31-01-2024

QKD Concepts and Considerations

Grant Agreement No.:	101100680
Work Package:	WP6
Task Item:	Task 1
Nature of Document:	White Paper
Dissemination Level:	PU (Public)
Lead Partner:	FAU/DFN
Document ID:	GN5-1-23-FB1864

Authors:	Susanne Naegele-Jackson (FAU/DFN), Eduardo Jacob (EHU), Ane Sanz (EHU), Ilias Papastamatiou (GRNET), Piotr Rydlichowski (PSNC), Josef Vojtech (CESNET), Elisabeth Andriantsarazo (CESNET), Marija Emso (CARNET), Janos Mohacsi (KIFÜ), Andor Jeszenszky (KIFÜ), Peter Kaufmann (DFN), Ivana Golub (PSNC), Aleksandar Garcevic (AMRES), Pavle Vuletic (AMRES)

Abstract

This document provides National Research and Education Networks (NRENs) in the GÉANT community with an overview of current issues related to Quantum Key Distribution (QKD), describing state-of-the-art solutions and ongoing technological challenges.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document provides National Research and Education Networks (NRENs) in the GÉANT community with an overview of current issues related to Quantum Key Distribution (QKD). General considerations, such as standardisation, interoperability, and operational aspects related to equipment are discussed, helping NRENs who are contemplating implementing a QKD network decide if this is right for them.

Further context to aid with this decision is provided by a look at projects and initiatives in the GÉANT Community that already have some experience with QKD implementations, and by a review of the issues and requirements of trusted nodes, as well as general security considerations regarding QKD.

The document serves as a summary and is intended to help the reader get a fast understanding of the current state-of-the art of this technology and related issues and concerns.

1 Introduction

Quantum Key Distribution (QKD) is generally expected to be the first major application of quantum communication for secure transmissions. QKD is based on the basic principles of quantum mechanics and can deliver secure transmissions through quantum-based key exchange. However, to date, this requires special and expensive hardware and there are many concerns regarding the standardisation and certification of new QKD protocols and QKD equipment.

This document provides an overview of current issues related to QKD, and discusses theoretical considerations, for example, QKD versus Post Quantum Cryptography (PQC), and the latest standardisations and recommendations, as well as practical aspects of QKD networks, ranging from interoperability of hardware and device monitoring to considerations of what could constitute a trusted node in a QKD network. QKD projects and initiatives in EuroQCI are also presented, along with several national QKD projects supported by a number of NRENs. The document also explores the challenges of device implementations and shows why there is a need for device certification.

Any network provider who contemplates implementing a QKD network usually has the following questions:

- Should funds be allocated for this hardware, or do Post Quantum Cryptography algorithms provide sufficient security?
- Is bought equipment standardised and certified? Are there issues concerning hardware interoperability?
- How can QKD networks be monitored and operated?
- Who has already implemented QKD networks?
- How can I define a trusted node in my network?
- How can I monitor and operate QKD networks?
- Why do devices still need to be certified even though QKD is information-theoretic secure technology?

This document aims to answer all of these questions from a current perspective:

- Section 2 discusses general considerations, such as standardisation, interoperability and operational aspects related to equipment.
- Section 3 provides an overview of European initiatives or national projects that implement QKD networks.
- Section 4 discusses issues surrounding trusted nodes and their physical requirements, but also availability and authentication requirements.
- Section 5 details security issues and related equipment certification.
- Section 6 provides conclusions and next steps.

2 General Aspects for Deployment and Implementation

2.1 An Introduction to QKD Networks

Quantum Key Distribution is a point-to-point technology, and a QKD network (QKDN) enables the creation of a chain of QKD links and the exchange of keys between any two designated (point-to-point) QKD nodes in the network. A QKD link is a physical channel that is based on the principles of quantum mechanics and is used for generating quantum keys, and together with the pair of QKD modules it connects (sender and receiver), it forms the fundamental building block of a QKDN.

A multi-point QKD or a QKD network requires additional components: the use of trusted repeating, and optical switches or passive splitters (Figure 2.1) [TAN-2019]. Optical switches and splitters enable the connection of multiple nodes without the risk of compromising confidential data. This provides greater flexibility in determining their physical location within the network, as they are not required to be located within a trusted node. However, a disadvantage is that they introduce signal attenuation on the link of several decibel (dB).

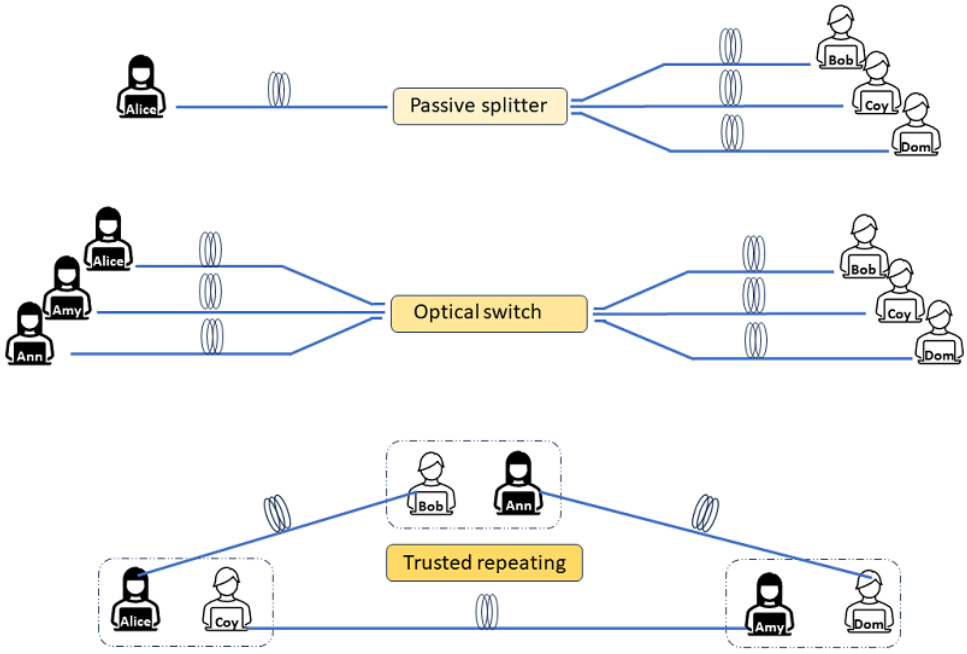

Figure 2.1: Using passive splitters, optical switches or trusted repeating to implement a multi-point QKD network

Trusted relaying involves the exchange of keys between two remote QKD nodes through multiple trusted nodes. The path between the receiver and transmitter is determined, and the required number of keys, generated on the QKD links along that path, is requested. After that, the keys are sent through encrypted channels, and it is essential for each node where encryption/decryption is performed to be a trusted node [MEH-2021].

The functionality of a QKDN is divided into the following layers (Figure 2.2) [ITU-2019]:

- Quantum layer
- Key management layer
- QKDN control layer

Each node contains a QKD module (QKD RX/TX) and a Key Manager (KM). When it is necessary to provide a key to the service layer for the purposes of encrypting a certain channel, the cryptographic application requests a key from the QKD system, the KM retrieves the key from memory and forwards it to the cryptographic application. There is a clear demarcation line between the user network and application in the service layer that requests the key and the functionalities performed below the service layer which are all under the responsibility of the QKDN.

Each QKD module on the physical quantum link sends a random bit sequence to the KM within the same node. The KM then stores these keys in memory (key store) or makes the keys available to the application. If there is a need to transmit a key to a remote QKD node, the QKDN controller determines the route, before the keys are encrypted using KM and transmitted via KM links. In addition to managing routes, the QKDN controller is responsible for controlling KM links and QKD links, overseeing various processes, and ensuring compliance with policies. The QKD manager is responsible for monitoring and managing all QKD nodes and QKD links within the QKDN. It monitors the performance of the QKDN and manages security aspects.

In the quantum layer, where the QKD link is established between two trusted nodes (QKD modules), this can be achieved by using several different technologies (QKD, TF-QKD, etc.) or QKD protocols (BB84, COW, etc.). It is, for example, possible to create a QKD link between nodes 1 and 2 using the BB84 protocol, and a QKD link between nodes 2 and 3 using the Coherent One-Way (COW) protocol [LAV-2022].

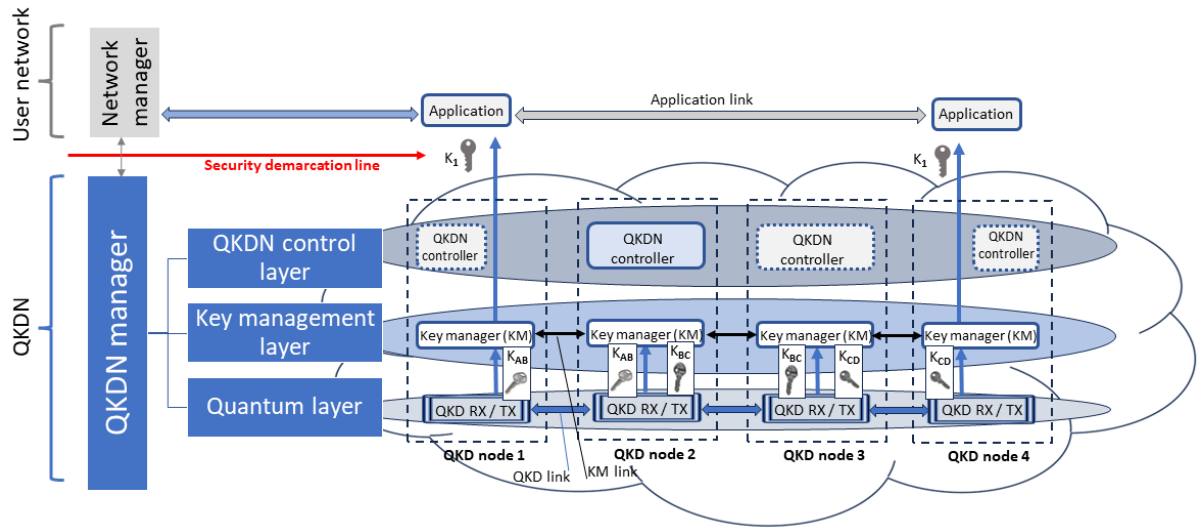

Figure 2.2: Layered structure of a user network and QKDN

More information on the various QKD technologies can be found in Section 5.

2.2 QKD or PQC

Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) are two different approaches that can be used to ensure the security of information in the quantum computing era. As Quantum Computing is expected to break RSA and ECC in the near future, a new breed of quantum secure algorithms to sign and exchange keys, referred to as PQC, are being developed. Quantum Key Distribution makes it possible to exchange symmetric keys without relying on public key algorithms, whether they are traditional or quantum safe. Both technologies have become crucial in the field of security and cryptography, and, due to their great potential and the interest they generate, they are actively researched and developed. However, although both are considered mechanisms that ensure quantum-safe security, it is important to highlight their similarities and differences to determine which approach is better suited to each scenario.

QKD is a technology for securely distributing cryptographic keys between two parties using the principles of quantum mechanics. It relies on the fact that measuring a quantum state changes it, so that any attempt of an eavesdropper to intercept the key can be automatically detected. Therefore, the main advantage of QKD is that it provides a highly secure method for key distribution, ensuring that the generated keys are secure and have not been eavesdropped.

PQC, on the other hand, is a type of cryptography designed to be secure against attacks performed by quantum computers, which are expected to be able to break traditional cryptographic algorithms in the short to medium term future. PQC algorithms usually rely on mathematical problems that are thought to be difficult to solve even for quantum computers. Examples of these algorithms include lattice-based cryptography, code-based cryptography, and hash-based cryptography [KUM-2020], [BER-2017]. One of the main advantages of PQC is that it is compatible with existing infrastructures and it does not require specialised hardware, making implementation easier. In this context, the implementation of PQC algorithms does not exclude the use of traditional ones such as RSA or ECC, since the integration of both is compatible and provides an extra layer of security against quantum attacks.

Considering the main characteristics of QKD and PQC, although they are both aimed at enabling quantum-safe communications, Table 2.1 summarises the strengths and weaknesses of each approach.

	Quantum Key Distribution (QKD)	Post-Quantum Cryptography (PQC)
Strengths	Highly secure method of key distribution.	Provides an extra layer of security against quantum-computing attacks.
	Intercepting the key without detection is theoretically impossible.	Software-based, it does not require specialised hardware or new infrastructure. This reduces the implementation cost.
Weaknesses	Requires specialised hardware and new infrastructures. This results in a higher cost.	PQC algorithms are still under development and in the standardisation process.
	Reduced scalability and limited range. In order to reach long distances or complex topologies, trusted nodes are required.	Some PQC algorithms may be less efficient than traditional algorithms.

Table 2.1: Comparison of QKD and PQC

As both QKD and PQC have their own strengths and weaknesses, the choice between the two depends on the specific requirements and characteristics of each use case. Several factors should be taken into account before selecting the most appropriate technology for designing the solution, such as the complexity and cost of the implementation, the integration compatibility with existing infrastructures, and the required security level.

However, it may not always be necessary to select only one of the technologies. Solutions based on the combination of QKD and PQC present themselves as a novel and promising approach in the field of quantum-safe security. QKD and PQC can be combined in different ways for multiple purposes. Examples of such hybrid solutions include the use of QKD keys to generate and distribute the keys that are then used by PQC algorithms, or the use of PQC-based digital signatures to enhance the authentication process on QKD devices [DOW-2020; YAV-2022; YAN-2021; WAN-2021].

The development of hybrid solutions that combine both QKD and PQC is an area that holds great promise, and it is currently under active research and development. As there are many challenges regarding the implementation and the integration of these technologies, the ongoing research is crucial to enable the development of effective and secure new solutions.

In view of the activities of the European Quantum Communication Infrastructure (EuroQCI), how to efficiently connect QKD and PQC infrastructures in order to provide complete solutions is particularly interesting. Some NRENs participated in activities focused on such matters through the OpenQKD project. The infrastructure presented in Figure 2.3 [YAV-2022] was prepared and tested as a proof of concept [RYD-2022].

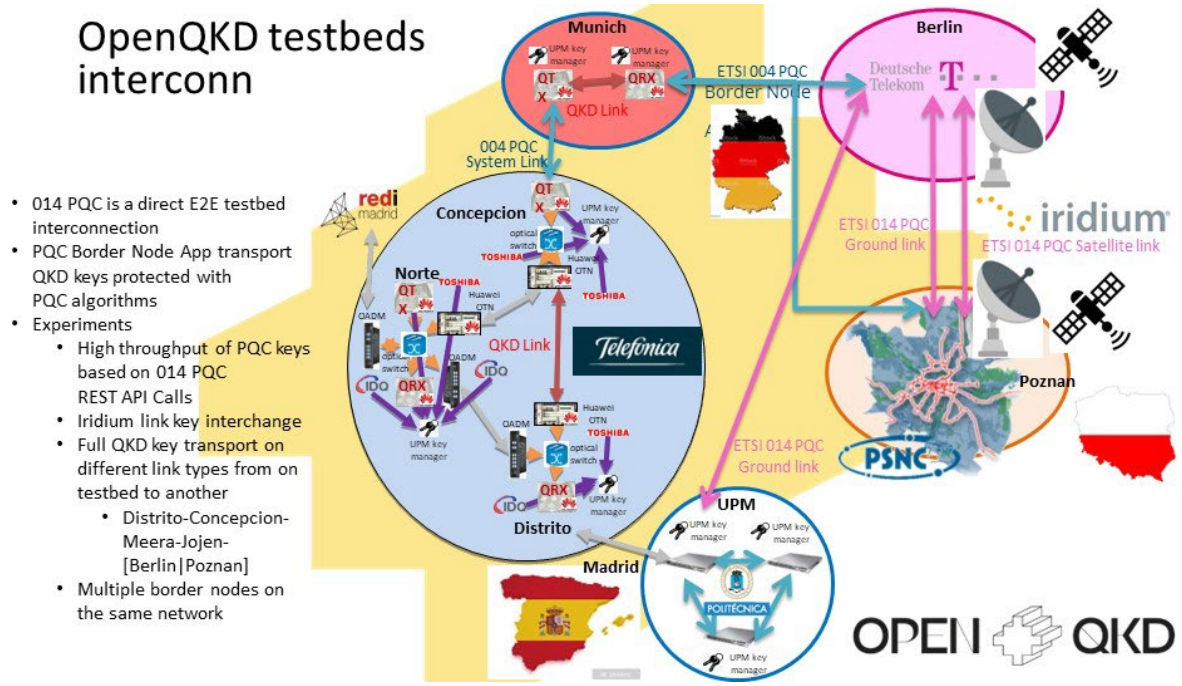

Figure 2.3: Proposed QKD and PQC integration using OpenQKD testbeds

2.3 Standardisation and Certification

In recent years, QKD has emerged as a leading technology in the field of quantum-safe communications. The growing interest from various countries, public authorities, and private sector organisations has led to an increasing number of QKD-based implementations, resulting in the technology evolving very quickly. Consequently, the need for standardisation is crucial to ensure interoperability, reliability, and the security of these implemented systems. Standards play a vital role in facilitating the interoperability of QKD systems, enabling their integration into existing infrastructures, establishing proper interfaces between different components, and ensuring compliance with specified requirements regarding performance and security. Therefore, QKD standards help to reduce the complexity of implementations and promote broader adoption of the technology.

