Light Quantum Key Distribution Network Security Estimation Tool

Sara Nikula[a], Pekka Koskela[b], Outi-Marja Latvala[c] and Sami Lehtonen[d]
VTT Technical Research Centre of Finland, Finland
{*firstname.lastname*}*@vtt.fi*

Keywords: Quantum Key Distribution, Quantum Key Distribution Network, Light Security Tool, Security Estimation.

Abstract: Quantum key distribution offers a way to create and distribute secure encryption keys based on the laws of quantum physics, which means that these protocols are secure even in the presence of an adversary with unlimited computing power. These keys can be forwarded over several hops in quantum key distribution networks (QKDN). At the moment, any established solutions to assess the security of these networks don't exist. This paper describes a concept of light tool for security status estimation, which provides a holistic estimation of quantum key distribution network systems' security status, especially concentrating in quantum issues that might not arise when assessing classical networks. Our approach is to make high abstraction level questions concerning the status of specific security issues. Rather than providing detailed questions, we try to reach a holistic view of QKDN security, where the questions will also guide the future security development. We present sets of questions which concern different areas of quantum key distribution network security. With the help of these questions, we offer a high-abstraction level tool for estimating the security of quantum key distribution networks.

1 INTRODUCTION

Quantum key distribution (QKD) protocols offer a way for two users, who have an access to a quantum and a classical communication channel, to form and distribute keys securely. These can be used to encrypt the subsequent communication. The quantum channel is needed for transmitting key information in the form of, for example, photon polarization. The main difference to classical key agreement protocols is that the security of QKD protocols is not based on mathematical problems, but rather on the laws of quantum physics, such as the fact that the quantum state of a single photon cannot be cloned. Hence, any attempt to eavesdrop the quantum channel will lead to an increased error rate in the resulting bit string, and thus the communicating parties will be able to infer that something has gone wrong. (Huang et al., 2016; Bennett and Brassard, 2014)

The advantage of utilizing QKD is that its security doesn't depend on the assumed computing power of the potential adversary. This means that it remains as a secure key distribution protocol even though quantum computers are developing rapidly and even if some new mathematical break-throughs would question the security of quantum-resistant key exchange algorithms.

Quantum key distribution protocols are defined as point-to-point interaction between two adjacent nodes. In order to manage and distribute the produced keys in a practical way, these nodes can be connected with each other to form a quantum key distribution network in which keys can be transmitted over several hops. These networks need two types of channels. Quantum channels are used for creating secure keys via quantum key distribution protocols. Classical channels are needed for the post-processing of these keys and for passing control information, which is needed to maintain the network.

For example, we might want to create and transmit secure keys to an application, which would use them for communicating securely with another application over the internet. We would start by creating these keys in a quantum link, using some quantum key distribution protocol. Then, we would create the final secure keys out of the raw bits in the post-processing (also called key distillation) phase, and finally, we would pass these keys forward in the key distribution network to the target applications. Under transmission, the data can be secured by decrypting it in a trusted node and encrypting it again for the next

[a] https://orcid.org/0000-0002-2299-8030
[b] https://orcid.org/0000-0002-2380-2781
[c] https://orcid.org/0000-0001-8083-8986
[d] https://orcid.org/0000-0003-0736-0036

Nikula, S., Koskela, P., Latvala, O. and Lehtonen, S.
Light Quantum Key Distribution Network Security Estimation Tool.
DOI: 10.5220/0012022100003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 587-596
ISBN: 978-989-758-666-8; ISSN: 2184-7711
Copyright © 2023 by SCITEPRESS – Science and Technology Publications, Lda. Under CC license (CC BY-NC-ND 4.0)

hop in some quantum-safe manner, using a key produced in a QKD protocol previously conducted with the next node. (Takahashi et al., 2019; Yu et al., 2017)

General tools to assess the information security status of an organization do exist, e.g., (Kyberturvallisuuskeskus, 2021). There are also well-known frameworks for assessing the maturity of processes or organizations, e.g., Capability Maturity Model (CMM) (Paulk et al., 1993) or Cybersecurity Capability Maturity Model (C2M2) (Christopher et al., 2014). QKD is a relatively new technology that has not yet been utilized in a large scale. At the moment, established solutions to assess the security of a QKDN system do not exist. Existing tools to assess information security of a network may not be sufficiently detailed to be applied to quantum key distribution networks, because these include special infrastructure and protocols deviating from classical networks. This paper aims to provide a tool to estimate the security of a quantum key distribution network specifically. We focus on aspects concerning quantum threat, because quantum key distribution protocols are aimed to be a safe key distribution method even in the presence of a quantum attacker, and assume that classical information security is well implemented. This is because tools to assess classical information security already exist, and covering all classical information security aspects of a network would be redundant. Our tool can be realized for example as a spreadsheet.

