemes to log into the nodes remotely.

## 7. Conclusions

The unconditional security of quantum key distribution networks (QKDN) is often assumed by theorists of quantum key transmission protocols without a rigorous cyber security analysis or flaunted as an advertising slogan by market players. In this work, following recent recommendations from standardization bodies, we have conducted a detailed analysis of the QKDN security threats. Based on this analysis, we then carefully evaluated the possible preventive controls to guarantee the maximum level of security for a QKDN. With considerable evidence, this study allowed us to conclude that, at the current state of developments and advances of QKD technology, a QKDN can hardly guarantee information-theoretic security like the QKD primitive. Indeed, every concrete QKDN deployment must provide authentication mechanisms for nodes, users, and applications. It is however important to underline that the authentication lower level of security does not compromise the information-theoretic security provided by QKD protocols. However, although violation of authentication does not compromise previously exchanged keys, at least in the current state of our knowledge, the entity authentication mechanisms require using cryptographic schemes based on the resolution of a conventional (non-quantum) computational problem. In these circumstances, the best that can be done at present is to integrate QKD with cryptographic schemes based on computational problems difficult for both classical and quantum computers. Post-quantum cryptography (PQC) concerns the design and development of public-key schemes based on computational problems for which quantum computers do not seem to offer substantial performance gains over conventional ones. Therefore, the integration between QKD and PQC schemes currently represents the only viable solution on the shorter term for quantum-safe computer networks, including QKDNs.

In 2016 the National Institute of Standards and Technology (NIST) started an evaluation process whose initial goal was to select at least one PQC algorithm realizing a Key Encapsulation Mechanism (KEM) [67] and one PQC algorithm for digital signatures [68]. The NIST selection process should be completed by the end of 2024, with the publication of the first complete draft of the standard. In July 2022, NIST announced that it had selected the first four algorithms to standardize: CRYSTALS-kyber [69] for KEM, and CRYSTAL-Dilithium [70], FALCON [71], and SPHINCS [72] for digital signatures. These and the other algorithms that will form the standard are the results of evaluations that have considered other factors beyond the primary one of security. Performance, implementation costs (in terms of RAM or number of chip gates), and various other characteristics—from the choice of security parameters to the impact in terms of performance on widely used protocols such as TLS, IPsec, and SSH [61]—have been taken into account. These features were subjected to careful analysis and measurements through prototypes implemented by proponents and gradually perfected thanks to interactions with evaluators. Presumably, the definitive standard will contain two or three alternatives for both KEM and digital signatures, based on different approaches to having backups in case of cryptoanalytic breakthroughs.

For QKDNs, KEM may generate an authenticated initial key and trigger message authentication through a Wegman–Carter scheme. The authentication of communicating parties is necessary for any KEM to produce a truly authentic key. It can be achieved through the support of post-quantum public-key infrastructures and certificates, particularly thanks to one of the recent NIST digital signature standards previously cited.

The mainstream in network security consists of assembling multiple security mechanisms into protocol suites that constitute international standards and are implemented in one or more layers of the OSI stack. Thus, we will presumably see integration in QKDNs and related application networks of PQC versions of standards such as TLS, IPsec, and SSH. Table 4 summarizes, in relation to the required functionality, the types of protection and controls that can be used in a QKDN, providing a concise picture of the necessary integration between quantum and post-quantum cryptography.

It is worth remarking that PQC, relying on computational complexity, is likely to provide only a partial and temporary solution to the problem of QKDN security. The underlying concern is that there may exist undiscovered quantum algorithms (or even classical ones) that could potentially compromise the security of these cryptographic systems in the long term. In addition, studies have recently emerged in the literature showing that some

PQC systems are already currently vulnerable (this is the case for SIKE, the instantiation of SIDH that recently advanced to the fourth round of NIST's standardization process) [73]. In contrast, quantum cryptography represents the ultimate solution because it reestablishes security and confidentiality by relying on unbreakable principles of nature. Thus, in order to guarantee the security of QKDNs in the long-term perspective, it is necessary to develop research on QKDNs to avoid relying their security exclusively on PQC solutions. Another limitation of this paper is that the analysis is restricted to the case of point-to-point trusted node QKD networks. We have not considered the case of multi-user networks, in particular those based on entangled states, which are a hot topic currently being tested. A detailed security analysis of these networks would therefore merit a separate discussion, which is outside the scope of this paper, remaining an open issue for possible future work. Finally, a possible experimental development of this work could concern the checking of the security of QKD networks through the implementation of validation tests at various layers.