Several standardisation bodies are actively involved in the development of QKD-related topics, resulting in the publication of some standards and ongoing efforts that are part of the standardisation roadmap. Among these bodies, the European Telecommunications Standards Institute (ETSI) has made significant progress in the development of QKD standards through its Industry Specification Group (ISG) on QKD [ETSI-ISG-QKD]. ETSI aims to address standardisation issues related to QKD with the active collaboration of key stakeholders from the scientific, industrial, and commercial sectors. It has already published several standards that focus on areas such as use cases, interfaces, implementation requirements and component characterisation. In addition, ETSI is working on standards that are expected to be published in the upcoming months. The tables below summarise all available ETSI standards, including those under development at the moment, sorted by publication date, along with their objectives and key contents.

Identification	Title	Date published	Description
GS QKD 002	QKD; Use Cases	2010-06 (V1.1.1)	Application scenarios and description of different identified use cases.
GS QKD 008	QKD; QKD Module Security Specification	2010-12 (V1.1.1)	Definition of functional security objectives: security requirements, module specification, ports and interfaces, roles, software security, physical security, etc.
GS QKD 005	QKD; Security Proofs	2010-12 (V1.1.1)	Requirements and evaluation criteria for practical evaluation of QKD systems.
GS QKD 011	QKD; Component characterization: characterising optical components for QKD systems	2016-05 (V1.1.1)	Specifications and procedures for the characterisation of optical components for use in QKD systems, including examples of specific tests and procedures.
GS QKD 003	QKD; Components and Internal Interfaces	2018-03 (V2.1.1)	Definition of properties of components and internal interfaces of QKD systems, including quantum physical devices and classical equipment present in most QKD systems.

Identification	Title	Date published	Description
GR QKD 007	QKD; Vocabulary	2018-12 (V1.1.1)	Definitions and abbreviations used in relation to QKD and ETSI ISG-QKD documents.
GS QKD 014	QKD; Protocol and data format of REST-based key delivery API	2019-02 (V1.1.1)	Description of a communication protocol and data format for a QKD network to supply cryptographic keys to an application based on a REST API.
GS QKD 012	QKD; Device and Communication Channel Parameters for QKD Deployment	2019-02 (V1.1.1)	Description of main communication resources involved in a QKD system and the architectures that can be adopted to perform a QKD deployment over an optical network infrastructure.
GS QKD 004	QKD; Application Interface	2020-08 (V2.1.1)	Specification and description of API between QKD KM and applications., including sequence diagrams for different scenarios.
GS QKD 015	QKD; Control Interface for Software Define Networks	2022-04 (V2.1.1)	Definition of the interface between a SDN-QKD node and a SDN controller, description of the flow of information and the information model.
GS QKD 018	QKD; Orchestration Interface for Software Defined Networks	2022-04 (V1.1.1)	Definition of the interface between an SDN orchestrator and an SDN controller of a QKD network, description of the information flow and the information model.
GS QKD 016	QKD; Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules	2023-04 (V1.1.1)	Specification of a Protection Profile for the security evaluation of pairs of QKD modules under the Common Criteria.

Table 2.2: ETSI ISG-QKD published standards

Identification	Title	Expected date	Description
GS QKD 016	QKD; Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules	2023-12	This document is expected to update, extend and revise the GS QKD 016 V1.1.1 document. Current status: Waiting for publication
GS QKD 010	QKD Implementation security: protection against Trojan horse attacks in one-way QKD systems	2023-12	Design, construction, characterisation and operation of QKD systems that are intended to protect against Trojan horse attacks. Current status: Stable draft

Identification	Title	Expected date	Description
GS QKD 005	QKD; Security Proofs Revision	2024-01	This document is expected to update, extend and revise the GS QKD 005 V1.1.1 document. Current status: Stable draft
GR QKD 017	QKD; Network Architectures	2024-02	Review of the variety of architectures that have been proposed for QKD networking. Current status: Stable draft
GS QKD 020	QKD; Protocol and data format of REST-based Interoperable Key Management System API	2024-02	Specification of a REST API that allows key management systems to interoperate to pass keys horizontally between two systems located in a common trusted node. Current status: Early draft
GR QKD 007	QKD; Vocabulary Revision	2024-03	This document is expected to update, extend and revise the GR QKD 007 V1.1.1 document. Current status: Early draft
GR QKD 019	QKD; Design of QKD interfaces with Authentication	2024-03	Report on the design of classical interfaces for QKD systems that include authentication. Current status: Stable draft
GS QKD 013	QKD Characterisation of Optical Output of QKD transmitter modules	2024-03	Definition of procedures for characterising specific properties of complete QKD transmitter modules. Current status: Stable draft
GS QKD 021	QKD; Orchestration Interface of Software Defined Networks for Interoperable Key Management System	2024-03	Interface between the SDN Orchestrator and the SDN Controller of QKD networks for cooperating key management systems. Current status: Early draft
GS QKD 015	QKD; Control Interface for Software Define Networks	2024-04	This document is expected to update, extend and revise the GS QKD 015 V1.1.1 document. Current status: Start of work
GS QKD 014	QKD; Protocol and data format of REST-based key delivery API	2024-07	This document is expected to update, extend and revise the GS QKD 014 V1.1.1 document. Current status: TB adoption of WI

Table 2.3: ETSI ISG-QKD standards under development

However, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) is also involved in the development of multiple recommendations related to QKD, focusing on enabling the integration of QKD in large-scale communication infrastructures through the implementation of QKD Networks (QKDN). This effort is being carried out by Study Group 13 (SG 13 - Future Networks and Emerging Network Technologies), which primarily addresses the network and architectural aspects of QKDN, and Study Group 17 (SG 17 - Security), which focuses on security aspects [ITU-T-SG13], [ITU-T-SG17].

In addition, the Focus Group on Quantum Information Technology for Networks (FG-QIT4N) has been dedicated to producing various technical reports concerning QKDN, with a specific emphasis on the implications of Quantum Information Technologies (QITs) for quantum networks [ITU-T-QIT4N]. Both study groups, as well as the focus group, have already published a range of recommendations, which are summarised in the tables below.

Reference	Title	Date published	Description
Y.3800	Overview on networks supporting QKD	2019-10	Description of technologies, capabilities, and security considerations to provide support for the designs, deployment, operation and maintenance of the implementation of QKDN.
Y.3801	Functional requirements for quantum key distribution networks	2020-04	Specification of functional requirements for quantum layer, key management layer, QKDN control layer and QKDN management layer.
Y.3802	Quantum key distribution networks - Functional architecture	2020-12	Definition of a functional architecture model of QKDN, specifying detailed functional elements and reference points, architectural configurations, and basic operational procedures.
Y.3803	Quantum key distribution networks - Key management	2020-12	Description for the design, deployment and operation of key management of a QKDN, describing functional elements and procedures.
Y.3804	Quantum key distribution networks - Control and management	2020-09	Specification of functions and procedures for QKDN control and management based on the requirements specified in the Y.3801 document.
Y.3805	Quantum Key Distribution Networks - Software Defined Networking Control	2021-07	Specification of requirements, functional architecture, reference points, hierarchical SDN controller and overall operational procedures of SDN control.
Y.3806	Quantum key distribution networks - Requirements for quality of service assurance	2021-09	Specification of high-level and functional requirements of QoS assurance for QKDN, including QoS planning, monitoring, optimisation, provisioning, protection, and recovery.

Reference	Title	Date published	Description
Y.3807	Quantum key distribution networks - Quality of service parameters	2022-02	Specification of QoS and network performance on QKDN, describing associated relative parameters and their definitions.
Y.3808	Framework for integration of quantum key distribution network and secure storage network	2022-02	Overview of Secure Storage Networks for QKDN, including functional requirements, functional architecture module, reference points and operational procedures.
Y.3809	A role-based model in quantum key distribution networks deployment	2022-02	Description of roles, a role-based model and service scenarios in QKDN from different deployment and operation perspectives.
Y.3810	Quantum key distribution network interworking - Framework	2022-09	Specification of the framework of QKDN interworking, including description of reference models, functional models of gateway functions, and interworking functions.
Y.3811	Quantum key distribution networks - Functional architecture for quality of service assurance	2022-09	Overview of functional architecture of QoS assurance for QKDN, including functional entities and basic operational procedure.
Y.3812	Quantum key distribution networks - Requirements for machine learning based quality of service assurance	2022-09	Specification of high-level and functional requirements of ML-based QoS assurance for QKDN, including description of functional model, and use cases.
Y.3813	Quantum key distribution network interworking - Functional requirements	2023-01	Specification of functional requirements for QKDN interworking, describing the requirements for the different layers and elements present in the QKDN.
Y.3814	Quantum key distribution networks - Functional requirements and architecture for machine learning enablement	2023-01	Specification of one possible set of functional requirements and a possible architecture for an ML-enabled QKDN, including an overview, and the functional requirements and architecture.
Y.Sup70	ITU-T Y.3800-series - Quantum key distribution networks - Applications of machine learning	2021-07	Presentation of application of ML in the quantum layer, key management layer and control layer of QKDN, including use case background, issues, benefits, etc.

Reference	Title	Date published	Description
Y.Sup74	Standardisation roadmap on quantum key distribution networks	2023-03	Standardisation roadmap of QKD, describing the landscape with related technical areas of trust technologies. Status: In force (prepublished)
Y.Sup75	Quantum key distribution networks - Quantum-Enabled Future Networks	2023-03	Status: In force (prepublished)

Table 2.4: ITU-T SG-13 standards

Reference	Title	Date published	Description
X.1702	Quantum noise random number generator architecture	2019-11	Definition of a generic functional architecture of a quantum entropy source and a common method to estimate and validate the entropy of a noise source under evaluation.
X.1710	Security framework for quantum key distribution networks	2020-10	Specification of a framework including requirements and measures to combat security threats to QKDNs.
X.1712	Security requirements and measures for quantum key distribution networks - key management	2021-10	Specification of security threats and requirements for key management in QKDN, and security measures of key management to meet the security requirements.
X.1714	Key combination and confidential key supply for quantum key distribution networks	2020-10	Description of key combination methods for QKDN and specification of security requirements for key combination and key supply to applications.
X.1715	Security requirements and measures for integration of quantum key distribution network and secure storage network	2022-07	Definition of security requirements and measures for integrating a QKDN with a SSN in the service layer and PKI.
X.STR-SEC-QKD	Security considerations for quantum key distribution networks	2020-03	Description of the perspective of QKD, security considerations of QKDN, standardisation issues of QKDN.
XSTR-HYB-QKD	Overview of hybrid approaches for key exchange with quantum key distribution	2022-05	Study of the possibilities to accommodate QKD protocols in the context of hybrid approaches for key exchange.
X.sec_QKDN_tn	Security requirements and designs for quantum key	2024-03	Identification of security threats and definition of security requirements

Reference	Title	Date published	Description
	distribution networks - trusted node		of trusted nodes, including some examples. Status: Under study
X.sec_QKDN_CM	Security requirements and measures for quantum key distribution networks - control and management	2024-04	Specification of use cases, security threats in the context of quantum computing, security requirements and security measures for controllers and managers of QKDN. Status: Under study
X.sec_QKDN_AA	Authentication and authorization in QKDN using quantum safe cryptography	2024-04	Study of authentication and authorisation for QKDN, IDs and their management in QKDN and public key certifications in QKDN. Status: Under study
X.sec_QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)	2025-03	Specification of security requirements for QKDN interworking, including security threats, and authentication and authorisation aspects. Status: Under study

Table 2.5: ITU-T SG-17 standards

Reference	Title	Date published	Description
D2.1	QIT4N Terminology: Quantum Key Distribution Networks	2021-11	Survey of terminology relevant to QKDN and categorisation according to specific technical directions.
D2.2	QIT4N use case: Quantum Key Distribution Network	2021-11	Description of different QKDN use cases, classified into 6 categories.
D2.3 part 1	Quantum key distribution network (QKDN) protocols part 1: Quantum layer	2021-11	Description of QKD protocols in the quantum layer, including workflows, features, parameters, etc.
D2.3 part 2	Quantum key distribution network (QKDN) protocols part 2: Key management layer, QKDN control layer, and QKDN management layer	2021-11	Description of QKD protocols with respect to the key management layer, QKDN control layer and QKDN management layer.
D2.4	Quantum Key Distribution NEtwork transport technologies	2021-11	Discussion on QKDN transport technologies such as transport system components, technical solutions, typical scenarios of the coexistence of quantum and classical signals, etc.

Reference	Title	Date published	Description
D2.5	Standardisation outlook and technology maturity part 2: quantum key distribution network	2021-11	Overview of QKD technology, industry status, QKDN standardisation landscape and future standardisation suggestions.

Table 2.6: ITU-T FG-QIT4N Technical Reports

The ISO/IEC also has a standardisation subcommittee, JTC 1/SC 27, which is responsible for developing standards, technical specifications and reports, best practices, and related documents in the field of information security, cybersecurity and privacy protection [ISO-IEC-JTC1-SC17]. This subcommittee, in the field of QKD, has developed a two-part standard targeting the security requirements, test and evaluation methods for QKD, as summarised in Table 2.7.

Reference	Title	Date published	Description
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	20238-08	Identification of security requirements and potential attacks.
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	2023-09	Description of test and evaluation methods to validate and fulfil security requirements.

Table 2.7: ISO/IEC standards

The Internet Engineering Task Force (IETF) Quantum Internet Research Group (QIRG), has made significant contributions to the field of quantum communications by publishing several internet drafts [IETF-QIRG]. These primarily focus on providing an introduction to the progression towards the realisation of the Quantum Internet and quantum communication networks. While these documents do not specifically concentrate on QKD, they acknowledge the importance of QKD technology as an initial stage in the development of the Quantum Internet. QKD is recognised as a foundational component that serves as a starting point for subsequent, more advanced stages of the Quantum Internet. As a result, both of these documents are considered valuable in the context of QKD standardisation efforts.

Reference	Title	Date published	Description
RFC 9340	Architectural Principles for a Quantum Internet	03-2023	Description of the framework and introduction to basic architectural principles for a quantum internet.
draft-irtf-qirg-quantum-internet-use-cases-16	Application Scenarios for the Quantum Internet	10-2023 (V19)	Overview and categorisation of applications expected to be used on the Quantum Internet and a description of some general requirements.

Table 2.8: IRTF standards

Similarly, and related to quantum communications in general, the IEEE also has a working group, QuantumComm - Software-Defined Quantum Communication, which is currently working on a new standard for software-defined quantum communications [IEEE-QC].

Reference	Title	Date published	Description
P1913	YANG Model for Software-Defined Quantum Communication	-	Definition of a YANG model that enables configuration of quantum endpoints in a communication network to dynamically create, modify or remove quantum protocols and applications. Status: Active PAR

Table 2.9: IEEE standards

2.4 QKD Hardware and Interoperability

From the QKD development and deployment perspective, the crucial element is the development of software and hardware interoperability interfaces. Availability and usage of interoperable interfaces would allow the operating of different QKD vendors under one infrastructure, and use of different Key Management Systems. This particular area was also a point of interest and activities of NRENs who participated or coordinated National QCI projects, KMS systems are an integral part of these projects. In terms of EuroQCI infrastructure context, the interoperability is discussed by a common document published by the European Commission: EuroQCI ConOps (Concept of Operations) [STE-2023].

The following tables show the ongoing standardisation work regarding interoperability aspects.

SDO	Document number	Document title	Version	Date published
ETSI	GS QKD 004	Quantum Key Distribution (QKD): Application Interface	V2.1.1	2020-08
	GS QKD 014	Quantum Key Distribution (QKD): Protocol and data format of REST-based key delivery API	V1.1.1	2019-02
	GS QKD 015	Quantum Key Distribution (QKD): Quantum key Distribution control interface for Software Defined Networks	V2.1.1	2022-04
	GS QKD 018	Quantum Key Distribution (QKD): Orchestration Interface of Software Defined Networks	V1.1.1	2022-04
ITU-T SG 13	Y.3800 (ex Y.QKDN_FR)	Overview on networks supporting quantum key distribution Corrigendum 1		2019-10 2020-04
	Y.3801 (ex Y.QKDN-req)	Functional requirements for quantum key distribution networks		2020-04

SDO	Document number	Document title	Version	Date published
	Y.3802 (ex Y.QKDN_Arch)	Quantum key distribution networks - Functional architecture		2020-12
	Y.3803 (ex Y.QKDN_KM)	Quantum key distribution networks - Key management		2020-12
	Y.3804 (ex Y.QKDN_CM)	Quantum key distribution networks - Control and management		2020-09
	Y.3805 (ex Y.QKDN_SDNC)	Quantum key distribution networks - Software-defined networking control		2021-12
	Y.3806 (ex Y.QKDN-qos-req) (ex Y.QKDN-qos-gen)	Quantum key distribution networks - Requirements for quality of service assurance		2021-09
	Y.3807 (ex Y.QKDN-qos-pa)	Quantum key distribution networks - Quality of service parameters		2022-02
	Y.3810 (ex Y.QKDN-iwfr)	Quantum key distribution network interworking - Framework		2022-09
	Y.3811 (ex Y.QKDN-qos-arc)	Quantum key distribution networks - Functional architecture for quality of service assurance		2022-09
	Y.3812 (ex Y.QKDN-qos-ml-req)	Quantum key distribution networks - Requirements for machine learning based quality of service assurance		2022-09

Table 2.10: Published standards in reference to aspects of interoperability

SDO	Document number	Document title	Version	Expected publication date
ETSI	GS QKD 020	Quantum Key Distribution (QKD): Protocol and data format of REST-based Interoperable Key Management System API	V1.1.1	2023-09
ITU-T SG 11	Q.QKDN_profr	Quantum key distribution networks - protocol framework		Drafting
	Q.QKDN_Ak	Protocols for Ak interface for QKDN		Drafting
	Q.QKDN_Ck	Protocols for Ck interface for QKDN		Drafting

SDO	Document number	Document title	Version	Expected publication date
	Q.QKDN_Kx	Protocols for Kx interface for QKDN		Drafting
	Q.QKDN_Kq-1	Protocols for Kq-1 interface for QKDN		Drafting
ETSI	GS QKD 017	Quantum Key Distribution (QKD): Network architectures	V1.1.1	2023-07
ITU-T SG 13	Y.3813 (ex Y.QKDN-iwrq)	Quantum key distribution networks interworking - functional requirements		Drafting (Consented)
	Y.3814 (ex Y.QKDN-ml-fra)	Quantum key distribution networks - functional requirements and architecture enhancement for machine-learning based quality of service assurance		Drafting (Consented)
	Y.QKDN-qos-iw-req	Requirements of QoS assurance for QKDN interworking		Drafting
	Y.QKDN-qos-ml-fa	Quantum key distribution networks - functional architecture enhancement for machine-learning based quality of service assurance		Drafting
	Y.QKDN-qos-mmq	Quantum key distribution networks - Measurement methodology for QoS parameters		Drafting
	Y.QKDN-iwac	Quantum key distribution networks interworking - architecture		Drafting
	Y.QKDN-amc	Quantum key distribution networks - Requirements and architectural model for autonomic management and control		Drafting
	Y.QKDNf-fr	Framework of Quantum Key Distribution Network Federation		Drafting
	Y.QKDNi-SDNC	Quantum Key Distribution Network Interworking - Software Defined Networking Control		Drafting
	Y.QKDN-rsfr	Framework of quantum key distribution network resilience		Drafting

Table 2.11: Draft / revision standards in reference to aspects of interoperability

As a part of the OpenQKD project activities, some NRENs participated in the preparation of interoperability tests between different QKD vendors. The challenge was that the vendors are at different levels of implementation works for the specific interface, for example, ETSI GS 020. At this stage it is important to properly design the interoperability tests and respect the current state of interfaces specification proposal.