In the next section we describe the QKDN architecture. In Section 3 we present our tool. The tool is divided into parts that concentrate on different security aspects of the QKDN. Security of the network is estimated with the help of high abstraction level questions, which help to assess and improve the security of the system. In Section 4 we discuss the strengths, weaknesses and improvement and expansion potential of our tool. Section 5 concludes the paper.

2 QKDN ARCHITECTURE

Quantum key distribution network architecture can be separated into three layers. At the bottom we have the infrastructure layer, which usually consists of a classical and a quantum part integrated with each other, see Figure 1. The classical section consists of routers, servers and classical links, and the quantum section consists of switches, splitters, relays, and quantum links. Above the infrastructure layer is the management and control layer, which is used for orchestration of resources and devices of the QKDN. At the top there is the user and application layer, where the key services of the QKDN are provided and used.

The security of a QKDN can be inspected and estimated by concentrating on different sectors of the system, which together form the holistic security of the whole system. These sectors are discussed more carefully in Section 3. Based on a generic network architecture, Figure 1, the security critical parts can be defined as the security of physical assets, integration, response capability of the system, orchestration and management, and the skills of human resources, see Figure 2. The security level can then be estimated through known vulnerabilities and threats with risk analysis according to the extent of provided services and how critical these services are.

Several international standardisation organisations, such as ITU and ETSI, provide standards and recommendations concerning quantum key distribution protocols, their security levels and their implementation. These standards can be exploited to estimate the maturity level of the security solutions and technology. Appendix gives a brief overview of some of the currently available standards and recommendations concerning QKDNs.

3 ASSESSING THE SECURITY OF QUANTUM KEY DISTRIBUTION NETWORKS

In the following sections, we present nine short sets of questions which enable a security expert to assess security of a QKDN. The sets of questions are divided according to the different sections of the whole system. Each part is covered in its own subsection together with a table of security questions. We have structured the tool so that the answer to a question can be flexibly expressed as a percentage. The 0 and 100 % answers are provided in the tables, and the user compares their system to these extremes to get a result, e.g., ”75% complete”.

3.1 Protocols

Protocols are the main component of the quantum key distribution process. In order to perform quantum key distribution, two kinds of protocols are needed: a quantum protocol, which consists of transmitting the key information in quantum states, and classical protocols, which are needed to extract the classical key material from the quantum information and ensure the security of the process. Quantum protocols can be divided into discrete variable (DV-QKD) protocols, such as BB84 (Bennett and Brassard, 2014) and B92 (Bennett, 1992), and continuous-variable (CV-QKD)

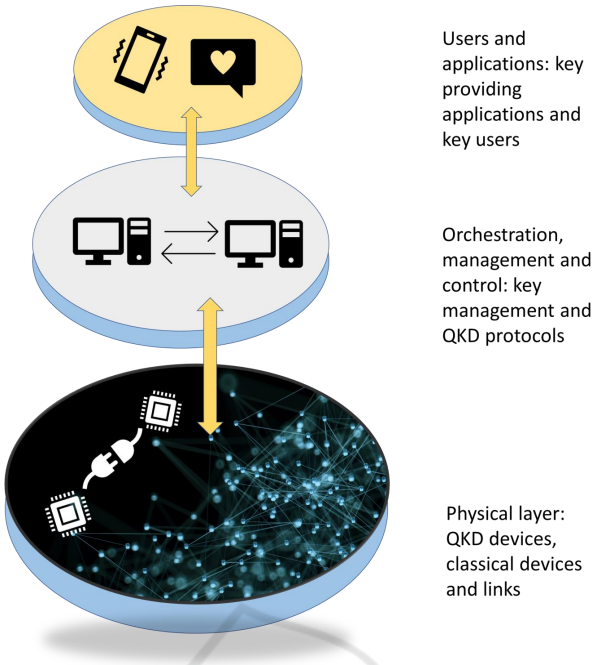

Figure 1: Generic QKD network architecture.