**Table 4.** Types of protection and preventive security controls that can be used in a QKDN in accordance with the required functionality.

| Functionality | Protection | Preventive Controls |
|---|---|---|
| Local users' access | Physical and logical security perimeters | Physical access control; multi-factor (e.g., passwords and biometric data) logging procedures; access control policies |
| Remote users' access | Post-quantum cryptographic (PQC) protocols for remote access and logical security perimeters | Remote login through PQC extensions of protocols like SSH or TLS; PQC-aware X.509 certificates |
| Key bit forwarding | Mutual authenticated encryption between the QKDN nodes involved in quantum key bit relay | PQC key encapsulation mechanisms (KEM) and PQC-aware X.509 certificates at network startup (possibly via standard protocols like SSH or TLS); Wegman–Carter message authentication schemes and OTP encryption at runtime |
| Key bit storage | File, filesystem, or database encryption with possible use of secure hardware modules (HSM) | XOR encryption or computational symmetric encryption (e.g., AES) with larger keys; storage in HSM |
| Key bit delivery | Mutual authenticated encryption between the QKDN-KSA end-points and cryptographic applications | PQC extensions of protocols like IPSec, SSH, or TLS in function of the use case requirements |

An accurate selection of the conventional mechanisms to be used and their interfacing with the QKD primitive and the entire QKDN network must be defined according to the use cases for which the network is intended and represents an important aspect of the QKDN architecture itself. As a continuation of the present work, we are defining a suite of effective and practical cryptographic schemes to protect the QKDN that will be deployed in the context of the QUANCOM project with respect to its assumed use cases.

**Author Contributions:** Conceptualization, G.S.; methodology, G.S.; writing—original draft preparation, E.L. and G.S.; writing—review and editing, E.L. and G.S.; supervision, G.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was co-funded by European Union - PON Ricerca e Innovazione 2014-2020 FESR /FSC - Project ARS01 00734 QUANCOM - Quantum Systems and Technologies for IT Security in Communication Networks.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** This paper is dedicated to the memory of Giovanni Schmid, a wonderful person and brilliant researcher. The first author is honored to have had the privilege of collaborating with him and to have completed this publication in his memory.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| CC | Common Criteria |
| CIA | Confidentiality, Integrity, Availability |
| ECC | Elliptic Curve Cryptography |
| ETSI | European Telecommunications Standards Institute |
| ITU-T | InternationalTelecommunication Union – Telecommunication |
| KM | Key Management |
| KMA | Key Management Agent |
| KSA | Key Supply Agent |
| MDI-QKD | Measurement-Device-Independent Quantum Key Distribution |
| MOM | Method, Opportunity, Motive |
| NIST | National Institute of Standards and Technology |
| OTP | One-Time Pad |
| PQC | Post-Quantum Cryptography |
| QKD | Quantum Key Distribution |
| QKDN | Quantum Key Distribution Network |
| QRBG | Quantum Random Bit Generator |
| RSA | Rivest–Shamir–Adleman |