QKD systems can be implemented using different topologies that reflect intended services specification or physical links constraints. These elements are managed and configured within the Key Management Systems (KMS) that will be standardised and independent from QKD systems vendors. This element will also be responsible for establishing cross-border QKD links where independent KMS systems connect and exchange services. The same specifically applies for space-segment QKD systems where the physical link is different and an interface between space-based and terrestrial based systems is required.

Many elements regarding QKD system networks, its interoperable interfaces, KMS and multi domain operation are still being discussed.

2.5 Monitoring and Operations

QKD systems, although they may differ in terms of physical realisations, have several key parameters that should be monitored to ensure efficient and secure functioning. QKD systems monitoring needs to be done on two levels: at physical links and systems, and at the Key Management Systems (KMS) level. KMS monitoring provides insight into the QKD systems' topology, key flows and service levels. Below are the main parameters in detail, along with guidance on how to monitor them:

2.5.1 Quantum Bit Error Rate (QBER)

This parameter reveals the noise level in the QKD system. If this noise level is close to zero, it indicates that nearly all the information sent from one party was received in the same form by the second party. In other words, QBER represents how many bits of information were lost in the transmission and provides hints about potential problems, depending on the type of QKD system used. Another important function of this measure is that it can reveal any attempts at eavesdropping by a third party. Therefore, QBER is also used to inform the users if the connection and the key are secure or if the distribution has failed.

QBER is monitored by comparing a random subset of sent and received bits. It is then calculated as the number of differing bits divided by the total number of compared bits. A reduced correlation between these two subsets would increase the QBER. If the value stays below 11% (based on protocol implemented), the connection is considered secure, and the key can be used.

2.5.2 Time Synchronisation

Stations at both ends of a QKD system need to be synchronised to prevent the introduction of errors. For the system to function correctly, both parties must register the same bit within the same time window. This can become problematic if the channel lengths differ or if there is variation in the additional equipment used.

Synchronisation is achieved through clock jitter measurement, which evaluates the timing performance of the system. This measurement provides insight into the amount of delay present at the receiving end of the QKD system.

2.5.3 Key Rate

This parameter provides insight into actual physical key exchange rate over the quantum link. It is directly related to the length and quality of the link and fibre. It is worth noting that this value is not constant and changes constantly together with the system's optical parameters. These parameters are continually monitored and adjusted to achieve lowest possible QBER and highest quality of the link. Key exchange is performed in blocks

until the key buffer is filled. The initial QKD system setup takes a longer time as the first key needs to fill-in the initial key buffer.

2.5.4 KMS Level Monitoring

The key Management Systems monitoring provides not only insight into the physical parameters detailed in Sections 2.5.1 to 2.5.3 but also other higher level parameters of the QKD systems. These include topology layout, status of each link, key consumer status, key buffer levels, buffer fill-in and empty ratios. Key request statistics (number of keys, lengths of keys), apart from monitoring, also enable QKD systems configuration on physical and application levels.

2.5.5 Specific QKD System Parameters

Depending on the type of QKD system and physical implementation, there may be additional parameters that can be monitored and to get deeper insight into QKD link performance and characteristics. Depending on the vendor, there are usually two types of QKD systems - operational and Research and Development (R&D). The R&D system is in most cases the same from a physical point of view, but it offers monitoring of additional parameters that can help with service and system development scenarios.

Figure 2.4 and Figure 2.5 below show examples of QKD systems monitoring scenarios using the Grafana tool:

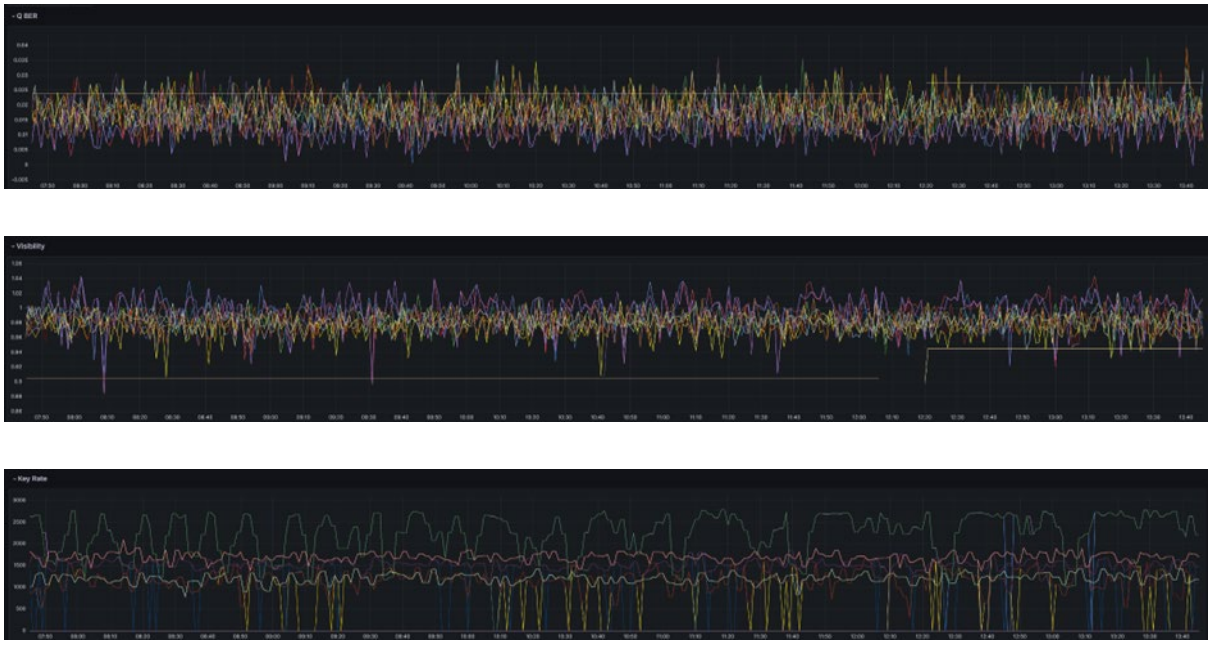

Figure 2.4: Operational parameters collected in a time series database and visualised with Grafana showing time (x-axis) and QBER (Quantum it Error Ration in %), Visibility (in %), and Key Rate in bits/s

Basic operational parameters are collected in a time series database for further processing and analysis. The example was taken on a Clavis 3 system during a test by CESNET and visualised using Grafana.

Figure 2.5: Grafana based graphs of the QKD in CESNET showing key rate, QBER, visibility, detection count

3 QKD Projects and Initiatives in the GÉANT Community

3.1 Projects and Initiatives in EuroQCI

A large number of NRENs lead or participate in the National Quantum Communication Infrastructure (NatQCI) projects, and there are also NRENs that participate indirectly in the NatQCIs. Through the Quantum Strategy Group and the GN5-1 Network Development Work Package (WP6) Quantum Technologies subtask, GÉANT facilitates the information sharing between the NRENs. The exchange of expertise and collaboration among NRENs are crucial elements in establishing a secure and operational EuroQCI.

The field of quantum communication is highly specialised and rapidly evolving. The exchange of expertise involves sharing knowledge, insights, and best practices among NRENs. This collaboration allows each network to benefit from the strengths and experiences of others, fostering a collective understanding of quantum communication technologies. By collaborating, NRENs can contribute to the advancement of quantum communication technologies collectively. This may involve joint research and development efforts, the sharing of research findings, and collaboration on testing and implementing new quantum solutions.

Some examples of the NRENs that participate in the EuroQCI initiative are provided in the sections that follow. This list is by no means complete but reflects on the work of NRENs that are part of the WP6 group:

- HellasQCI – Greece | GRNET (COO)
- PIONIER-Q – Poland | PSNC (COO)
- CroQCI – Croatia | CARNET (COO)
- BE-QCI - Belgium | BELNET
- IrelandQCI – Ireland | HEANET
- QCIHungary – Hungary | KIFÜ
- RoNaQCI – Romania | RoEduNet
- CZQCI – Czechia | CESNET
- QCINed – The Netherlands | SURF
- CYQCI – Cyprus | CYNET

3.1.1 HellasQCI

The Greek National Infrastructures for Research and Technology (GRNET), which operates under the auspices of the Ministry of Digital Governance, is the coordinator for the HellasQCI project that builds the Greek National Quantum Communication infrastructure.

The HellasQCI consortium includes governmental authorities, industrial partners and key Greek research institutes, which are able to address the needs for an operational HellasQCI infrastructure.

The objective of the HellasQCI project, which is part of the EuroQCI European network, is to contribute to the safe-keeping of critical data and infrastructures in domains such as egovernment, healthcare, financial industry and other critical areas. This will be achieved by incorporating systems and technologies based on principles of

quantum technology, more specifically by the distribution of quantum keys (QKD) to existing communication infrastructures, which will offer an exceptionally secure form of encryption, providing an extra layer of security.

The implementation of the project involves the creation of three quantum infrastructure metropolitan networks in Athens, Thessaloniki, and Heraklion in Crete which will connect with three optical Ground Stations (OGSs) in Helmos, Holomontas, and Skinakas. Those network infrastructures will utilise quantum technology equipment (QKD), ground optical fibres, and satellite technologies. The creation of this quantum infrastructure, combined with other initiatives will create a secure network for ground and satellite communications, ensuring the highest level of security in the government and private sectors.

HellasQCI will:

- Develop and deploy advanced quantum systems and networking technologies (QKD) (Figure 3.1).
- Perform 16 advanced use cases in different application scenarios in several domains: national security, public health, industry, critical infrastructures, ICT, and research.
- Provide a holistic training environment for technical, research, and end-users staff.
- Collaborate with PETRUS CSA and other national QCI proposals on building together the EuroQCI: HellasQCI has formed 7 bilateral partnerships with Ireland, Luxembourg, Austria, Bulgaria, Cyprus, Malta, and Poland.
- Establish the HellasQCI community, including all relevant national stakeholders that can benefit and support the HellasQCI networks, gather expertise and share knowhow on QCI and QKD.
- Align with the QKD security standards, certifications, and regulations.

Figure 3.1: HellasQCI project network topology

3.1.2 CroQCI - Croatia | CARNET (COO)

CroQCI, which stands for Croatian Quantum Communication Infrastructure, is Croatia's national project. It is part of the first implementation phase of EuroQCI which is supported by the Commission's Digital Europe Programme. The duration of the CroQCI project is 30 months (lasting from 1 January 2023 to 30 June 2025.).

The project involves nine partner institutions:

- Croatian Academic and Research Network (CARNET)
- Ruđer Bošković Institute (IRB)
- Marine Electronic Center Ltd (PCE)
- University of Zagreb University Computing Centre (SRCE)
- Institute of Physics (IF)
- University of Zagreb, Faculty of Electrical Engineering and Computing (FER)
- University of Zagreb Faculty of Transport and Traffic Sciences (FPZ)
- Transmitters and Communications Ltd (OIV)
- Office of the National Security Council (UVNS)

The Croatian Academic and Research Network acts as the coordinator of project partner beneficiaries as well as the leader of several work packages.

The project objectives are:

- Setting and piloting the deployment of advanced experimental quantum systems and communication networks, complemented and integrated with classical security technologies.
- Building and testing devices and systems combining the best of quantum, post-quantum classical and quantum-enhanced solutions.
- QCI network architecture design.
- Composing terrestrial-based solutions while assuring fulfilment of the preconditions for space connectivity.
- Education that will comply with the maturity of the technology, current and future needs.
- Testing of project use-cases.

In addition, performances and readiness checks of experimental systems for atomic clock synchronisation and quantum memory for use in CroQCI network are planned as a part of the project activity.

3.1.3 CZQCI – Czechia | CESNET

The Deploy Advanced Quantum Communication Infrastructure (QCI) in the Czech Republic project (CZQCI) is implemented within the framework of the Digital Europe Programme under contract number 101091684.

CZQCI will deploy quantum communication infrastructure in the Czech Republic. The infrastructure composed of advanced experimental European QKD devices will comprise:

- A backbone connecting the cities of Prague, Brno, and Ostrava, serving as a first long distance quantum communication network.
- Metropolitan side branches connecting public authorities and testing advanced use cases and scenarios.

- Advanced testing and training infrastructure concentrated in a single laboratory providing a representative sample of diverse QKD technologies.

CZQCI will design and perform training programmes to prepare users and experts from all sectors for the exploitation of future quantum communication infrastructures.

The infrastructure and expertise developed by CZQCI will enable the testing of advanced communication scenarios involving public institutions and users from industry, testing operational demands over long distance and long time, and testing QKD and network components. The ambitious testing exercises will pave the way to large-scale deployment of QCI.

CZQCI will engage in international collaboration to exchange experiences, and prepare connections to neighbouring countries and integration into EuroQCI. CZQCI will increase awareness of quantum technologies among diverse target audiences.

In the Czech Republic, the responsible public authorities have delegated the responsibility for QCI deployment to CyberSecurity Hub, an institute co-founded by three leading Czech universities to coordinate cybersecurity research and knowledge transfer on the national level. Seven academic institutions with expertise in quantum technologies join the deployment consortium to concentrate the national knowledge relevant to quantum communication and facilitate its transfer through training and dissemination. The participants are:

- Coordinator CYBERSECURITY HUB, ZU
- ISI CAS - USTAV PRISTROJOVE TECHNIKY AVCR VVI
- CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB CZ
- CTU - CESKE VYSOKE UCENI TECHNICKE V PRAZE CZ
- MU - Masarykova univerzita CZ
- UPOL - UNIVERZITA PALACKEHO V OLOMOUCI CZ
- IT4I@VSB VSB - TECHNICAL UNIVERSITY OF OSTRAVA CZ
- BUT - VYSOKE UCENI TECHNICKE V BRNE CZ

This way, CZQCI will present a significant contribution to increasing cybersecurity efforts in Europe through the promotion and adoption of European quantum communication technologies.

The project is planned to run between from 1 March 2023 to 31 August 2026, however, the call for national co-funding is still in progress.

3.1.4 PIONIER-Q – Poland | PSNC (COO)

The PIONIER-Q project is a QCI proposal prepared by the Polish community and is coordinated by the Poznan Supercomputing and Networking Center (PSNC). The partners of PIONIER-Q are all High Performance Computing (HPC) centres in Poland: the Poznań Supercomputing and Networking Center, the NASK National Research Institute, ICM, the Interdisciplinary Centre for Mathematical and Computational Modelling, Gdńsk University of Technology, Wroclaw University of Science and Technology, and the Academic Computer Centre Cyfronet AGH, that are also part of the PIONIER consortium of Polish National Research and Education Network. The main goals of the project are to:

- Build the QCI network based on the PIONIER network infrastructure and services.
- Implement a number of use cases and scenarios.
- Provide a research platform for the community.

- Organise training and workshops.
- Cooperate with other QCI projects.
- Integrate with the EuroQCS-Poland project infrastructure.

The PIONIER-Q project will use the existing QKD infrastructure that was implemented by PSNC under the OpenQKD project and the National Laboratory for Photonics and Quantum Technologies (NLPQT) project, in which PSNC established a local, metro QKD infrastructure in the POMZAN network and a long-distance Poznan to Warsaw QKD link with 380 km of length with 5 trusted nodes.

Each PIONIER-Q partner prepared its own use case based on its existing infrastructure and services. These are related to medical data, local administration, networking, and computing services.

PIONIER-Q aims to connect not only QCI and Quantum Computing activities but also reference a time and frequency transmission system that uses optical carrier technology and was developed under the NLPQT project.

Proposed PIONIER-Q use cases connect various applications and services from the public sector to achieve synergy in terms of infrastructure security. HPC centres that are part of the PIONIER-Q consortium have a wide range of different existing services and can provide multiple scenarios not only for the EuroQCI infrastructure but also for the EuroQCS infrastructure. The entire EuroQCI and EuroQCS infrastructure will be managed, operated, and monitored by PSNC using its existing infrastructure, as well as specially developed tools and services.

3.1.5 QCIHungary - Hungary | KIFÜ

The Deploy Advanced QCI project in Hungary (QCIHungary, see Figure 3.2) is implemented within the framework of the Digital Europe Programme under Contract number 101081247 .