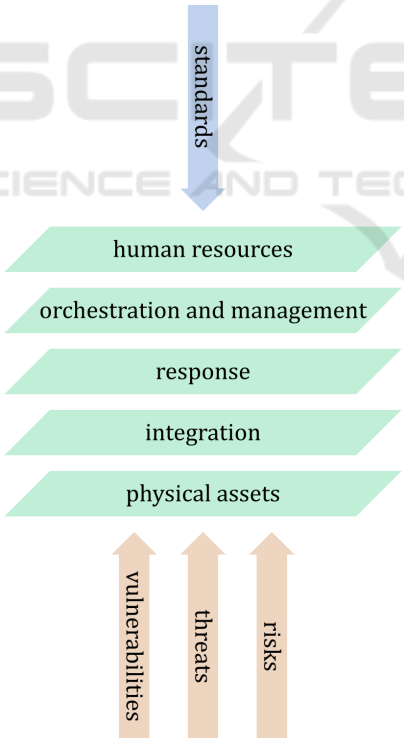

Figure 2: Generic QKD security architecture.

protocols, such as the protocol used in (Huang et al., 2016). These two protocol types differ from each other in their working principles and security proofs, but both are based on utilizing quantum physics for detecting possible attacks. Classical protocols are used for post-processing the data and assessing the error rate of the channel, and they have a significant role in the security of the final secret keys. An example of a classical post-processing protocol is (Brassard and Salvail, 1994).

The security of the used protocols can be assessed with the help of the questions in Table 1.

Table 1: Assessing the security of protocols, answer scale 0–100 %.

Has the quantum security of the used protocols been theoretically proven?
Does the implementation of the protocols comply with quantum theory in such a way that the security of the protocols is maintained?
Do the devices available enable implementing the chosen quantum protocols correctly?
Has the security level of the final secure keys been defined?
Has information leakage during the quantum and classical protocols been taken into account when assessing the security level of these keys?

3.2 Infrastructure

Infrastructure refers to the devices that form a network. In a QKD network, this usually includes classical network devices, such as routers and servers, and

QKD specific devices, such as relays, switches and mirrors (Tayduganov et al., 2021; Arteaga-Díaz et al., 2022). The free space and optical links are similar or same for both classical and quantum side. These devices together form a QKD network. The choice of the used quantum protocol is dependent on the infrastructure. As stated in (ETSI, 2010b), some channel types only allow secure implementation of certain protocols, due to the noise rate of the channel.

Security of the infrastructure should be considered from two viewpoints: for every device individually and for the network infrastructure as a system. The system and devices will have different security threats and vulnerabilities, and they need to be studied separately. Relations and paths between the different components of the network can be assessed. For example, if an attacker has compromised a single device, this will not necessarily threaten the whole system, and the event may stay hidden. But in some cases, access to one device can lead to access to another, more critical, device in the same system. These kinds of paths are depicted as attack graphs in (Wang et al., 2007). In the case of a system wide attack, the impacts may be noticed widely. For example, a successful DDoS attack will cause a slowdown of the operation of the whole system.

Information security, consisting of confidentiality, integrity and authenticity of the data, must be ensured in all parts of the infrastructure. Data must be secured against tampering, and the privileges to see and use the data need to be controlled. This covers all data travelling through the infrastructure, and it can be either control data or data of different services. For example, in trusted relay QKD networks, session keys to be shared are decrypted and re-encrypted at trusted nodes so that they can be securely sent through a classical channel (Yu et al., 2017). This ensures the confidentiality of the data. Similarly, the infrastructure needs to enable ensuring authenticity and integrity of the data.

The information security status of the infrastructure and data can be assessed with the help of the questions in Table 2.

Table 2: Assessing the security of the infrastructure, answer scale 0–100 %.

Is control traffic encrypted with a quantum safe method?
Is data traffic encrypted with a quantum safe method?
Have quantum safe access control and authentication protocols been implemented in the network?
Has the quantum security of individual devices been estimated and tested?
Has the quantum security of the whole infrastructure consisting of these devices been estimated?
Is the estimation method tested or based on some standards?
Are security critical devices placed in such a secured place that they can be considered as trusted nodes?

3.3 Human Capability

QKD networks include devices and protocols, which deviate from classical networks. Supervising the secure functioning of this kind of a system requires knowledge from several different fields: knowledge of physics in order to assess and set up the quantum key distribution infrastructure, knowledge of information security to prepare for possible threats, and knowledge of classical communication and networking infrastructure in order to build and maintain the network.

For the maintainer of a QKDN, this might be a challenge from a personnel point of view. For example, assessing the sufficient signal-noise-ratio of a CV-QKD link requires both knowledge of possible attacks and ability to assess the properties of the quantum link (Huang et al., 2016). Furthermore, (ETSI, 2010c) states that operating QKD related equipment in unsuitable conditions, such as excess humidity or temperature, can increase the failure probability of a device, and this can be a security threat. The personnel in charge of this equipment must be aware of these limitations and requirements. These kind of QKD specific areas of knowledge may be outside the expertise of many specialists otherwise capable of monitoring network security.