## References

1. Mayers, D. Unconditional security in quantum cryptography. *J. ACM (JACM)* **2001**, *48*, 351–406. [CrossRef]
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
3. Qiu, J. Quantum communications leap out of the lab. *Nature* **2014**, *508*, 441–442. [CrossRef] [PubMed]
4. Elliott, C.; Colvin, A.; Pearson, D.; Pikalo, O.; Schlafer, J.; Yeh, H. Current status of the DARPA quantum network. In Proceedings of the Quantum Information and Computation III, Orlando, FL, USA, 28 March–1 April 2015; SPIE: Bellingham, WA, USA, 2005; Volume 5815, pp. 138–149.
5. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
6. Dynes, J.; Wonfor, A.; Tam, W.S.; Sharpe, A.; Takahashi, R.; Lucamarini, M.; Plews, A.; Yuan, Z.; Dixon, A.; Cho, J.; et al. Cambridge quantum network. *NPJ Quantum Inf.* **2019**, *5*, 101. [CrossRef]
7. Choi, T.; Yoon, S.; Kim, T.Y.; Kim, H. Design and Implementation of Quantum Key Distribution Network Control and Management. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 20–22 October 2021; pp. 724–727.
8. Lella, E.; Gatto, A.; Pazienza, A.; Romano, D.; Noviello, P.; Vitulano, F.; Schmid, G. Cryptography in the Quantum Era. In Proceedings of the 2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy, 6–9 June 2022; pp. 1–4.
9. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
10. Diffie, W.; Hellman, M.E. New directions in cryptography. In *Secure Communications and Asymmetric Cryptosystems*; Routledge: London, UK, 2019; pp. 143–180.
11. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
12. Blake, I.; Seroussi, G.; Seroussi, G.; Smart, N. *Elliptic Curves in Cryptography*; Cambridge University Press: Cambridge, UK, 1999; Volume 265.
13. Heron, S. Advanced encryption standard (AES). *Netw. Secur.* **2009**, *2009*, 8–12. [CrossRef]
14. Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-Hashing for Message Authentication, 1997. Available online: https://datatracker.ietf.org/doc/html/rfc2104 (accessed on 18 October 2023).
15. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
16. Sharma, P.; Agrawal, A.; Bhatia, V.; Prakash, S.; Mishra, A.K. Quantum key distribution secured optical networks: A survey. *IEEE Open J. Commun. Soc.* **2021**, *2*, 2049–2083. [CrossRef]
17. Abushgra, A.A. Variations of QKD protocols based on conventional system measurements: A literature review. *Cryptography* **2022**, *6*, 12. [CrossRef]
18. Mangipudi, G.M.; Eswaran, S.; Honnavalli, P.B. Quantum Cryptography and Quantum Key Distribution Protocols: A Survey on the Concepts, Protocols, Current Trends and Open Challenges. *Protoc. Curr. Trends Open Challenges* **2022**. Available online: https://ssrn.com/abstract=4069541 (accessed on 18 October 2023 ).
19. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 4. [CrossRef]

20. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 5. [CrossRef] [PubMed]
21. Arnon-Friedman, R.; Dupuis, F.; Fawzi, O.; Renner, R.; Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.* **2018**, *9*, 459. [CrossRef] [PubMed]
22. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
23. Stucki, D.; Legre, M.; Buntschu, F.; Clausen, B.; Felber, N.; Gisin, N.; Henzen, L.; Junod, P.; Litzistorf, G.; Monbaron, P.; et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **2011**, *13*, 123001. [CrossRef]
24. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef] [PubMed]
25. Martin, V.; Aguado, A.; Salas, P.; Sanz, A.; Brito, J.; Lopez, D.R.; López, V.; Pastor, A.; Folgueira, J.; Brunner, H.; et al. The madrid quantum network: A quantum-classical integrated infrastructure. In *Photonic Networks and Devices*; Optica Publishing Group: Burlingame, CA, UDA, 2019; p. QtW3E-5.
26. Huang, D.; Huang, P.; Li, H.; Wang, T.; Zhou, Y.; Zeng, G. Field demonstration of a continuous-variable quantum key distribution network. *Opt. Lett.* **2016**, *41*, 3511–3514. [CrossRef]
27. Tessinari, R.S.; Bravalheri, A.; Hugues-Salas, E.; Collins, R.; Aktas, D.; Guimaraes, R.S.; Alia, O.; Rarity, J.; Kanellos, G.T.; Nejabati, R.; et al. Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol city 5GUK test network. In Proceedings of the 45th European Conference on Optical Communication (ECOC 2019), Dublin, Ireland, 22–26 September 2019; pp. 1–4.
28. Pfleeger, C.P.; Pfleeger, S.L. *Security in Computing—Fifth Edition*; Prentice Hall: Upper Saddle River, NJ, USA, 2015.
29. Tsai, C.W.; Yang, C.W.; Lin, J.; Chang, Y.C.; Chang, R.S. Quantum key distribution networks: Challenges and future research issues in security. *Appl. Sci.* **2021**, *11*, 3767. [CrossRef]
30. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
31. Hua, X.; Hu, M.; Guo, B. Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State. *Entropy* **2022**, *24*, 841. [CrossRef]
32. Liu, X.; Liu, J.; Xue, R.; Wang, H.; Li, H.; Feng, X.; Liu, F.; Cui, K.; Wang, Z.; You, L.; et al. 40-user fully connected entanglement-based quantum key distribution network without trusted node. *PhotoniX* **2022**, *3*, 2. [CrossRef]
33. NIST-CSRS . Post-Quantum Cryptography Standardization; 2022. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022 (accessed on 18 October 2023).
34. ITU-T. *Study Group (SG) 13: Future Networks and Emerging Network Technologies*; ITU-T: Geneva, Switzerland, 2022. Available online: https://www.itu.int/en/ITU-T/studygroups/2022-2024/13/Pages/default.aspx (accessed on 18 October 2023).
35. ITU-T. *Study Group (SG) 17: Security*; ITU-T: Geneva, Switzerland, 2022. Available online: https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx (accessed on 18 October 2023).
36. *Standard ISO/IEC JTC 1/SC 27*; Information Security, Cybersecurity and Privacy Protection. International Standard Organization: Geneva, Switzerland, 2022.
37. ETSI . *Industry Specification Group (ISG) on Quantum Key Distribution (QKD)*; ETSI: Valbonne , France, 2022. Available online: https://www.etsi.org/committee/1430-qkd (accessed on 18 October 2023).
38. ETSI . Technical Committee (TC) Cyber (Cybersecurity); ETSI: Valbonne , France, 2022. Available online: https://www.etsi.org/committee/cyber (accessed on 18 October 2023).
39. *ITU-T SG 13 Standard itu-t y.3802*; Quantum Key Distribution Networks—Functional Architecture. International Telecommunication Union: Geneva, Switzerland, 2020.
40. *ITU-T SG 13 Standard itu-t y.3800 corrigendum 1*; Overview on Networks Supporting Quantum Key Distribution. International Telecommunication Union: Geneva, Switzerland, 2020.
41. *ITU-T SG 17 Standard itu-t x.1710*; Security Framework for Quantum Key Distribution Networks. International Telecommunication Union: Geneva, Switzerland, 2020.
42. *ITU-T SG 17*; Corrigendum 1—Security Requirements and Measures for Quantum Key Distribution Networks—Key Management. Standard itu-t x.1712. International Telecommunication Union: Geneva, Switzerland, 2022.
43. Sun, S.; Huang, A. A review of security evaluation of practical quantum key distribution system. *Entropy* **2022**, *24*, 260. [CrossRef] [PubMed]
44. ID Quantique. XG Series, 2022. Available online: https://www.idquantique.com/quantum-safe-security/xg-series-qkd/ (accessed on 18 October 2023).
45. Toshiba. *Digital Solutions—Quantum Key Distribution*; Toshiba: Tokyo, Japan, 2022.
46. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 60. [CrossRef]
47. Garcia-Escartin, J.C.; Sajeed, S.; Makarov, V. Attacking quantum key distribution by light injection via ventilation openings. *PLoS ONE* **2020**, *15*, 14. [CrossRef] [PubMed]
48. Kumar, R.; Mazzoncini, F.; Qin, H.; Alléaume, R. Experimental vulnerability analysis of QKD based on attack ratings. *Sci. Rep.* **2021**, *11*, 9564. [CrossRef] [PubMed]