The project aims to lay the foundations of a national quantum communication infrastructure in Hungary, with the eventual goal to participate in the creation of a larger pan-European quantum network. The plan is to connect the capital, Budapest, with three cities in three different directions (Győr, Nagykanizsa, Szeged) with the future possibility of cross-border connections with Austria, Slovakia, Slovenia, Croatia, and Romania. Within Budapest, a metropolitan network is envisioned to be employed for various purposes. The backbone and a part of the metropolitan network will be constructed from commercially available quantum key distribution (QKD) systems.

The project also builds on previous Hungarian research to develop a continuous variable as well as an entanglement-based QKD system over optical fibres. In addition to terrestrial, optical fibre-based QKD systems would be prepared for later satellite-based QKD connections by developing a freespace quantum link and by the installation of a quantum-capable ground station. Existing deployment efforts will be complemented by developing the necessary supporting software.

Another important aspect of the project is training and education. Methodologies and training materials will be developed for various audiences and a simulator software for the courses. The project will actively engage in international collaborations with neighbouring and other EU countries in order to exchange practical experiences and to coordinate future work.

The project will be run between 1 January 2023 and 30 June 2025 by four institutions: the Governmental Agency for IT Development as consortium leader, Budapest University of Technology and Economics, Eötvös Loránd University, and Wigner Research Centre for Physics.

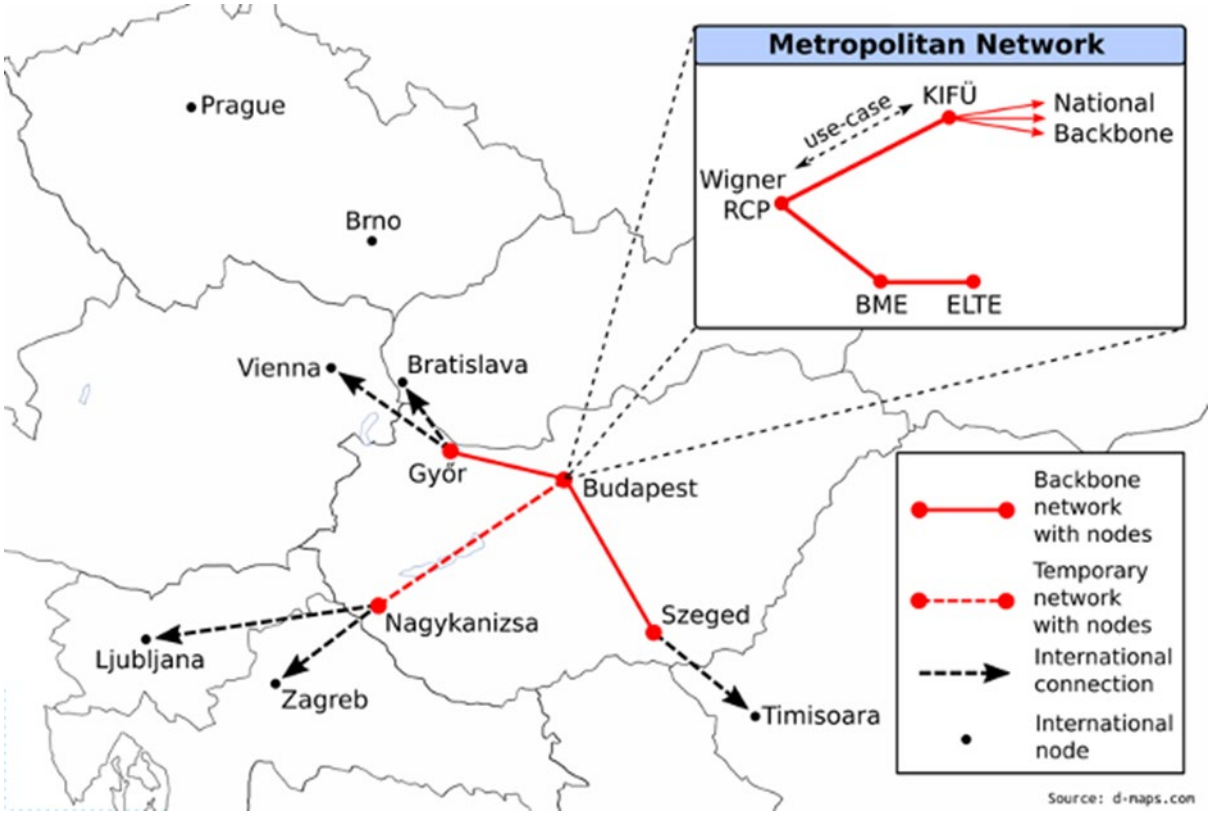

Figure 3.2: QCIHungary project network topology

3.2 Projects and Initiatives from R&E (National/Regional) Organisations

This section highlights some of the ongoing work as part of national/regional QKD-related projects, specifically of NRENs that are part of the WP6 group (Section 3.2.1 to 3.2.3 only show a few examples of these).

3.2.1 I2Basque

I2Basque, the Basque Country NREN, connects all higher education and research centres of the Autonomous Region of the Basque Country to GEÁNT via the Spanish NREN RedIRIS. The topology of the network is quite simple with a ring that brings together two smaller rings and connections to several additional sites. Figure 3.3 shows the topology and geographical distances.

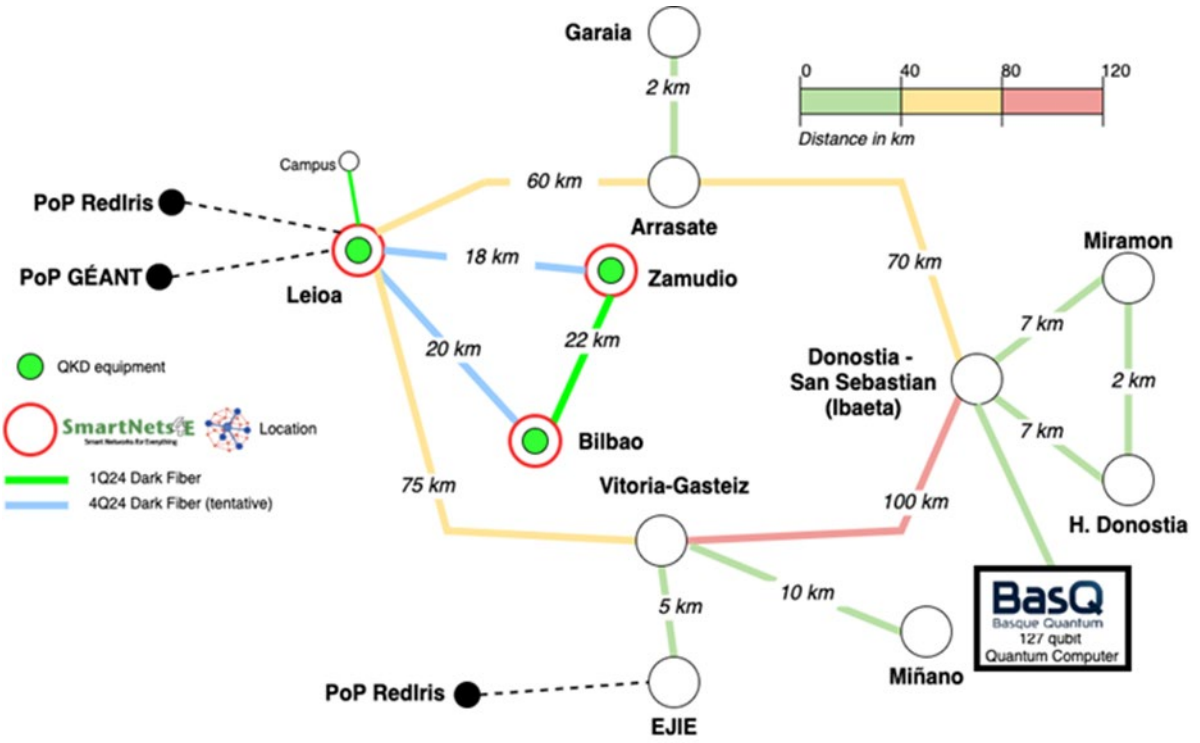

Figure 3.3: Topology and geographical distances of the I2Basque network

In recent years, interest in quantum technologies has increased. The IKUR quantum initiative is promoted by the Basque Country Government Universities and Research Department, and is synchronised with the Spanish Government Complementary Quantum Communications Plan. IKUR merges all the Basque Country quantum-related R&D activities and research groups. The Basque NREN I2Basque, connected via RedIRIS to GEÁNT, was already linking at layer 3 all the centres involved, as well as the future (2025) IBM Quantum Computer located in the San Sebastian - Ibaeta node.

When the project proposal SareQuant was submitted to IKUR, there were already many ongoing quantum R&D activities, but no direct research involving quantum communications and applications like Quantum Key Distribution was being undertaken. The SareQuant (Sare is the Basque word for network) proposal was approved with a two-fold objective and corresponding activities, as presented in Figure 3.4:

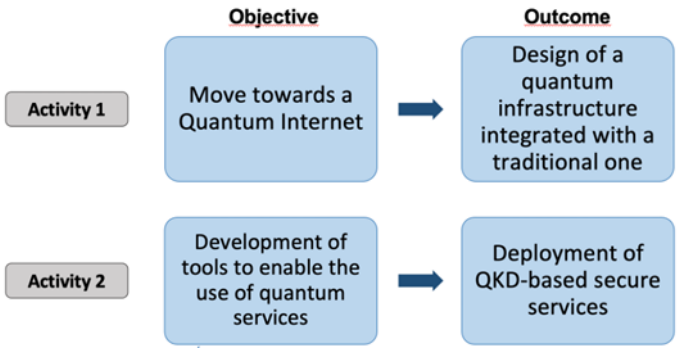

Figure 3.4: SareQuant proposal objectives and planned outcomes

The first objective was to study the (near) future adaptation of the actual I2Basque, into a quantum-capable NREN. Depending on the locations of the research being done, the adaptation can be undertaken either by

replacing leased lines by dark optical fibres carrying the secured data, the service channel and the quantum channel, or by dark optical fibres that only convey the service and quantum channels between locations already linked by leased lines. For this, a study of the network, the short and long term needs of the R&D teams and their locations is being undertaken. Additionally, the involvement of other stakeholders like public institutions (public health service, Basque Government IT services or the Basque Cybersecurity Agency) or the industrial sector is expected. Some of them are already connected to I2Basque or have collocated nodes and, again, the connection alternatives will be studied.

The second objective will be achieved by supporting short- and long-lived experiments. The inner triangle (Figure 3.3) is where short life experimentation cycles are going to be done. In this case, the links of the triangle will be deployed in parallel to actual I2Basque Links. The experiments target not only traditional QKD applications like high capacity (100Gbs) carrier link encryption but also specific applications like 5G/6G core or industrial applications.

The long life experimentation will involve some of the previously mentioned stakeholders like public institutions and presumably will imply the deployment of quantum links between them to evaluate the use of QKD and post quantum cryptography experiments on a pre-production environment. Another midterm objective will be to link the R&D centres to the 127 qbit Basque quantum computer that will be located in 2025 at the Donostia-San Sebastian (Ibaeta) campus.

For this purpose, four pairs of different QKD devices are in the process of acquisition and deployment. In order to obtain a more heterogeneous infrastructure and to enable a complete evaluation of the solutions, three different QKD technologies have been selected: prepare-and-measure Discrete-Variable Quantum Key Distribution (DV-QKD), prepare-and-measure Continuous-Variable Quantum Key Distribution (CV-QKD), and entanglement-based QKD.

For the short-lived experiments, the equipment will be deployed over the inner triangle (Figure 3.3) which in fact is an overlay over the University of the Basque Country Smart Networks for Everything (SmartNets4E) experimental facility [SmartNets4E]. This facility is deployed over three different sites spread over roughly 20 kilometres, and one of them is colocated with the I2Basque, RedIRIS, and GEÁNT Point of Presence (PoP) in the Basque country. During the first iterations of the long-lived experiments some of this equipment might be lent to public stakeholders. At the time of writing, one of the links is being commissioned and conversations with RedIRIS to provide the remaining links are ongoing.

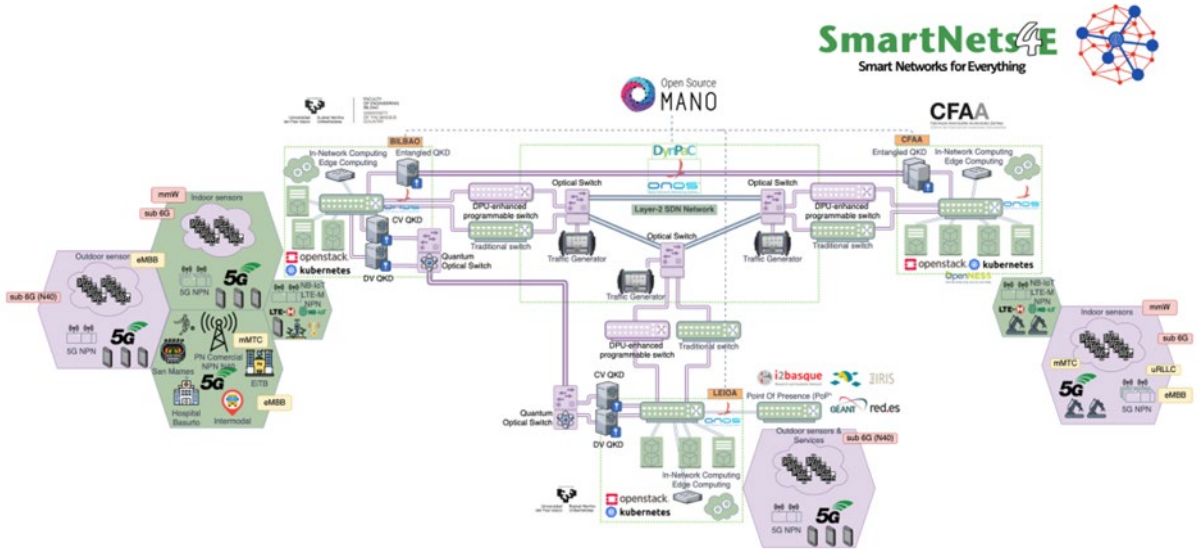

Figure 3.5: SmartNets4E experimental facility

The activities described above will contribute to seed the design of a suitable Quantum NREN that will support not only the pure R&D activities of the Basque Country, but also to build capacities and to help public bodies and industrial stakeholders to manage these new technologies. Finally, this infrastructure and resources, being part of the IKUR initiative and I2Basque will be connected to the Spanish EuroQCI initiative, which is in line with EuroQCI's plans to "*design quantum cryptography encryption methods based on quantum physics*", "*develop technology based on Quantum Key Distribution cryptography approaches*" and deploy this "*technology into the current existing telecommunications networks to facilitate an additional ultra-secure layer in the transmission of information*" [EuroQCI].

3.2.2 Germany

In Germany there is a diverse landscape of universities, research institutes, and companies working on varying aspects of quantum communication and quantum computing. Very large endeavours with a focus on quantum communication and QKD are research projects such as the QuNet Initiative with its industry support initiative DivQSec and the Quantum Repeater.Link project (QR.X) [DivQSec; QRX; QuNet]. The SQuaD umbrella project was established to coordinate and support all interested parties from quantum research and industry to make sure that the latest innovations and quantum technologies are transferred to industrial applications in the long run [SQuaD].

3.2.3 Czech Republic

In 2023 the Czech government approved investments for the implementation of a Quantum Key Distribution (QKD) infrastructure that will connect the major cities of Czechia, including Prague, Brno, and Ostrava. These funds will also be allocated to the development of metropolitan networks in these cities, as well as for advancements in universities. Many universities have already started to introduce new academic programs focused on teaching students about quantum technologies and their underlying theories. Specifically, representatives from seven academic institutions have met to discuss these initiatives and explore ways to integrate the QKD network with existing network infrastructure. Currently, the aim is to transmit the quantum signal through the same fibre-optic cables used for classical light signals.

4 Trusted Intermediate Relay Nodes

While QKD offers information-theoretic security through the laws of quantum mechanics, problems occur when transmissions must be established over long distances using optical fibre. The noise in the channel leads to error probabilities that scale exponentially with the channel length [BRI-1998]. With distances over several hundred kilometres, the resulting key rates just become too low [STA-2014].

For directly connected QKD nodes, there are commercially available QKD modules that can realise a QKD link for distances of approximately 120 km. By increasing the distance between QKD nodes on a link, the performance of the QKD link decreases, specifically reducing the Secure Key Rate (SKR). With measurement-assisted relaying techniques such as Measurement Device Independent QKD (MDI-QKD) and Twin-Field QKD (TF-QKD) as described above, it is possible to achieve longer distances. Currently, there are commercially available TF-QKD modules that can realise a QKD link for distances greater than 500 km [KLI-2022].

Quantum repeaters that would allow transmission for greater distances are still under development. Once available, a series of quantum repeaters will create a chain of entangled photons using the entanglement swapping technique.

For the time being, if longer distances must be bridged in quantum key distribution, trusted intermediate relays must be used as nodes where keys are simply sent from node to node until the final destination has been reached.

At each such relay node, the message is encrypted with a new quantum key, i.e., there is a decryption/re-encryption process where the quantum signals are terminated via measurement and a new key is produced for the next leg of the path [EVA-2021]. This makes the relay node an attractive location for an attacker because the process leaves the secret message one user sends to another in clear text until it is re-encrypted with the new key.

At the moment certification and standardisation processes of such trusted intermediate nodes are still under study [ITU-2023]. Some of these requirements may also be established as part of EuroQCI, for example, in the HellasQCI project. The following section details how such relays could be defined for high-security use cases, but also for experimental networks for research and education in the NREN community, until more refined certification procedures become available.