The ability to prevent and recover from attacks depends on how well the organization is prepared for the attacks. Preparation includes for example assessing possible threats, training employees, and the everyday security routines and practices. For maintaining this ability, skills of employees and resources for developing these are important. If the organization in charge of the QKDN lacks competent personnel of its own, these human capability resources can also be obtained from third party consultants.

Human capability resources can be assessed with the help of the questions in Table 3.

3.4 Integration to Classical Network

Security assumptions on QKD protocols concentrate on the security of the quantum channel, over which the raw key bits are being transferred. However, if we wish to use the resulting keys in classical communications, it is not enough to guarantee the security of the

Table 3: Assessing the capabilities of human resources, answer scale 0–100 %.

Are secure practices developed and followed?
Is quantum security expertise available whenever needed?
Does this expertise cover all critical areas (quantum specific technologies, information security, classical networking)?
Are human and funding resources sufficient?
Are there means and plans to prevent possible attacks, especially quantum specific?
Has the personnel been trained to act in case of possible attacks?

quantum channel. Because QKDN systems need to have a classical part and they can provide services to classical networks, the integration between the classical section and the quantum section will be one source for attacks and affect the achieved security level of the whole system. This interface between the quantum channel and the classical network is specific to QKD networks, as in classical networks we don't need to do this kind of transition.

Essentially, in QKD, the keys are transferred from quantum signals to classical bits in a sifting process. This depends on the chosen QKD protocol, e.g. (Bennett and Brassard, 2014) or (Bennett, 1992). The sifted key bits are further processed in error correction, using for example LDPC codes (Limei et al., 2020), and privacy amplification, which is meant to enhance the security of the final key (Tang et al., 2019).

In order for the QKD protocol to be secure, a reliable authentication mechanism is needed. QKD protocols are used to distribute secure encryption keys, but authentication of the discussing parties is mandatory to make sure that the keys are being shared with an intended party. Authentication can be either realized through pre-shared keys (Kiktenko et al., 2020) or using a public key infrastructure and digital signatures (Wang et al., 2022). This also means it's a critical intersection between quantum and classical channels, as the signal sent through the quantum channel is authenticated via the classical channel.

Integration to a classical network can be assessed with the help of the questions in Table 4.

3.5 Vulnerability Status

Vulnerability status refers to surveying the possible vulnerabilities in the different parts of the network. Vulnerabilities in a QKD network can arise either from QKD specific protocols and infrastructure or classical software and infrastructure. In some cases,

Table 4: Assessing the integration to a classical network, answer scale 0–100 %.

Have the interfaces between the classical and quantum network been listed?
Have the possible security issues in these interfaces been analyzed?
Has the method used in this analysis been tested or based on some standards?
Is the authentication method used in the post-processing phase of the key bit strings quantum secure?

even though a vulnerability would have been detected in some part of the system, there exists a known fix, which can mitigate the caused threat. According to (Forum of Incident Response and Security Teams, 2019), an official fix, meaning a complete vendor solution, is the most preferable option in these cases.

Deviations between theoretical and practical security are one prominent source of vulnerabilities, as stated in (ETSI, 2010b). Immaturity of the current quantum key distribution technology leads to contradictions between theoretical security and practical implementations of these protocols. Even though discrete variable protocols, such as BB84 (Bennett and Brassard, 2014) and B92 (Bennett, 1992), in theory offer unconditional security, their current physical realizations are still imperfect due to e.g. challenges in emitting only single photon at a time (Lütkenhaus, 1999). This is characteristic for current QKD techniques and should be taken into account when assessing the security of a QKDN, regardless of which protocols are used. Also (ETSI, 2018c) states that deviations between implementation and theoretic security should be assessed and, if possible, reduced.

The vulnerability status can be assessed with the help of the questions in Table 5.

Table 5: Assessing the vulnerability status of the system, answer scale 0–100%.

Is there a list of the main vulnerabilities in the QKD protocols deployed in the network?
Is there a list of the main vulnerabilities in the physical infrastructure of the network from the quantum computing point of view?
Is there a list of the main vulnerabilities in the classical software protocols deployed in the network?
Have these vulnerabilities been further assessed? For example, does exploiting them require some kind of special equipment?
Has the probability of each of these vulnerabilities being exploited been estimated?