49. *Standard gs qkd 005 v1.1.1*; Security Proofs. European Telecommunications Standards Institute: Valbonne, France, 2010.
50. *Standard gs qkd 008 v1.1.1*; QKD Module Security Specification. European Telecommunications Standards Institute: Valbonne, France, 2010.
51. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA , 2014.
52. CCRA. *The Common Criteria*; CCRA: Lansing, MI, USA, 2022.
53. Katz, J.; Yung, M. Unforgeable encryption and adaptively secure modes of operation. *Fast Softw. Encryption'00* **2000,** , *LNCS vol*, 284–299.
54. Canvel, B.; Hiltgen, A.; Vaudenay, S.; Vuagnoux, M. Password interception in a SSL/TLS channel. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 583–599.
55. Mull, T. Measuring the Performance Impact of TLS Encryption Using TPC-C, 2021. Available online: https://www.yugabyte.com/blog/measuring-the-performance-impact-of-tls-encryption-using-tpcc/ (accessed on 18 October 2023).
56. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
57. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [CrossRef]
58. Beullens, W.; D'Anvers, J.P.; Hulsing, A.; Tania, L.; Panny, L.; de Saint Guilhem, C.; Smart, N. *Post-Quantum Cryptography Current State and Quantum Mitigation*; Technical Report (v.2); European Union Agency for Cybersecurity: Chalandri, Greece, 2021.
59. *ITU-T SG 13 Standard itu-t y.3803*; Quantum Key Distribution networks—Key Management. International Telecommunication Union:Geneva, Switzerland, 2020.
60. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
61. Stallings, W. *Cryptography and Network Security: Principles and Practices—Eighth Edition*; Pearson Education, Inc.: Upper Saddle River, NJ, USA, 2020.
62. Carter, J.L.; Wegman, M.N. Universal classes of hash functions. *J. Comput. Syst. Sci.* **1979**, *18*, 143–154. [CrossRef]
63. Wegman, M.N.; Carter, J.L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, *22*, 265–279. [CrossRef]
64. Siegel, A. On universal classes of extremely random constant-time hash functions. *SIAM J. Comput.* **2004**, *33*, 505–543. [CrossRef]
65. Ehrenkranz, T.; Li, J. On the state of IP spoofing defense. *ACM Trans. Internet Technol. (TOIT)* **2009**, *9*, 1–29. [CrossRef]
66. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2027–2051. [CrossRef]
67. ETSI SG CYBER. *Quantum-Safe Public-Key Encryption and Key Encapsulation*; Technical Report tr 103 823 v1.1.2; European Telecommunications Standards Institute: Valbonne , France, 2021.
68. ETSI SG CYBER. *Quantum-Safe Signatures*; Technical Report tr 103 616 v1.1.1; European Telecommunications Standards Institute: Valbonne, France, 2021.
69. Schwabe, P. Kyber Home, 2020. Available online: https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/03/ (accessed on 18 October 2023).
70. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Dilithium–Algorithm Specifications and Supporting Documentation (Version 3.1), 2021. Available online: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (accessed on 18 October 2023).
71. Fouque, P.A.; Hoffstein, J.; Kirchner, P.; Lyubashevsky, V.; Pornin, T.; Prest, T.; Ricosset, T.; Seiler, G.; Whyte, W.; Zhang, Z. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST's Post-Quantum Cryptography Standardization Process; 2018; Volume 36.
72. Bernstein, D.J.; Hopwood, D.; Hülsing, A.; Lange, T.; Niederhagen, R.; Papachristodoulou, L.; Schneider, M.; Schwabe, P.; Wilcox-O'Hearn, Z. SPHINCS: Practical stateless hash-based signatures. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 368–397.
73. Castryck, W.; Decru, T. An efficient key recovery attack on SIDH. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Cham, Switzerland, 2023; pp. 423–447.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.