4.1 Trusted Nodes in EuroQCI Environments (Government/National Security Authorities)

In the context of EuroQCI, a trusted node refers to a network node that is considered secure and reliable for the purpose of transmitting and processing quantum information. In quantum communication, the security of information is based on the principles of quantum mechanics, such as the no-cloning theorem and the uncertainty principle.

Trusted nodes play a critical role in maintaining the security of the network by ensuring the integrity and confidentiality of quantum information. To be considered a trusted node within the EuroQCI, certain criteria need to be met. These criteria typically include:

- **Quantum Technology**: The node should employ quantum technology, such as quantum key distribution (QKD) or quantum teleportation, for secure communication.
- **Secure Infrastructure**: The node should have robust physical and technical security measures in place to protect against eavesdropping, tampering, or other forms of attacks.

- **Authentication and Authorisation**: The node should have mechanisms for authentication and authorisation to ensure that only authorised entities can access and use the network resources.
- **Key Management**: The node should have reliable key management protocols to generate, distribute, and update cryptographic keys used for secure communication.
- **Compliance and Certification**: The node should comply with relevant standards and undergo certification processes to validate its security and trustworthiness.

It is important to note that the specific requirements for trusted nodes within the EuroQCI may evolve as the national quantum communication projects (NatQCIs) progress, and standards are defined.

4.1.1 Trusted Nodes in the HellasQCI Project

In view of the absence of European requirements for the EuroQCI trusted nodes, the consortium of HellasQCI, in consultation with the National Security Authorities (NSAs) of Greece and its Security Advisory Board (SAB) applied a comprehensive framework for auditing and securing the HellasQCI trusted nodes.

In the case of the HellasQCI project, the trusted nodes constitute both:

- The relay nodes of the HellasQCI backbone networks (long-distance) from the Optical Ground Stations (OGS) to the Metropolitan test-sites (Athens, Thessaloniki, and Heraklion,Crete).
- The end nodes of the governmental sector.

The HellasQCI Trusted Nodes framework specifies mainly the physical security requirements of the sites and restrict the access of the unauthorised personnel to the premises and the quantum equipment. The HellasQCI framework is based on the following:

- **The National Industrial Security Regulation (NISR)**: The applicable legislative framework in Greece for the protection of premises, personnel, and classified information. NISR provides guidelines and requirements for securing physical facilities and premises where sensitive or classified information is stored or processed. This involves implementing access controls, surveillance systems, and other measures to prevent unauthorised access. In parallel, NISR ensures the safety and security of personnel. This encompasses the establishment of security protocols to be followed by the personnel.
- **ISO/IEC 27001**: The international standard for information security management addresses physical security and the security of personnel as critical components. This includes measures such as controlled entry, surveillance, and protection against environmental threats. The standard encourages organisations to implement safeguards to prevent unauthorised physical access to sensitive areas and recommends defining roles and responsibilities, conducting awareness training, and implementing measures to ensure that employees are aware of and adhere to security policies.
- **ITIL**: The Information Technology Infrastructure Library provides best practices for IT service management. For achieving an efficient IT service delivery at the end-nodes, a comprehensive understanding of physical security and personnel security need to be complemented with specific security standards and guidelines tailored to each organisation and regulatory requirements.
- **Trusted nodes Audits**: Audits play a crucial role in ensuring the integrity and security of trusted nodes that host sensitive equipment. In the realm of secure facilities, where the protection of premises and classified material is paramount, audits serve as a systematic and comprehensive means of evaluating the effectiveness of security measures. By subjecting trusted nodes to regular audits, organisations can identify vulnerabilities, assess compliance with security protocols, and mitigate potential risks. Audits help to validate the implementation of rigorous access controls, physical security measures, and personnel training programs, ensuring that the trusted nodes operate in alignment with established security policies and industry standards.

The scope of the audits to the HellasQCI trusted nodes is mainly to ensure compliance with NISR requirements. More specifically, the procedure under consideration includes the following steps:

- **Audit Checklist**: Create a detailed checklist based on regulatory requirements (NISR), industry best practices, and specific security policies. The checklist should be focused on physical security aspects and security of personnel. The questions should be posed to the site representatives.
- **Review Security Policies and Procedures**: Examine existing security policies and procedures to ensure that they are aligned with the regulatory requirements of NISR.
- **Physical Security Assessment**: Evaluate physical security measures, such as access control systems, perimeter security, surveillance cameras, and intrusion detection systems.
- **Personnel Security Assessment**: Review personnel security measures, including access authorisation procedures and training programs.
- **Risk Assessment**: Identify potential threats and vulnerabilities and prioritise areas for improvement.
- **Generate Audit Report**: Compile findings into a comprehensive audit report, including identified vulnerabilities, areas of non-compliance, and recommendations for improvement.
- **Implement Corrective Actions**: Work with relevant stakeholders to implement corrective actions based on the audit findings and make the trusted nodes suitable for hosting the QKD equipment.

4.2 QKD Nodes for Research and Education

When it comes to QKD as a possible service in the NREN community that serves research and education, the requirements and restrictions on what could constitute a trustworthy QKD node should be defined. If such a service were to be established, it might not include all NRENs, as some of them may decide to focus on Post Quantum Cryptography and rely on updating existing complexity-based algorithms for the secure exchange of cryptographic keys.

However, for an implementation of QKD and QKD-trustworthy relay nodes, the first pilot phase of such a service could be based on an approach and conditions that would guarantee reasonably strengthened nodes that are suitable for experimental environments. The requirements and restrictive conditions could then be elevated in a second phase – possibly once official certification standards have been published.

The following sections provide a potential checklist that could serve as an initial requirement to obtain reasonably accredited relay nodes.

4.2.1 Physical Security Requirements

The placement of QKD nodes should be at locations close enough to neighbouring QKD nodes with noise levels that would guarantee satisfactory secure key rates. The buildings housing the nodes should be without windows to prevent any type of light injection attacks, and should be shielded to prevent electromagnetic emanations (for more details, see Section 5). The Federal Office for Information Security in Germany warns that typical building materials such as concrete walls or glass do not offer efficient shielding and that only close-meshed steel can sufficiently protect against electromagnetic radiation [FOIS; BSI-2023a; BSI-2023b]. They offer specific guidelines for the shielding of buildings for high-security use cases in document BSI TR-03209 - 1 but acknowledge that for civilian use cases there are no binding limits for electromagnetic emanations [BSI-TR].

For elemental threats such as fire, flooding or storms, standard housing requirements are already in place for NREN nodes would also apply. In fact, possible locations for a pilot phase for experimental QKD in the GÉANT community could be current NREN nodes, where security measures and monitoring are mostly in effect for access control, power supply, climate control, sprinkler systems, and so forth, and the appropriate reporting and

automated alerting systems are well defined and are subject to regular functional tests including preventive training of staff.

These measures should include Fibre-to-the-Building (FTTB) as well as Fibre-to-the-Desk (FTTD) requirements. Access control should not only prevent theft of hardware or software by illegally accessing buildings but should also include access control to all types of interfaces; hardware should not provide removable data storage and USB or SD-card ports. Cell phone use should be prohibited at locations of trustworthy QKD nodes.

4.2.2 Key Availability Requirements

For a relay node to be a trustworthy node means that it should reliably provide its purpose around the clock. For a QKD node this means that the QKD service is provided and that the node is hardened so that in the case of attacks special measures come into play making sure that the data is protected as long and as much as possible.

For secure quantum communication, the availability of the key material at each QKD node is of the highest priority. The process of generating key material must be able to keep up with the demand for keys from applications and the key store must not run dry, because this would essentially mean that the transmission on that link is stopped. At the same time key stores must be protected to prevent the illegal extraction of key material [SCH-2012].

The availability of keys can be affected by denial-of-service attacks: since the key generation process is aborted as soon as unusually high error rates are detected, such an attack may be carried out by actively breaking or bending cables, or the adversary may just passively listen and thus produce higher error rates [RAS-2011]. However, such a denial-of-service attacks can be mitigated by using remaining key material as efficiently as possible before the key store runs empty, for example, for alerting the network management centre with a secured message and then switching to classical encryption as a fallback [RAS-2009], [SCH-2010]. For a QKD service in the R&E community such mitigation policies and reinforcement strategies would have to be considered.

4.2.3 Authentication Requirements

For any node storing and relaying information, loss of data availability, confidentiality, integrity or correctness of data must be prevented. The correctness of data is tightly linked with the assurance that the correctly authenticated person (or software agent) with the appropriate permissions is involved when data is accessed. Authentication is essential between two users, Alice and Bob, in a point-to-point link, but this concept must be extended to the whole quantum channel with messages being relayed hop-by-hop. A quantum channel is authenticated if each message going across this link is authenticated – a process known as continuous authentication [SCH-2012]. With continuous authentication spoofing attacks can be prevented where an adversary with illegitimate access to the channel can gain information and interfere, i.e., an initial authentication between Bob and Alice is not enough, it must be assumed that active attacks (spoofing or DDoS, or other types of interference) can always happen [GIL-2000].

Most quantum identity authentication protocols are based on pre-shared keys or secrets between Bob and Alice, i.e., Bob recalculates a given authentication tag based on a secret previously shared with Alice to see if Alice is indeed the sender of the message. Authentication must pertain to service providers and institutions as well and not be limited to Bob and Alice.

In QKD networks with multiple nodes, trust relationships and a security framework must be set up for cooperation between nodes that ensure that the security capabilities of the trusted QKD relays can be kept on a sufficiently high level to satisfy the security conditions agreed by all network members. This does not necessarily mean that all nodes must share secrets between each other: there are methods for the authentication of a transmission with only neighbouring nodes sharing secrets [RAS-2010]. Similarly, signature schemes can be constructed based on point-to-point QKD as part of a multiparty QKD consensus scheme for the establishment of trust relationships in QKD networks [LUO-2023]. Multi-party QKD usually involves Quantum Secret Sharing (QSS) protocols and quantum digital signatures [WIL-2019].

Authentication without shared secrets is based on the notion that if Alice does not wish to share a secret with Bob, it is still possible to refer Bob to others that already have shared secrets with Alice and who can then function as verification authorities for Bob. Bob may query all these nodes and can use multiple paths to convince themselves that the authentication tag is correct [RAS-2010].

4.2.4 Standardisation and Certification Requirements

As device certifications and standardisations become available, QKD networks should enforce and verify compliance at all QKD nodes.

4.2.5 Pilot Phase for Multi-Domain QKD

In a first experimental phase a QKD network with trustworthy nodes for research and education purposes could be set up and tested following a gradual approach with increasing (but initially still imperfect) security conditions/requirements that could offer interesting perspectives on policies, guidelines and checklists.

Potential first NREN use cases may be monitoring with QKD and hardening of the control plane. A similar use case is described for trusted node QKD at an electrical utility where data from grid sensors but also commands from the operations centre require a trustworthy communications security infrastructure [EVA-2021].

5 Understanding Security

As described above, the naturally occurring properties of quantum mechanics make the QKD method secure as they enable sender and receiver to find out about any eavesdropping that may have occurred during the exchange process of the symmetric keys. Any security limitations stem from the fact that QKD devices may not behave exactly like the QKD model and may leak certain properties that can be exploited by eavesdroppers. QKD has two families of protocols:

- Discrete-Variable (DV) QKD, based on single-photon detection.
- Continuous-Variable (CV) QKD. based on coherent detection (optical homodyne or heterodyne detection) [QI-2021], [GIL-2023].

These QKD protocols have different methods of implementation. Protocols using Prepare-and-Measurement (PM) use measurements of unknown single quantum states, and are capable of detecting eavesdropping and how much of the data was potentially affected by it. Another method of implementation comprises Entanglement-Based (EB) protocols where entangled photon pairs are used. A third category are Device-Independent (DI) and Measurement-Device-Independent (MDI) protocols that employ Bell state measurements.

5.1 Prepare-and-Measurement Schemes

In prepare-and-measurement schemes such as BB84 , photon polarisation is used with one rectilinear base with vertical polarisation at 0° and horizontal polarisation at 90°, and a second diagonal base with vertical polarisation at 45° and horizontal polarisation at 135° [BEN-2014]. This scheme then allows the assignment of the bit value “0” to a horizontally polarised photon and a bit value of “1” to a vertically polarised photon, for instance.

During the key distribution process, the sender (Alice) creates a series of random bits (photons representing 0 or 1 in either basis - qubits) over a quantum transmission channel. The receiver (Bob) measures the polarisation of these photons without knowing the base that the sender used, i.e. the receiver randomly selects either of the two bases and notes each selected base and obtained value (see Figure 5.1, bottom layer). After all qubits are exchanged, the sender and receiver can discuss over a classical (authenticated) channel which bases were selected for measurement and drop any bits where the receiver did not measure with the same base as the sender (see Figure 5.1, sifting process) [MIN-2010], [DEN-2011].

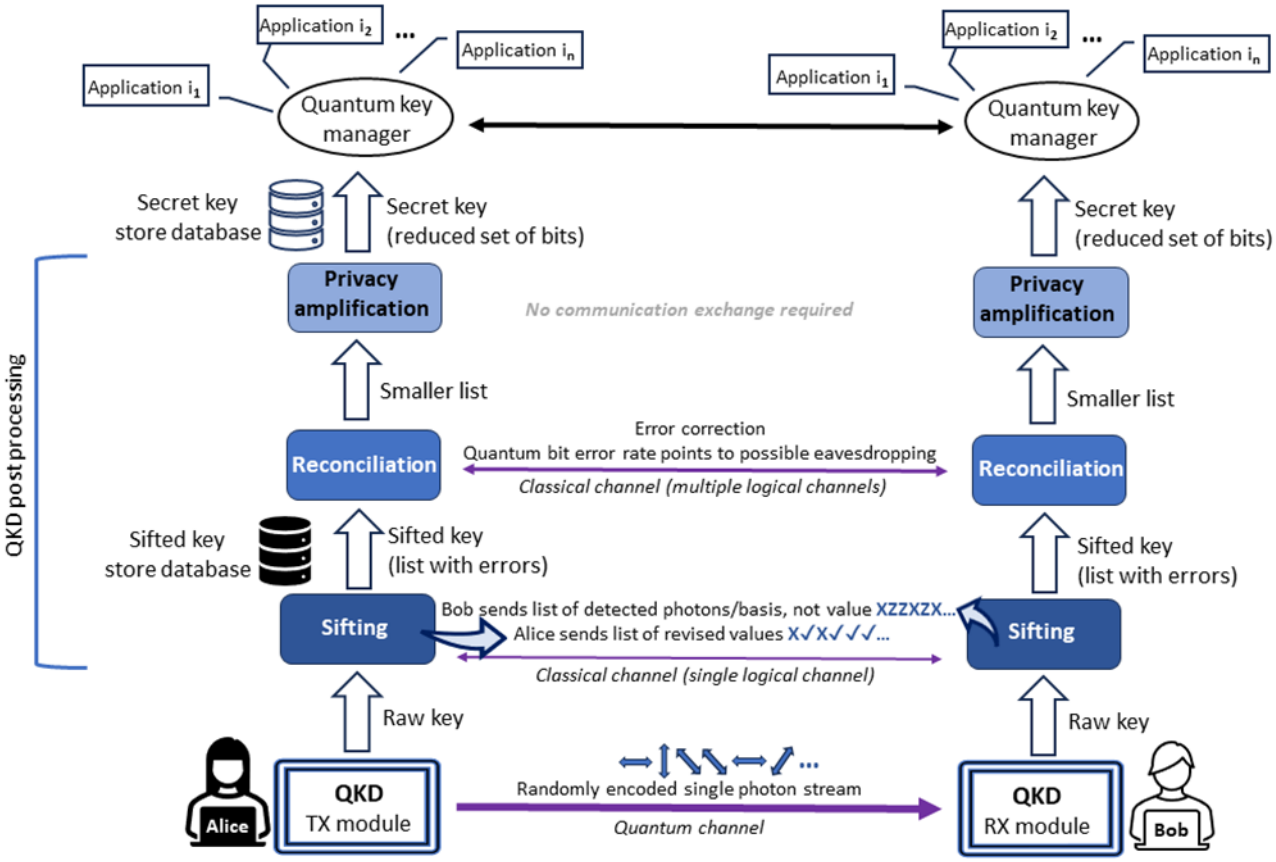

Figure 5.1: Stages of BB84

This key sifting is part of QKD post-processing and allows the sender and receiver to come up with secure keys because an eavesdropper must guess each measurement base with a 50% chance of selecting the wrong base, which would lead to the receiver measuring a different value from the one the sender created. In other words, physical measurements without applying the correct bases lead to errors in information retrieval and leave the eavesdropper without an exact copy of the state of each qubit. The more bits that are sent, publicly compared and discarded, the higher is the probability to detect an eavesdropper. In the end, the key is composed of all bits that remain after the publicly compared bits were discarded [Win-2010]. In an ideal world and without any eavesdroppers, this sifted (raw) key should be identical for both sender and receiver. However, eavesdropping and noise in the environment affect the qubit exchange, and additional post-processing procedures are necessary, such as error estimation and error correction (Figure 5.1, key reconciliation) on the raw sifted key. Sender and receiver can determine a Quantum Bit Error (QBER) rate by directly comparing and discarding bits that may have been affected by errors from imperfections of the single photon source, from detectors or the noise of the Quantum channel (Brillouin scattering, polarisation mode and chromatic dispersion). If the exchange shows a QBER beyond a certain threshold, the process will have to be repeated. To correct these naturally occurring errors, the sender computes a syndrome of the sifted key and sends it to the receiver. Post-processing also includes a step called privacy amplification which is an effort to minimise the potential information that an eavesdropper may have gained about the key. After all post-processing procedures have been applied to the sifted raw key the final secure key is obtained [NOT-2020].