3.6 Threat Status

Threat status refers to surveying the possible threats towards the QKDN. (International Telecommunication Union, 2020b) divides threats into three categories: intentional threats posed by a malicious actor, threats caused by administration, and accidental threats. Administrative threats are caused by a failure in administration, and accidental threats result from technical failures. Malicious threats include for example eavesdropping, corruption of data, denial of service attacks or unauthorized physical access to the network.

Maintenance situations can also be a security threat. As stated in (International Telecommunication Union, 2020b), interests and aspirations of operators, users and third parties related to the QKDN should be identified. Also (Kyberturvallisuuskeskus, 2021) states that organizations should be aware of dependencies on suppliers, subcontractors and other relevant third parties, as these can be relevant from information security point of view.

Attacks directed especially towards QKD protocols usually require an access to the physical channel, as in (Shao et al., 2022). Other, software-including parts of the QKDN can possibly be attacked online, without physical access to the device. (Forum of Incident Response and Security Teams, 2019) classifies attacks requiring physical access to the devices as less severe than attacks that can be realized through a network. QKD protocols and their implementations are still under development, and this means that new attacks and vulnerabilities are probable. This is why a list of possible threats needs to be actively maintained and updated.

Survey of security threats can be done, e. g., as in (International Telecommunication Union, 2020b), where the threats are grouped according to whether they threaten confidentiality, integrity or availability of the data, as well as the type of the attack. In QKDN, one of the critical assets are the keys delivered to the client applications. The security of QKD protocols is based on the fact that eavesdropping of the channel can be detected, but it does not provide any means to prevent this kind of attacks; thus availability of keys can be destroyed by disturbing the network. Confidentiality and integrity of the assets can be destroyed by attacks on other, classical, parts of the key management system, where the produced keys are being transmitted and stored. One aspect of threats to availability is the QKDN capacity to provide key material to its users and applications. When the system isn't able to create keys needed anymore very little can be done. The actual need must be measured in advance. High utilization rate might be a vulnerability.

Threat status can be assessed with the help of the questions in Table 6.

Table 6: Assessing the threat status, answer scale 0–100 %.

Have the possible threats towards the QKDN been listed?
Have all protocols, devices and other parts of the QKDN been covered in this list?
Have these threats been further analyzed?
Have the probabilities of these threats been assessed?
Is this list of threats and their probabilities actively maintained and updated?
Have the suppliers and clients associated with the QKDN been reviewed?

3.7 Response Capability of the System

Response capability of the system refers to its ability to detect realized attacks and respond to them. Detection of an attack requires knowledge about possible attacks and means to measure them. For example, in ideally realized classical DV-QKD protocols, eavesdropping of a quantum channel can be detected in an increased error rate (Bennett and Brassard, 2014; Bennett, 1992). On the other hand, some attacks targeted to CV-QKD protocols enable eavesdropping without increasing the error rate (Jouguet et al., 2013). Some attacks only become possible with imperfections or errors in implementation (Pereira et al., 2021). As mentioned in Section 3.2, sometimes the origin of the attack is hard to locate as the effects can be seen in the whole network.

Some of the attacks targeted at QKD protocols are more probable than others. Some are currently hard to realize and thus improbable in practice, but developments in technology can change this. After detecting an attack, the system should be able to respond to it by mitigating further damages and preventing the attacker from gaining access to the rest of the network.

Response capability of the system can be assessed with the help of the questions in Table 7.

3.8 Risk Status

Risk status refers to the role of the QKD network as a key service provider. According to (Kyberturvallisuuskeskus, 2021), the organization should identify critical services it is producing, as well as all infrastructure, devices and processes needed for it. The organization should be aware of how long its customers

Table 7: Assessing the response capability of the system, answer scale 0–100 %.

What is the status of attack and threat analysis, especially in sense of quantum computing?
Do you have tools to detect realized attacks, including quantum specific attacks?
How mature are these tools?
Are these tools justified, i.e., based on reliable research?
Do these tools cover all possible attacks towards the quantum specific parts of QKDN?
Is there networking with other companies or associations having quantum security know-how?
Does the network contain redundancy, enabling the network to recover from possible attacks and continue providing key services?

can survive without these services and have plans for dealing with this kind of disturbance situations.

Defining the risk status of a QKD network does not deviate much from any other kind of a network. QKD networks' function is to provide secure key material for some application domain. Depending on this domain, realization of information security threats can have different impacts. For example, if a QKDN is assumed to provide keys for a critical national infrastructure, a realized threat will have more severe impact than if the QKDN delivers keys for private IoT devices at homes. The risk will also increase if the service is widely used and therefore covers a wide operation or business area. Severity of a risk can be thought of as a combination of its probability and effect, where the effect consists of extent and criticality of impacts.

Risk status can be assessed with the help of the questions in Table 8.

Table 8: Assessing the risks status, answer scale 0–100 %.

Has the main role of the QKDN been assessed?
Which are the main applications using it?
Does the QKDN maintainer have a plan for managing disturbance situations?
Have the possible effects of a realized attack been assessed?
What are the possible worst-case-scenarios if the QKDN is compromised?
How long can the QKDN be out of use before severe damage is caused to the client?

3.9 Management Capability

Management capability refers to resources available for maintaining the information security of the whole QKD network. These resources can include, e.g., employees, devices, and software. Maintaining information security can be viewed as three steps: having a plan, deploying it, and keeping the plan and the deployment up-to-date. New attacks and risks arise continuously, and the plan and the deployment must be updated according to them.

Managing information security of an organization has been covered in several papers and guidelines. (Kyberturvallisuuskeskus, 2021) refers to it as an information security strategy or information security program. (International Telecommunication Union, 2020a) provides a detailed description of a recommendation for information security management process. Management of information security of a QKDN does not differ much from other organizations, as it mostly covers the practices in the organization and is less dependent on the detailed infrastructure deployed. It can be based on the risks and threats status defined in the previous sections, which also cover the QKDN infrastructure in more detail.

Management state can be assessed with the help of the questions in Table 9.

Table 9: Assessing the management of the system, answer scale 0–100 %.

Is there a plan for maintaining the information security of the QKDN, which also takes into account the development of quantum computing?
Has the information security maintenance plan been designed according to the risk status of the network?
Has the information security maintenance plan been designed according to the threat status of the network?
Is this plan deployed?
Is this plan and its deployment continuously updated according to new emerging threats and attacks, especially due to quantum computing development?

4 DISCUSSION

In the current form, our network security assessment tool does not specify details of the concerned quantum key distribution network. The advantage of this approach is that this tool serves as a simple general-purpose tool to guide security work for dif-

ferent types of QKD networks, regardless of their detailed infrastructure or organization behind the network. QKDN technology is still being developed and more advanced attacks against QKD protocols are being found, therefore it is impossible to cover all possible security issues in QKDNs. However, our approach can point out main shortages in security and guide the development work of network maintainers.

The strength of using high abstraction level questions rather than gathering every possible detailed question makes our tool lightweight and time saving. In spite of this, it covers many security topics and can guide the security work to the right direction. The downside of this approach is that some security aspects, which are not explicitly addressed, may remain unnoticed. Security experts should be used to produce answers to these questions, widening the coverage in each security aspect and thus tackling the challenge of possibly implicit issues. The enclosed paper presents answers in a table format but also other kinds of user interfaces could be considered, e.g. slide bars.

In the future, our tool can be made more accurate by defining more detailed questions per different QKD solutions and technologies. Doing so without the trade off of losing simplicity of performing the security estimation is a research topic. These questions would address the low-level implementation of the network, security practices, possible threats and other aspects addressed in this paper. The low-level implementation questions could be grouped according to the infrastructure type, QKD protocol and technologies, intended use cases of the distributed keys, and so on. The proposed approach could also be part of a security standard, providing a formal way to define security level of a system. The question patterns could also be developed further for more careful consideration and definition by adding weight of questions.

Regardless of the detailed structure of the questions used in analyzing the security level of a network, it is important to document the results and use the same questions and measurement methods in the future. This ensures repeatability and enables to track the development of the information security status of the QKDN over time.

5 CONCLUSIONS

Quantum key distribution networks offer a way to deliver cryptographic keys in a secure way even in the era of quantum computers. However, at the moment no established solutions for assessing the security of this kind of networks exist. Here we have introduced an approach to assess the security of quantum key distribution networks with our lightweight tool. Our method is to divide the network security in different domains, which are examined separately with the help of a set of high-level questions. By answering these questions, the network maintainer creates a view of the security level of the network, as well as information on how to enhance it further. In the future, the tool can be developed further by adding more detailed technical specific low-level questions about the different domains presented in this paper. However, adding accuracy leads to balancing between simple-lightweight and accurate-complex with the trade off of losing some simplicity and thus making the tool more time consuming.