5.2 Entanglement-Based Protocols

In entanglement-based protocols (such as first proposed by Artur Ekert in 1991 [EKE-1991]), a source generates entangled photon pairs and sends one half to Alice and the other half to Bob. Both Alice and Bob then measure polarisation along different axes independently from each other and later publicly announce the different angle orientations they used. Bits where the angular orientation was the same are then used as bits for the key, see Figure 5.2 [WAK-2002], [JEN-1999].

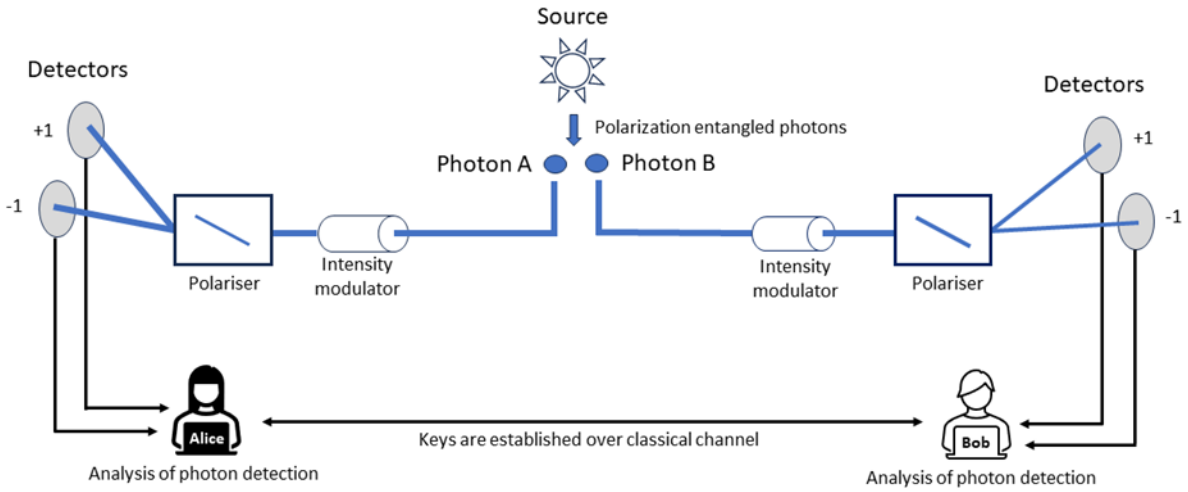

Figure 5.2: Alice and Bob each individually analyse one half of an entangled photon pair for keys

5.3 Security Considerations on the Detection Side

The amount of the final secure key material that is needed determines the number of quantum bits that have to be sent over the quantum channel for the generation of the initial raw key and must also take into account the material needed for post-processing [MEH-2015], [FUN-2010]. For One-Time-Pad (OTP), encrypting keystreams of random digits are merged with the unencrypted text one by one, i.e. OTP methods require as much key material as the amount of the plain text (Figure 5.3) [MEH-2015], [XU-2015]. Important security considerations are, therefore, if enough key material can be generated, or if there is a risk of the link being cut because key storage reservoirs run dry.

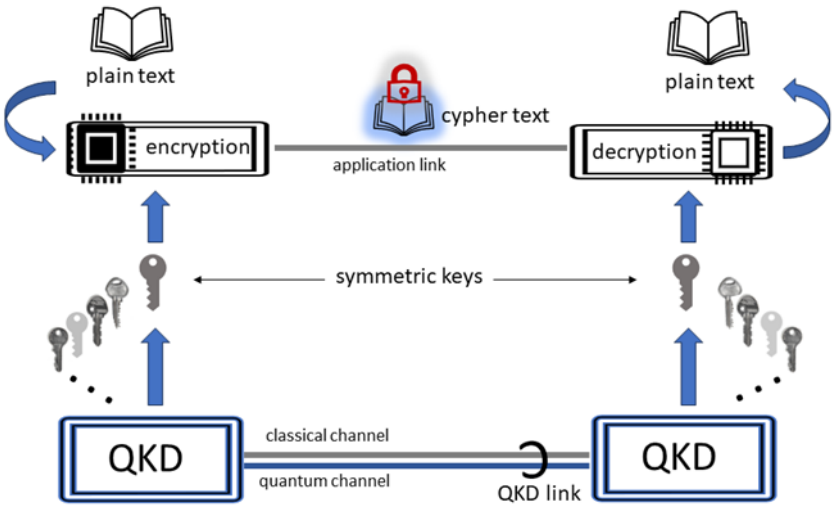

Figure 5.3: For OTP key material is merged with unencrypted text [ITU-2019]

Although the QKD algorithm is information-theoretically secure, attackers may gain illegal knowledge of the key by exploiting flaws in the implementations of the devices in side-channel attacks where cryptography is broken because the system inadvertently leaks information [FUN-2010], [RAM-2021].

However, 100% of the sifted key and syndrome in the key reconciliation process can be recovered by analysing a single power consumption trace measured during the syndrome computation on a sender's side [PAR-2021]. Simple power analysis can be used for directly interpreting measurements of power consumption of cryptographic operations, and their instruction sequence may also yield information on the data values that are being processed [KOC-1999].

Similarly, electromagnetic radiation may be exploited when electrons move across semiconductor logic gates, which are constructed out of transistors and produce electromagnetic radiation when charge is applied or removed [KOC-1999]. The emissions of electromagnetic waves from the phase modulator can be exploited to interpret the four classes of bit and base combinations in the BB84 protocol during the raw key exchange [KIM-2018]. The amount of run time used for private key operations can be mis-used in eavesdropping efforts as well [KOC-1999], [DHE-1998].

Different kinds of timing side-channel attacks may also occur when Bob's environment has a mismatch in detector timing. Faked-state attacks or timeshift attacks are possible when Bob's single photon detectors are not perfectly aligned with each other (Figure 5.4). Bob will have two separate detectors (one for 0-bit values and another one for 1-bit values). For each incoming photon there is only a very small detection window of a few nanoseconds, and the arrival time of the photon should ideally correspond to the middle of that window so that the pulse can be registered. If there is a time shift between both detectors due to manufacturing variations, an eavesdropper could cut in line, and could intercept and measure the quantum states provided by Alice with random basis selection and replace them with faked states and send those on to Bob.

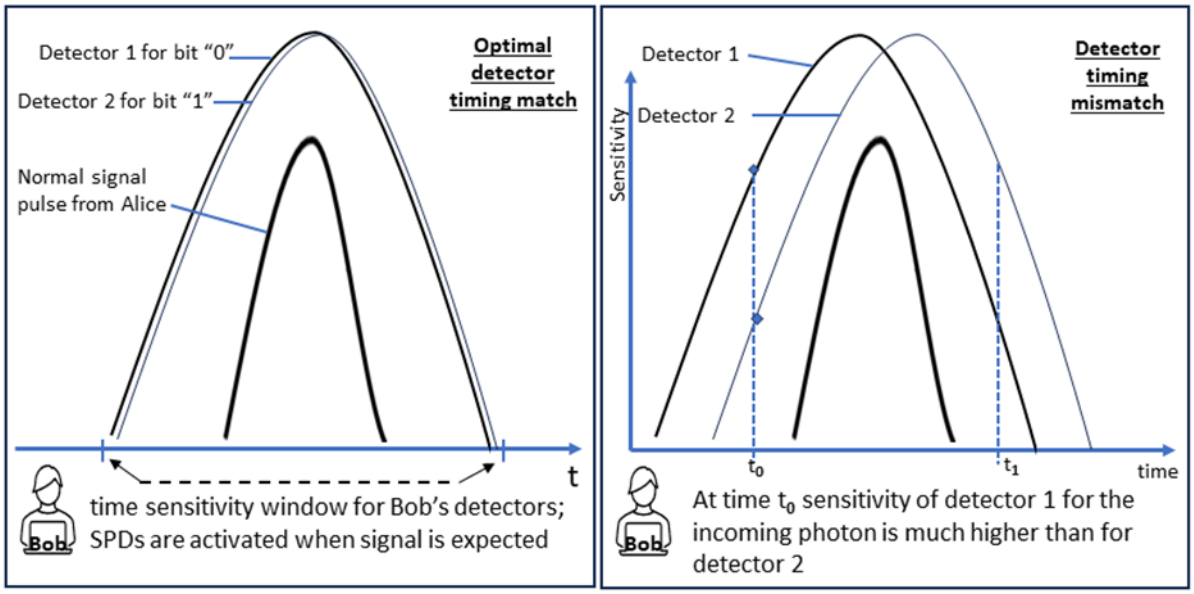

Figure 5.4: A single photon detectors (SPD) mismatch

In Figure 5.4 the left image shows optimal timing, while the image on the right is an example of timing mismatch of single photon detectors (SPD). At time t0 sensitivity of detector 1 for the incoming photon is much higher than for detector 2 and this can be exploited to intercept, replace the quantum states from Alice, and replace the new faked states that will then continue on to Bob [Qi-2005], [Mak-2006].

By generating very short light pulses and by controlling the timing of the faked states, the attacker can affect the sensitivity of the 0 and 1 detectors and thus, through blinding, can enforce that Bob's output in the end has identical bases and bit values as sent by Alice [Mak-2006; Qi-2005; DEN-2011; GER-2011; JAI-2011]. In this way the attacker would end up with the same raw key as Bob, and since the post-processing discussions over the classical channel are unencrypted apply the same sifting, key reconciliation, and privacy amplification procedures. An attacker's timeshifts to move the sender's signal forward or backward without even measuring can exploit the same detector imperfections (see Figure 5.5) [Qi-2005].

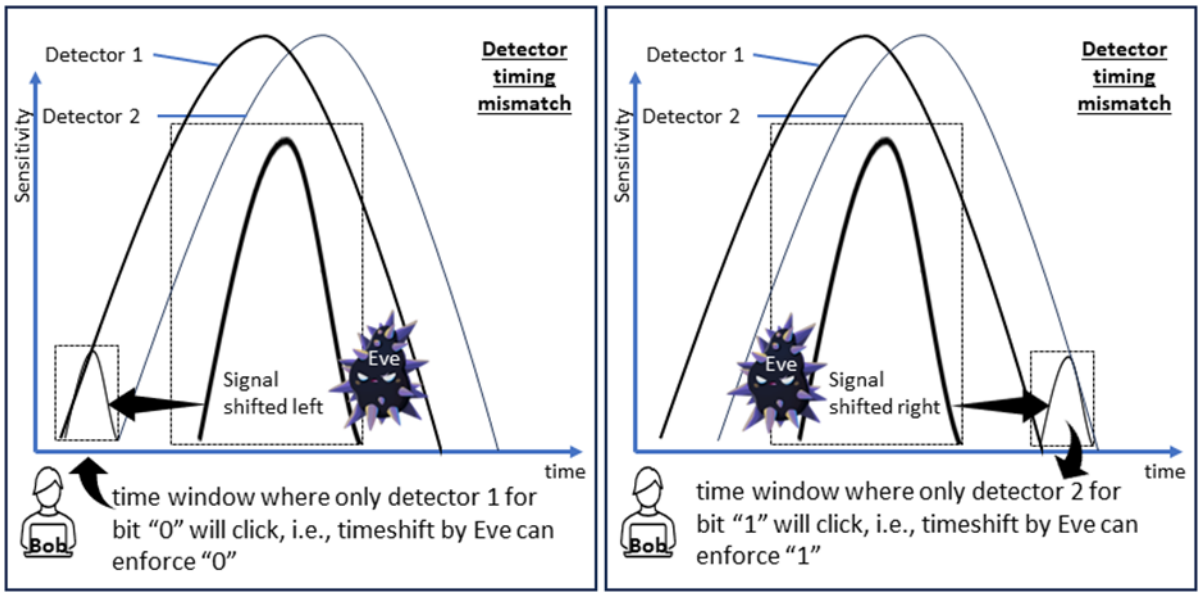

Figure 5.5: Exploiting misaligned detectors with timing mismatch

In Figure 5.5 eavesdropper Eve exploits misaligned detectors and timeshifts Alice's signal to enforce certain outcomes [Qi-2005], [MAK-2006].

A side-channel attack based on time that simply exploits the dead time of single photon detectors without the need for measurements of any qubits sent by Alice is also possible [WEI-2011]. The attacker sends attenuated light pulses of one of the polarisations of the protocol (H, V, +45° or −45°) into the quantum channel during the time interval when the single photon detector is inactive (its dead time), which is right after a detection event. Depending on intensity and polarisation, Bob is partially blinded on the selected polarisation and all events outside of Bob's time window will not be considered. Later, when it comes to the sifting phase, only bits will be selected from detectors that were not blinded, leaving the attacker with significant information.

5.4 Security Considerations at the Source

Some of the loopholes on the detection side can be avoided by using entanglement-based schemes where single-photon detection components are not used. But this still leaves light sources as potential loopholes [ZHA-2010]. Ideally, the light source should produce single qubit photons for prepare-and-measurement protocols, but light sources such as highly attenuated lasers sometimes produce multi-photon signals instead of single-photon signals. This allows an eavesdropper to measure the photon number of each signal and split multi-photon signals so that one copy can be kept for eavesdropping while the other one is sent to the receiver. This is referred to as a Photon-Number Splitting (PNS) attack [LO-2005]. In entanglement-based schemes, PNS attacks are not effective because it is very unlikely that two entangled photon pairs are produced simultaneously [WIN-2010], [JEN-1999]. PNS attacks can be detected by Alice producing decoy states in addition to the standard BB84 states [LO-2005]. These decoy states are not used for key generation but are only intended to be used for detecting eavesdroppers. Alice intentionally produces these decoy states as multi-photon pulses and randomly replaces regular signal pulses with them. In the end, the protocol must be aborted if the loss of the decoy-states is abnormally less than the loss of signal pulses [HWA-2003].

With light injection into the light source, phase randomisation can also be compromised. For example, if Alice produces laser pulses where the random phase of the pulse is determined by the seed photons originating from spontaneous emission (see Figure 5.6). If an eavesdropper injects additional photons in the semiconductor medium, these injected photons will also be amplified and end up affecting the phase of the laser pulse, i.e., the

seed photons will be partially from the external source and only partially from the spontaneous emission. If the additional photons by the eavesdropper are more than the photons from the spontaneous emission, the resulting phase is mainly influenced by the phase of the external photons and Alice will not realise that her signal laser does not produce randomly phased laser pulses [SUN-2015].

Such an attack slightly differs from Trojan horse attacks where an eavesdropper sends light pulses into the optical channel that connects Alice and Bob, and uses the back-reflected light to analyse the information from Alice (see Figure 5.6) [SUN-2015], [GIS-2002]. This is possible if the eavesdropper's photons reach Alice's encoding system, the Trojan photons are encoded with the same information as Alice's photons, and then some of them may end up reflected back to the eavesdropper (indicated by the narrow arrow in Figure 5.6) [LUC-2015]. Trojan horse attacks can be prevented by technical measures such as activating phase or polarisation modulators, but only for the time interval when Alice's intended signal is there and by using filters for the operating wavelengths.

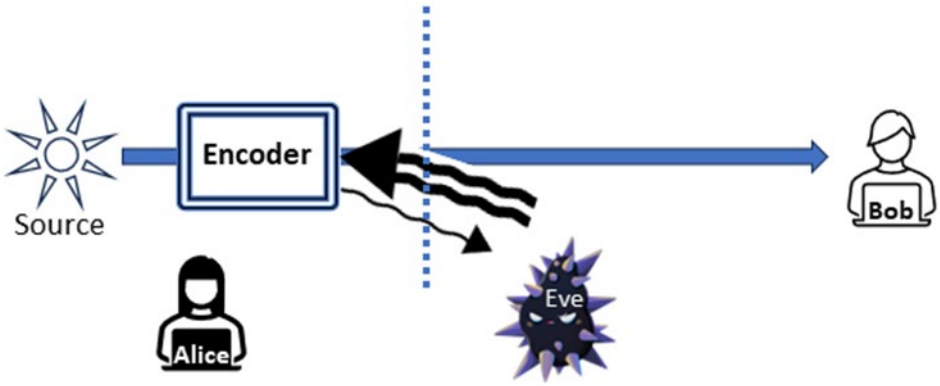

Figure 5.6: Trojan horse attack

5.5 Device Certification

In view of the many examples of possible device imperfections and manipulations on both detector side and source side, it is clear that device certifications are absolutely essential for secure QKD. Some imperfections may be sufficiently small for security bounds for a secure QKD protocol to still be established, but the difficulty of such procedures is that the systems must deal with states of light that are difficult to detect, have more degrees of freedom, and are not as well-defined as binary strings of bits in classical systems [MAK-2006].

Early certification efforts were emission approval tests, such as the Transient Electromagnetic Pulse Emanation Standard (TEMPEST) to counter eavesdropping on the electromagnetic emanations of digital equipment [TEM-1993], [BSI-2023]. In April 2023 ETSI released ETSI GS QKD 016 V1.1.1 (2023-04), a QKD protocol protection profile for the security evaluation of QKD modules [ETS-2023], [ETS-2023a]. A reference for evaluation criteria and requirements for QKD security proofs for QKD systems can be found in ETSI document ETSI GS QKD 005 V1.1.1 (2010-12) [ETS-2012]. Security proofs must match exactly the protection protocols to be able to show that a device is in range and can be considered safe.

5.6 DI-QKD and MDI-QKD Key Distribution Schemes

To avoid most of the device loopholes described above, two new quantum key distribution schemes were developed: the entanglement-based device-independent (DI)-QKD and the measurement-device-independent (MDI)-QKD.

In DI-QKD, entanglement detection is only based on measurement outcomes and their Bell-like correlations, and Alice and Bob can make these measurements independent from the devices that generated the quantum particles [CHE-2021]. In the scheme, pairs of entangled quantum particles are produced where one particle from each pair is for Alice and one for Bob. By measuring their particles, both Alice and Bob produce a key of a string of 1s and 0s. This is possible because each particle from Alice is entangled with the particle that Bob holds of the correlated pair and will thus yield the same result. To make sure that their channel is still secure Alice and Bob sporadically perform a test based on Bell's theorem to check if specific statistical correlations still hold (security is guaranteed if the Bell inequality is violated). If there is a mismatch and their particles are no longer entangled, then security can no longer be assured. In that case they would discard their measurements and restart the process. As Bob and Alice can perform these measurements without knowing anything about the device that produced them, the process is device independent [CHE-2022; WAN-2020; LO-2011]. Experiments with DI-QKD have been conducted, but with very limited distances (below 1km) and with very restricted key generation rates.

MDI-QKD is different from DI-QKD as it does not depend on the violation of a Bell inequality; in a way it is a time-reversed scheme of the QKD protocol where Alice does not send bipartite entangled states to Bob, but both Bob and Alice produce entangled states and send them to a third party (e.g., an untrusted relay). This third party then performs a Bell state measurement on the incoming signals that force them into Bell states that are correlated between Alice and Bob, and announces the measurement results over a public channel (see Figure 5.7). Alice and Bob can then use the data for keys, without even having to trust the third party, select the data for the key where they used the same basis (through an exchange over an authenticated public channel), and discard the rest. If the third party did send flawed data, it would impact the extraction of a key, because the correlation between Alice's and Bob's data would not be sufficient, and the process would have to be started over [DIA-2015].

Alice and Bob can also employ decoy state methods to verify that the obtained bit strings are adequately correlated [LO-2011]. Thus MDI-QKD requires Bob and Alice to have sources that are isolated with no information leakage from the transmitters (intensity and phase modulators) which is difficult to apply in practice [WAN-2020, OTT-2020, YE-2019]. The QKD transmitter must be able to not only on-off modulate each time bin within a state, but must also be able to modulate the phase in between the time bins and, in addition, is required to vary the intensity level so that the decoy states can be generated. Currently these intensity levels can be obtained by placing intensity modulators after a light source. In addition, phase modulators are used for encoding phase information. Both modulator types are based on LiNb03 crystals and are still very bulky, preventing QKD systems from being more compact [LO-2023].

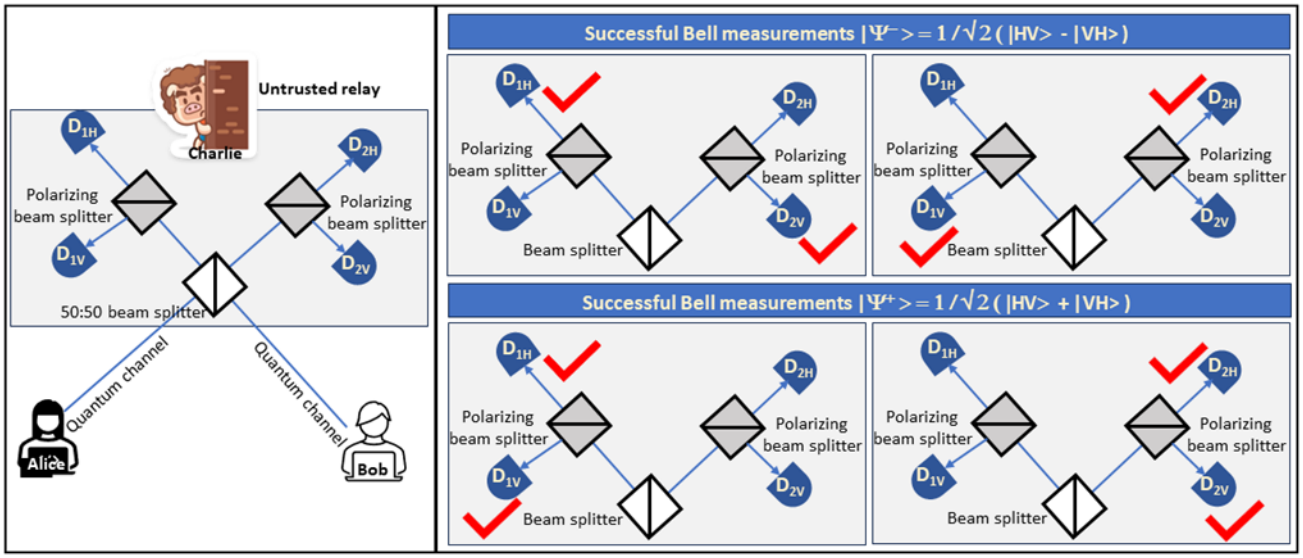

Figure 5.7: Bell state measurements on the input photons

In Figure 5.7, Charlie at the untrusted relay node performs Bell state measurements on the input photons from Alice and Bob. The measurement is successful when exactly two detectors click, so either D1H and D2V or D1V and D2H (for |Ψ-> = 1 / 2√(|HV> - |VH>) or D1H and D1V or D2H and D2V (for |Ψ+> = 1 / 2√(|HV> + |VH>) [LO-2011]. Further information is available online [Class].

In comparison to DI-QKD, with MDI-QKD better key rates and also larger distances can be achieved and all device loopholes on the detection side no longer apply, leaving sources as the only problem as they could be affected by information leakage or light injection attacks [ZEB-2018; WAN-2020; PAN-2020]. With the discrete-variable version of the MDI-QKD protocol longer distances can currently be achieved, but still with relatively low key generation rates. The continuous-variable version of MDI-QKD is capable of generating high key rates, but requires Alice and Bob to be relatively close to the third-party relay [DIA-2015], [YE-2019].

5.7 Twin-Field QKD

To overcome both distance and key rate limitations, Twin-Field (TF) QKD was proposed (and several variants such as phase-matching QKD, sending-or-not-sending QKD, and no phase post-selection TF-QKD (NPP-TFQKD), which can be regarded as an MDI-QKD scheme with single-photon Bell state measurement [LUC-2018; LI-2019; LIN-2018; HU-2022; CUI-2019; YIN-2019].

In TF-QKD, the information is not carried by a single photon, but by weak-coherent fields. Alice and Bob generate pairs of these phase-randomised weak-coherent fields which are combined and measured by a third party (single-photon Bell state measurement). Twin-Fields are the fields that were communicated to have the same random phase and are used to extract the key. For the correction of raw keys, Alice and Bob announce the random phase of each pulse. The new scheme can be implemented with current technology and noise levels over distances of hundreds of kilometres [LUC-2018], [WAN-2022]. Recently proposed mode-pairing quantum key distribution does not have the requirements of phase locking and phase tracking as is necessary for TF-QKD, but can offer significant gains on key rates with an additional post-processing step [WAN-2023]. Further developments in these areas are ongoing.

5.8 End-to-End Security

Apart from the exploitation of device imperfections, end-to-end security can also be compromised by other means. Even if the QKD channel is secure, Distributed Denial of Service (DDoS) attacks on the optical link may lead to the QKD protocol being aborted. A simple way to carry out such an attack is to increase the error rate on the transmission channel (presuming the attacker somehow gained access to the fibre) [PRI-2017; TEL-2023; HUG-2018]. Although this is easily detectable, the quantum signal will have to be rerouted. In some cases, it may also not be entirely clear if disturbances are actual DDoS attacks or excessive noise in the channel.

Another way to cause disruptions are man-in-the-middle attacks if identity authentication is not properly done, and Bob is not actually Bob. For successful implementation of QKD, the scenario must be avoided where an eavesdropper could somehow separate Alice from Bob, i.e., establish a separate channel between Alice and the eavesdropper, and then another channel from the eavesdropper to Bob. Without identity authentication Bob and Alice would create keys with the eavesdropper without realising they are not talking directly to each other [DUT-2021]. In order not to compromise the secure QKD protocol, the identity authentication protocol should also be based on quantum resources. Most Quantum Identity Authentication (QIA) protocols are based on pre-shared keys or secrets between Bob and Alice, and the authentication verification process must ensures that no single bit is revealed to the eavesdropper to avoid that the eavesdropper may learn from a series of protocol runs [ZAW-2019]. The pre-shared key must be encoded and stored in a quantum state so that any eavesdropper gaining illegal access to the key cannot copy it without detection due to the no-cloning theorem [DUT-2021].

Apart from Quantum identity authentication, Quantum authentication, in general, also comprises the areas of Quantum Message Authentication (QMA) and Quantum Entity Authentication (QEA) [PRI-2017, LI-2022]. The authentication of data or messages verifies that the data sent is indeed unchanged and has not been tampered with, whereas quantum entity authentication focuses on the verification of cloud services or network providers that are third parties that could potentially also leak information [CRA-2019], [KAN-2018].

The discussions above demonstrate that real quantum security is an abstract principle, and it is unrealistic to expect a technological implementation with infinite security. Nevertheless, as QKD relies on a method of encryption that is not based on mathematics, but rather on the naturally occurring properties of quantum mechanics, its security depends on the capabilities of the eavesdropper at the time of the key exchange. Storing and future decoding as in complexity-based systems does not apply and is a clear advantage [GIS-2002].

6 Conclusions

This document shed light on several ongoing issues related to Quantum Key Distribution with an emphasis on practical challenges that NRENs may encounter. After a short discussion comparing the pros and cons of QKD and PQC, the most recent standardisations and recommendations were listed, which also included a focus on interoperability. A brief introduction to monitoring was provided to give NRENs a rough guide on how to control QKD networks.

This was followed by an overview of ongoing QKD network activities, with initiatives that are part of EuroQCI, but also with nationally funded QKD projects. As trusted nodes are a main consideration for QKD networks at the moment, the document also discussed availability and authentication issues in the context of trusted nodes.

The final section provided insights into device implementations and their vulnerabilities and showed why device certifications are very important.

With this overview the document provided a summary of issues in an effort to help the reader get a fast understanding of the current state-of-the art. With continuous hardware developments by vendors and also with evolving standardisations and certifications, the way forward should be to keep constant track of this changing field, the new opportunities it may offer, and the new challenges that may arise.

References

[BEN-2014] Bennett, Charles H.; Brassard, Gilles (2014): Quantum cryptography: Public key distribution and coin tossing. In Theoretical Computer Science 560, pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025. https://arxiv.org/abs/2003.06557

[BER-2017] Bernstein, Daniel J.; Lange, Tanja (2017): Post-quantum cryptography. In Nature 549 (7671), pp. 188–194. DOI: 10.1038/nature23461. https://www.nature.com/articles/nature23461

[BRI-1998] Briegel, H.-J.; Dür, W.; Cirac, J. I.; Zoller, P. (1998): Quantum repeaters for communication. https://arxiv.org/abs/quant-ph/9803056

[BSI-2023] Emission tests for devices. Federal Office for Information Security (BSI), Germany. https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Geheimschutz/Abstrahlsicherheit/Abstrahlpruefungen-von-Geraeten/abstrahlpruefungen-von-geraeten_node.html

[BSI-2023a] BSI: Das Nationale Zonenmodell der Abstrahlsicherheit https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Geheimschutz/Abstrahlsicherheit/Das-Nationale-Zonenmodell/das-nationale-zonenmodell.html

[BSI-2023b] BSI: IT-Grundschutz-Kompendium https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

[BSI-TR] BSI TR-03209 – 1: Elektromagnetische Schirmung von Gebäuden https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03209/TR-03209_node.html

[CHE-2021] Chen, Geng; Zhang, Wen-Hao; Yin, Peng; Li, Chuan-Feng; Guo, Guang-Can (2021): Device-independent characterization of entanglement based on bell nonlocality. In Fundamental Research 1 (1), pp. 27–42. DOI: 10.1016/j.fmre.2021.01.004. https://www.sciencedirect.com/science/article/pii/S2667325821000042

[CHE-2022] Chen, Sophia: Hiding Secrets Using Quantum Entanglement. Physics 15, 116. July 27, 2022. https://physics.aps.org/articles/v15/116

[Class] https://e-academy.geant.org/moodle/course/view.php?id=372 (requires login)

[CRA-2019] Crawford, Heather; Atkin, Steven: Quantum Authentication: Current and Future Research Directions. https://wayworkshop.org/2019/papers/way2019-crawford.pdf

[CUI-2019] Cui, Chaohan; Yin, Zhen-Qiang; Wang, Rong; Chen, Wei; Wang, Shuang; Guo, Guang-Can; Han, Zheng-Fu (2019): Twin-Field Quantum Key Distribution without Phase Postselection. In Phys. Rev. Applied 11 (3). DOI: 10.1103/PhysRevApplied.11.034053. https://arxiv.org/abs/1807.02334

[DEN-2011] Denny, Travis (2011): Faked states attack and quantum cryptography protocols. https://arxiv.org/abs/1112.2230

[DHE-1998] Dhem, J.-F.; Koeune, F.; Leroux, P.-A.; Mestre, P.; Quisquater. J.-J.; Willems, J.-L.: A practical implementation of the timing attack. UCL Crypto Group Technical Report Series. Technical Report CG-1998/1. https://www.cs.jhu.edu/~fabian/courses/CS600.624/Timing-full.pdf

[DIA-2015] Diamanti, Eleni; Leverrier, Anthony (2015): Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. In Entropy 17 (12), pp. 6072–6092. DOI: 10.3390/e17096072. https://arxiv.org/abs/1506.02888

[DivQSec] https://divqsec.de/en/network/

[DOW-2020] Dowling, Benjamin; Hansen, Torben Brandt; Paterson, Kenneth G. (2020): Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. In Jintai Ding, Jean-Pierre Tillich (Eds.): Post-Quantum Cryptography, vol. 12100. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 483–502. https://pure.royalholloway.ac.uk/en/publications/many-a-mickle-makes-a-muckle-a-framework-for-provably-quantum-sec

[DUT-2021] Dutta, Arindam; Pathak, Anirban (2021): A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice? https://arxiv.org/abs/2112.04234

[EuroQCI] https://euroqci-spain.eu/

[EKE-1991] Ekert, A. K. (1991): Quantum cryptography based on Bell's theorem. In Physical review letters 67 (6), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. https://doi.org/10.1103/PhysRevLett.67.661

[ETS-2012] ETSI GS QKD 005 V1.1.1 (2010-12): Quantum Key Distribution (QKD); Security Proofs. https://www.etsi.org/deliver/etsi_gs/qkd/001_099/005/01.01.01_60/gs_qkd005v010101p.pdf

[ETS-2023] ETSI GS QKD 016 V1.1.1 (2023-04): Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

[ETS-2023a] ETSI releases World First Protection Profile for Quantum Key Distribution. April 27, 2023. https://www.etsi.org/newsroom/press-releases/2222-etsi-releases-world-first-protection-profile-for-quantum-key-distribution

[ETSI-ISG-QKD] ETSI - INDUSTRY SPECIFICATION GROUP (ISG) ON QUANTUM KEY DISTRIBUTION (QKD) https://www.etsi.org/committee/1430-qkd

[EVA-2021] Evans, Philip G.; Alshowkan, Muneer; Earl, Duncan; Mulkey, Daniel D.; Newell, Raymond; Peterson, Glen et al. (2021): Trusted Node QKD at an Electrical Utility. In IEEE Access 9, pp. 105220–105229. DOI: 10.1109/ACCESS.2021.3070222. https://ieeexplore.ieee.org/document/9405393

[FOIS] https://www.bsi.bund.de/EN/

[FUN-2010] Fung, Chi-Hang Fred; Ma, Xiongfeng; Chau, H. F. (2010): Practical issues in quantum-key-distribution postprocessing. In Phys. Rev. A 81 (1). DOI: 10.1103/PhysRevA.81.012318. https://arxiv.org/abs/0910.0312

[GER-2011] Gerhardt, Ilja; Liu, Qin; Lamas-Linares, Antía; Skaar, Johannes; Kurtsiefer, Christian; Makarov, Vadim (2011): Full-field implementation of a perfect eavesdropper on a

quantum cryptography system. In Nature communications 2, p. 349. DOI: 10.1038/ncomms1348.
https://www.nature.com/articles/ncomms1348

[GIL-2000] Gilbert, G.; Hamrick, M. (2000): Practical Quantum Cryptography: A Comprehensive Analysis (Part One).
https://arxiv.org/abs/quant-ph/0009027

[GIL-2023] Gillis, Alexander S.: What is quantum key distribution (QKD)? Retrieved August 23, 2023.
https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

[GIS-2002] Gisin, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo (2002): Quantum cryptography. In Rev. Mod. Phys. 74 (1), pp. 145–195. DOI: 10.1103/RevModPhys.74.145.
https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.74.145

[HU-2022] Hu, Xiao-Long; Jiang, Cong; Yu, Zong-Wen; Wang, Xiang-Bin (2022): Sending-or-not-sending twin field quantum key distribution with imperfect vacuum sources. In New J. Phys. 24 (6), p. 63014. DOI: 10.1088/1367-2630/ac7347.
https://iopscience.iop.org/article/10.1088/1367-2630/ac7347

[HUG-2018] Hugues-Salas, Emilio; Ntavou, Foteini; Ou, Yanni; Kennard, Jake. E.; White, Catherine; Gkounis, Dimitrios et al. (2018): Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN). OFC 2018 Conference. M2A.6. In: Conference, Optical Fiber Communication (2018): Optical Fiber Communication Conference. 11-15 March 2018, San Diego, California, United States. Washington, D.C., USA: OSA - The Optical Society (OSA technical digest (online)).
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8385709

[HWA-2003] Hwang, Won-Young (2003): Quantum key distribution with high loss: toward global secure communication. In Physical review letters 91 (5), p. 57901. DOI: 10.1103/PhysRevLett.91.057901.
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.91.057901