REFERENCES

Arteaga-Díaz, P., Denisenko, N., and Fernandez, V. (2022). Modeling the effect of steering mirrors on polarization for free-space quantum key distribution. *Optik*, 265:169434.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

Brassard, G. and Salvail, L. (1994). Secret-Key Reconciliation by Public Discussion. In Helleseth, T., editor, *Advances in Cryptology — EUROCRYPT '93*, pages 410–423, Berlin, Heidelberg. Springer Berlin Heidelberg.

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., and Dolan, T. (2014). Cybersecurity capability maturity model (C2M2). *Department of Homeland Security*, pages 1–76.

ETSI (2010a). ETSI GS QKD 002 V1.1.1 (2010-06) - Quantum Key Distribution; Use Cases.

ETSI (2010b). ETSI GS QKD 005 V1.1.1 (2010-12) - Quantum Key Distribution (QKD); Security Proofs.

ETSI (2010c). ETSI GS QKD 008 V1.1.1 (2010-12) - Quantum Key Distribution (QKD); QKD Module Security Specification.

ETSI (2016). ETSI GS QKD 011 V1.1.1 (2016-05) - Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems.

ETSI (2018a). ETSI GR QKD 003 V2.1.1 (2018-03) - Quantum Key Distribution (QKD); Components and Internal Interfaces.

ETSI (2018b). ETSI GR QKD 007 V1.1.1 (2018-12) - Quantum Key Distribution (QKD); Vocabulary.

ETSI (2018c). Implementation Security of Quantum Cryptography - Introduction, challenges, solutions.

ETSI (2019a). ETSI GS QKD 012 V1.1.1 (2019-02) - Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment.

ETSI (2019b). ETSI GS QKD 014 V1.1.1 (2019-02) - Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.

ETSI (2020). ETSI GS QKD 004 V2.1.1 (2020-08) - Quantum Key Distribution (QKD); Application Interface.

ETSI (2022a). ETSI GS QKD 015 V2.1.1 (2022-04) - Quantum Key Distribution (QKD); Control Interface for Software Defined Networks.

ETSI (2022b). ETSI GS QKD 018 V1.1.1 (2022-04) - Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks.

Forum of Incident Response and Security Teams (2019). Common Vulnerability Scoring System SIG. https://www.first.org/cvss/. Accessed 1.2.2023.

Huang, D., Huang, P., Lin, D., and Zeng, G. (2016). Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports, 6*.

International Telecommunication Union (2020a). Information security management processes for telecommunication organizations. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14044. Accessed 1.2.2023.

International Telecommunication Union (2020b). Security framework for quantum key distribution networks. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14452. Accessed 1.2.2023.

Jouguet, P., Kunz-Jacques, S., and Diamanti, E. (2013). Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A*, 87(6):062313.

Kiktenko, E., Malyshev, A., Gavreev, M., Bozhedarov, A., Pozhar, N., Anufriev, M., and Fedorov, A. (2020). Lightweight Authentication for Quantum Key Distribution. *IEEE Transactions on Information Theory*, PP:1–1.

Kyberturvallisuuskeskus (2021). Kybermittari. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter. Accessed 1.2.2023.

Limei, G., Qi, R., Jin, D., and Huang, D. (2020). QKD Iterative Information Reconciliation Based on LDPC Codes. *International Journal of Theoretical Physics*, 59:1717–1729.

Lütkenhaus, N. (1999). Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61.

Paulk, M. C., Curtis, B., Chrissis, M. B., and Weber, C. V. (1993). Capability maturity model for software, version 1.1. software engineering institute. Technical report, CMU/SEI-93-TR-24, DTIC Number ADA263403.

Pereira, D., Almeida, M., Facão, M., Pinto, A. N., and Silva, N. A. (2021). Impact of receiver imbalances on the security of continuous variables quantum key distribution. *EPJ Quantum Technology*, 8(1):1–12.

Pitwon, R. and Lee, B. H. (2021). Harmonising international standards to promote commercial adoption of quantum technologies. In *Quantum Technology: Driving Commercialisation of an Enabling Science II*, volume 11881, pages 53–62. SPIE.

Quantum Internet Research Group RG (2020). Quantum internet research group charter. https://datatracker.ietf.org/doc/charter-irtf-qirg/. Accessed 1.2.2023.

Shao, Y., Pan, Y., Wang, H., Pi, Y., Li, Y., Ma, L., Zhang, Y., Huang, W., and Xu, B. (2022). Polarization Attack on Continuous-Variable Quantum Key Distribution with a Local Local Oscillator. *Entropy*, 24(7):992.

Takahashi, R., Tanizawa, Y., and Dixon, A. (2019). A high-speed key management method for quantum key distribution network. *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 437–442.

Tang, B.-Y., Liu, B., Zhai, Y.-P., Wu, C.-Q., and Yu, W.-R. (2019). High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution. *Scientific Reports*, 9.

Tayduganov, A., Rodimin, V., Kiktenko, E. O., Kurochkin, V., Krivoshein, E., Khanenkov, S., Usova, V., Stefanenko, L., Kurochkin, Y., and Fedorov, A. (2021). Optimizing the deployment of quantum key distribution switch-based networks. *OPTICS EXPRESS, 29(16)*, 29(16):24884–24898.

Wang, L., Singhal, A., and Jajodia, S. (2007). Toward measuring network security using attack graphs. In *Proceedings of the 2007 ACM workshop on Quality of protection*, pages 49–54.

Wang, L.-J., Zhou, Y.-Y., Yin, J.-M., and Chen, Q. (2022). Authentication of quantum key distribution with post-quantum cryptography and replay attacks.

Working Group Quantum-safe Security. Cloud security alliance. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/. Accessed 1.2.2023.

Yu, W., Zhao, B., and Yan, Z. (2017). Software defined quantum key distribution network. *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pages 1293–1297.

APPENDIX

An overview of the mainstream international standardisation organisations and groups (ITU, ISO, IEC, CENELEC, IEEE, and ETSI) developing standards for quantum technologies is provided in (Pitwon and Lee, 2021). They also identify the areas where the standards will have the highest relevance without impeding future innovations. Although the standards and recommendations published by the different organizations discuss the same theme, they present slightly different views of the structures and main elements of quantum key distribution networks.

ITU-T

Recommendation ITU-T X.1710 provides a security framework to identify and mitigate security issues in quantum key distribution networks. The recommendation only considers intentional threats posed by malicious actors. Thus, security threats caused inadvertently by users or administrators are not covered. (International Telecommunication Union, 2020b)

According to ITU, the main information assets of QKDN are secure key data i.e. random bit strings, data related to key management, and data related to control and management information of QKDN. The functional elements of QKDN are divided into the following parts: QKD modules, which generate the keys; links i.e. classical and quantum channels between the QKD modules; key management nodes; QKDN controllers; and QKDN managers. For each part of the QKDN, the following threats are identified: deletion/corruption of data, eavesdropping, denial of service, spoofing, repudiation, and unauthorized physical access. This recommendation does not cover QKD protocol specific attacks or attacks towards the post-processing phase. (International Telecommunication Union, 2020b)

ETSI

ETSI provides many standards covering security of QKD systems. These standards include the following topics: interfaces (ETSI, 2022b; ETSI, 2022a; ETSI, 2020); communication protocols for QKD networks for supplying cryptographic keys to applications (ETSI, 2019b); main communication resources and arhcitectures related to fiber optical QKD networks (ETSI, 2019a); characterisations and specifications of optical components in QKD systems (ETSI, 2016); application scenarios of QKD (ETSI, 2010a); vocabulary (ETSI, 2018b); common components and interfaces in QKD systems (ETSI, 2018a); security requirements for QKD modules and reference for evaluating the security of practical quantum key distribution systems (ETSI, 2010b).

QKD Module Security Specification of ETSI (ETSI, 2010c) specifies security requirements for QKD modules. Complying with these requirements aims to ensure that the system will with high probability notice potential attacks via physical channels. The document specifies a secure physical structure of a single QKD module, interfaces which enable communication with the other parts of the system, requirements for software used in the module, provided security services, other provided services, and authentication of operators for controlling access to the module.

Security Proofs document of ETSI (ETSI, 2010b) classifies QKD devices after the security levels achievable to them and clarifies their possible roles in a larger system. Theoretical security refers to the mathematical security proofs of the protocols, whereas practical security refers to the implementation of these protocols.

IETF

The Internet Engineering Task Force (IETF) has a working group called ”Quantum Internet Research Group” (QIRG). The goal of QIRG is to study and find solutions on designing and building quantum networks. Its research topics involve routing, resource allocation, connection establishment, interoperability, security and API design. One of the key focus areas in the field of quantum networks will be cryptographic functions, such as quantum key distribution or quantum byzantine agreement. At the moment, QIRG has not yet provided any proposal for internet standards, i.e. RFC (Request for Comments), concerning quantum internet. (Quantum Internet Research Group RG, 2020)

CSA

Quantum-safe Security working group of CSA (Cloud Security Alliance) aims to support the cryptography community in the development and deployment of a quantum-safe framework to protect data, whether in movement or at rest (Working Group Quantum-safe Security,). The group has not yet provided any standards.