[IEEE-QC] IEEE Working Group (WG): Software-Defined Quantum Communication
https://sagroups.ieee.org/netsoft/home/qc/

[IETF-QIRG] ETF Quantum Internet Research Group (QIRG),
https://datatracker.ietf.org/group/qirg/about/

[ISO-IEC-JTC1-SC17] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection,
https://www.iso.org/committee/45306.html

[ITU-2019] ITU-T - Y.3800, Overview on networks supporting quantum key distribution, 2019.
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3800-201910-I!!PDF-E&type=items

[ITU-2023] ITU-T Work Programme, X.sec-QKDN-tn: Security requirements and designs for quantum key distribution networks - trusted node
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17988

[ITU-T-QIT4N] ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)
https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

[ITU-T-SG13] ITU-T Study Group 13 (SG13) - Future networks and emerging network technologies
https://www.itu.int/en/ITU-T/studygroups/2022-2024/13/Pages/default.aspx

[ITU-T-SG17] ITU-T Study Group 17 (SG17) - Security
https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[JAI-2011] Jain, Nitin; Wittmann, Christoffer; Lydersen, Lars; Wiechers, Carlos; Elser, Dominique; Marquardt, Christoph et al. (2011): Device calibration impacts security

of quantum key distribution. In Physical review letters 107 (11), p. 110501. DOI: 10.1103/PhysRevLett.107.110501.
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.107.110501

[JEN-1999] Jennewein, Thomas; Simon, Christoph; Weihs, Gregor; WeinfurterD, Harald; Zeilinger, Anton (1999): Quantum Cryptography with Entangled Photons. DOI: 10.48550/arXiv.quant-ph/9912117.
https://arxiv.org/abs/quant-ph/9912117

[KAN-2018] Kang, Min-Sung; Heo, Jino; Hong, Chang-Ho; Yang, Hyung-Jin; Han, Sang-Wook; Moon, Sung (2018): Controlled mutual quantum entity authentication with an untrusted third party. In Quantum Inf Process 17 (7). DOI: 10.1007/s11128-018-1927-5.
https://link.springer.com/article/10.1007/s11128-018-1927-5

[KIM-2018] Kim, Suhri; Jin, Sunghyun; Lee, Yechan; Park, Byeonggyu; Kim, Hanbit; Hong, Seokhie (2018): Single Trace Side Channel Analysis on Quantum Key Distribution. In : 2018 International Conference on Information and Communication Technology Convergence (ICTC). 2018 International Conference on Information and Communication Technology Convergence (ICTC). Jeju, 10/17/2018 - 10/19/2018: IEEE, pp. 736–739.
https://ieeexplore.ieee.org/document/8539703

[KLI-2022] Klink, K. van: Quantum Key Distribution in a Pan-European Network of National Research and Education Networks. Qualitative and Quantitative Aspects of Implementing a Quantum Key Distribution Network. University of Twente, The Netherlands, November 2022.
http://essay.utwente.nl/93637/1/van Klink_MA_EEMCS.pdf

[KOC-1999] Kocher, Paul; Jaffe, Joshua; Jun, Benjamin (1999): Differential Power Analysis. In Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, Michael Wiener (Eds.): Advances in Cryptology — CRYPTO' 99 vol. 1666. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 388–397.
https://link.springer.com/chapter/10.1007/3-540-48405-1_25

[KUM-2020] Kumar, Manoj; Pattnaik, Pratap (2020): Post Quantum Cryptography(PQC) - An overview: (Invited Paper). In : 2020 IEEE High Performance Extreme Computing Conference (HPEC). 2020 IEEE High Performance Extreme Computing Conference (HPEC). Waltham, MA, USA, 9/22/2020 - 9/24/2020: IEEE, pp. 1–9.
https://ieeexplore.ieee.org/document/9286147

[LAV-2022] Lavie, Emilien; Lim, Charles C.-W. (2022): Improved coherent one-way quantum key distribution for high-loss channels. DOI: 10.48550/arXiv.2206.08490.
https://arxiv.org/abs/2206.08490

[LI-2019] Li, Wei; Le Wang; Zhao, Shengmei (2019): Phase Matching Quantum Key Distribution based on Single-Photon Entanglement.
https://arxiv.org/abs/1906.06865

[LI-2022] Li, Xiang; Zhang, Kejia; Zhang, Long; Zhao, Xu (2022): A New Quantum Multiparty Simultaneous Identity Authentication Protocol with the Classical Third-Party. In Entropy (Basel, Switzerland) 24 (4). DOI: 10.3390/e24040483.
https://pubmed.ncbi.nlm.nih.gov/35455145/

[LIN-2018] Lin, Jie; Lütkenhaus, Norbert (2018): Simple security analysis of phase-matching measurement-device-independent quantum key distribution. In Phys. Rev. A 98 (4). DOI: 10.1103/PhysRevA.98.042332.
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.98.042332

[LO-2005] Lo, Hoi-Kwong; Ma, Xiongfeng; Chen, Kai (2005): Decoy state quantum key distribution. In Physical review letters 94 (23), p. 230504. DOI: 10.1103/PhysRevLett.94.230504.

https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.94.230504

[LO-2011] Lo, Hoi-Kwong; Curty, Marcos; Qi, Bing (2011): Measurement-device-independent quantum key distribution. DOI: 10.48550/arXiv.1109.1473. https://arxiv.org/abs/1109.1473

[LO-2023] Lo, Y. S.; Woodward, R. I.; Walk, N.; Lucamarini, M.; Marco, I. de; Paraïso, T. K. et al. (2023): Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution. In APL Photonics 8 (3), Article 036111. DOI: 10.1063/5.0128445. https://pubs.aip.org/aip/app/article/8/3/036111/2879070/Simplified-intensity-and-phase-modulated

[LUC-2015] Lucamarini, M.; Choi, I.; Ward, M. B.; Dynes, J. F.; Yuan, Z. L.; Shields, A. J. (2015): Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. In Phys. Rev. X 5 (3). DOI: 10.1103/PhysRevX.5.031030. https://journals.aps.org/prx/abstract/10.1103/PhysRevX.5.031030

[LUC-2018] Lucamarini, Marco; Yuan, Zhiliang; Dynes, James F.; Shields, Andrew J. (2018): Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters. DOI: 10.48550/arXiv.1811.06826. https://arxiv.org/abs/1811.06826

[LUO-2023] Luo, Yi; Li, Qiong; Mao, Hao-Kun; Chen, Nan (2023): How to Achieve End-to-end Key Distribution for QKD Networks in the Presence of Untrusted Nodes. https://arxiv.org/pdf/2302.07688.pdf

[MAK-2006] Makarov, Vadim; Anisimov, Andrey; Skaar, Johannes (2006): Effects of detector efficiency mismatch on security of quantum cryptosystems. In Phys. Rev. A 74 (2). DOI: 10.1103/PhysRevA.74.022313. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.74.022313

[MEH-2015] Mehic, Miralem; Niemiec, Marcin; Voznak, Miroslav (2015): Calculation of the Key Length for Quantum Key Distribution. In ElAEE 21 (6). DOI: 10.5755/j01.eee.21.6.13768. https://eejournal.ktu.lt/index.php/elt/article/view/13768

[MEH-2021] Mehic, Miralem; Niemiec, Marcin; Rass, Stefan; Ma, Jiajun; Peev, Momtchil; Aguado, Alejandro et al. (2021): Quantum Key Distribution. In ACM Comput. Surv. 53 (5), pp. 1–41. DOI: 10.1145/3402192. https://dl.acm.org/doi/pdf/10.1145/3402192

[MIN-2010] Mink, Alan; Frankel, Sheila; Perlner, Ray (2010): Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration. DOI: 10.48550/arXiv.1004.0605. https://arxiv.org/abs/1004.0605

[NOT-2020] Notz, Pascal Markus; Nikiforov, Oleg; Walther, Thomas (2020): Software bundle for data post-processing in a quantum key distribution experiment. https://doi.org/10.25534/tuprints-00014042

[OTT-2020] Ottaviani, Carlo; Spedalieri, Gaetana; Braunstein, Samuel L.; Pirandola, Stefano (2020): CV-MDI-QKD with coherent state: beyond one-mode Gaussian attacks. In IOPSciNotes 1 (2), p. 25202. DOI: 10.1088/2633-1357/ab92f6. https://iopscience.iop.org/article/10.1088/2633-1357/ab92f6

[PAN-2020] Pang, Xiao-Ling; Yang, Ai-Lin; Zhang, Chao-Ni; Dou, Jian-Peng; Li, Hang; Gao, Jun; Jin, Xian-Min (2020): Hacking Quantum Key Distribution via Injection Locking. In Phys. Rev. Applied 13 (3). DOI: 10.1103/PhysRevApplied.13.034008. https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.13.034008

[PAR-2021] Park, Dongjun; Kim, GyuSang; Heo, Donghoe; Kim, Suhri; Kim, HeeSeok; Hong, Seokhie (2021): Single trace side-channel attack on key reconciliation in quantum

key distribution system and its efficient countermeasures. In ICT Express 7 (1), pp. 36–40. DOI: 10.1016/j.icte.2021.01.013. https://www.sciencedirect.com/science/article/pii/S2405959521000138

[PRI-2017] Price, Alasdair B.; Rarity, John G.; Erven, Chris (2017): A quantum key distribution protocol for rapid denial of service detection. https://arxiv.org/abs/1707.03331

[QRX] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qr.x

[QuNet] https://qunet-initiative.de/

[QI-2005] Qi, Bing; Fung, Chi-Hang Fred; Lo Hoi-Kwong; Ma, Xiongfeng (2005): Time-shift attack in practical quantum cryptosystems. In Quantum Inf. Comput. 7, pp. 73–82. https://api.semanticscholar.org/CorpusID:15304129

[QI-2021] Qi, Bing (2021): Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection. In Phys. Rev. A 103 (1). DOI: 10.1103/physreva.103.012606. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.103.012606

[RAM-2021] Rambus Press: Side-channel attacks explained: everything you need to know. October 14, 2021. https://www.rambus.com/blogs/side-channel-attacks/

[RAS-2009] Schartner, Peter; Rass, Stefan (2009): How to overcome the 'Trusted Node Model' in Quantum Cryptography. In : 2009 International Conference on Computational Science and Engineering. 2009 International Conference on Computational Science and Engineering. Vancouver, BC, Canada, 8/29/2009 - 8/31/2009: IEEE, pp. 259–262. https://ieeexplore.ieee.org/document/5283524

[RAS-2010] Rass, S.; Schartner, P. (2010): Multipath Authentication without shared Secrets and with Applications in Quantum Networks. In Book: Arabnia, Hamid (2010): SAM2010. Proceedings of the 2010 International Conference on Security & Management: Worldcomp'10 : July 12-15, 2010, Las Vegas, Nevada, USA. [Las Vegas, Nev.]: CSREA Press. https://www.syssec.at/user/themes/syssec-theme/downloads/SAM5203FINAL.pdf

[RAS-2011] Rass, Stefan; Schartner, Peter (2011): A Unified Framework for the Analysis of Availability, Reliability and Security, With Applications to Quantum Networks. In IEEE Trans. Syst., Man, Cybern. C 41 (1), pp. 107–119. DOI: 10.1109/TSMCC.2010.2050686. https://ieeexplore.ieee.org/document/5499109

[RYD-2022] Piotr Rydlichowski. QKD Days in Madrid Workshop. 2022. https://openqkd.eu/registration-qkd-days/

[SCH-2010] Schartner, Peter; Rass, Stefan (2010): Quantum key distribution and Denial-of-Service: Using strengthened classical cryptography as a fallback option. In: 2010 International Computer Symposium (ICS2010). 2010 International Computer Symposium (ICS 2010). Tainan, Taiwan, 12/16/2010 - 12/18/2010: IEEE, pp. 131–136. https://ieeexplore.ieee.org/document/5685533

[SCH-2012] Schartner, Peter; Rass, Stefan; Schaffer, Martin (2012): Quantum Key Management. In Jaydip Sen (Ed.): Applied Cryptography and Network Security: InTech. https://www.intechopen.com/chapters/32077

[SmartNets4E] Smart Networks for Everything (SmartNets4E) https://i2t.ehu.eus/en/resources/8/smartnets4e

[SQuaD] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/squad

[STA-2014] Stacey, William; Annabestani, Razieh; Ma, Xiongfeng; Lütkenhaus, Norbert (2014): The Security of Quantum Key Distribution using a Simplified Trusted Relay.

https://arxiv.org/abs/1408.4426

[STE-2023] René J. STEINER, EuroQCi Concept of Operations
https://digital-strategy.ec.europa.eu/en/euroqci-conops-concept-operations

[SUN-2015] Sun, Shi-Hai; Xu, Feihu; Jiang, Mu-Sheng; Ma, Xiang-Chun; Lo, Hoi-Kwong; Liang, Lin-Mei (2015): Effect of source tampering in the security of quantum cryptography. In Phys. Rev. A 92 (2). DOI: 10.1103/PhysRevA.92.022304.
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.92.022304

[TAN-2019] Tang, Xinke (2019): Optically Switched Quantum Key Distribution Network. Apollo - University of Cambridge Repository. Thesis.
https://api.repository.cam.ac.uk/server/api/core/bitstreams/3feb12ca-225e-4ef4-b9d4-2b4060d836c0/content

[TEL-2023] Telanova: DDos attacks against QKD networks could be mitigated with SDN.
https://www.telanova.com/tnova-qkd

[TEM-1993] Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States (1993). ePrint.
https://irp.fas.org/eprint/tempest.htm

[WAK-2002] Waks, Edo; Zeevi, Assaf; Yamamoto, Yoshihisa (2002): Security of quantum key distribution with entangled photons against individual attacks. In Phys. Rev. A 65 (5). DOI: 10.1103/PhysRevA.65.052310.
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.65.052310

[WAN-2020] Wang, Weilong; Tamaki, Kiyoshi; Curty, Marcos (2020): Measurement-Device-Independent Quantum Key Distribution with Leaky Sources. DOI: 10.48550/arXiv.2001.08086.
https://arxiv.org/abs/2001.08086

[WAN-2021] Wang, Liu-Jun; Zhang, Kai-Yi; Wang, Jia-Yong; Cheng, Jie; Yang, Yong-Hua; Tang, Shi-Biao et al. (2021): Experimental authentication of quantum key distribution with post-quantum cryptography. In npj Quantum Inf 7 (1). DOI: 10.1038/s41534-021-00400-7.
https://www.nature.com/articles/s41534-021-00400-7

[WAN-2022] Wang, Shuang; Yin, Zhen-Qiang; He, De-Yong; Chen, Wei; Wang, Rui-Qiang; Ye, Peng et al. (2022): Twin-field quantum key distribution over 830-km fibre. In Nat. Photon. 16 (2), pp. 154–161. DOI: 10.1038/s41566-021-00928-2.
https://www.nature.com/articles/s41566-021-00928-2

[WAN-2023] Wang, Ze-Hao; Yin, Zhen-Qiang; Wang, Shuang; Wang, Rong; Lu, Feng-Yu; Chen, Wei et al. (2023): Tight finite-key analysis for mode-pairing quantum key distribution.
https://arxiv.org/abs/2302.13481

[WEI-2011] Weier, Henning; Krauss, Harald; Rau, Markus; Fürst, Martin; Nauerth, Sebastian; Weinfurter, Harald (2011): Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. In New J. Phys. 13 (7), p. 73024. DOI: 10.1088/1367-2630/13/7/073024.
https://iopscience.iop.org/article/10.1088/1367-2630/13/7/073024

[WIL-2019] Williams, Brian P.; Lukens, Joseph M.; Peters, Nicholas A.; Qi, Bing; Grice, Warren P. (2019): Quantum secret sharing with polarization-entangled photon pairs. In Phys. Rev. A 99 (6). DOI: 10.1103/PhysRevA.99.062311.
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.99.062311

[WIN-2010] Winkler, Justin (2010): Entanglement and Quantum Key Distribution.
http://www2.optics.rochester.edu/workgroups/lukishova/QuantumOpticsLab/2010/OPT253_reports/Justin_Essay.pdf

[XU-2015] Xu, Feihu; Curty, Marcos; Qi, Bing; Lo Hoi-Kwong (2015): Measurement-Device-Independent Quantum Cryptography. In IEEE J. Select. Topics Quantum Electron. 21 (3), pp. 148–158. DOI: 10.1109/JSTQE.2014.2381460. https://ieeexplore.ieee.org/document/6985598

[YAN-2021] Yang, Yong-Hua; Li, Pei-Yuan; Ma, Shi-Zhao; Qian, Xiao-Cong; Zhang, Kai-Yi; Wang, Liu-Jun et al. (2021): All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. In Optics express 29 (16), pp. 25859–25867. DOI: 10.1364/OE.432944. https://opg.optica.org/oe/fulltext.cfm?uri=oe-29-16-25859&id=453809

[YAV-2022] Yavuz, Attila A.; Earl, Duncan; Packard, Scott; Nouma, Saif Eddine: Hybrid Low-Cost Quantum-Safe Key Distribution. In : Quantum 2.0 Conference and Exhibition. Quantum 2.0. Boston, MA. Washington, D.C.: Optica Publishing Group, QTu4C.5. https://opg.optica.org/abstract.cfm?URI=QUANTUM-2022-QTu4C.5

[YE-2019] Ye, Wei; Zhong, Hai; Wu, Xiaodong; Hu, Liyun; Guo, Ying (2019): Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis. https://arxiv.org/abs/1907.03383

[YIN-2019] Yin, Hua-Lei; Fu, Yao (2019): Measurement-Device-Independent Twin-Field Quantum Key Distribution. In Scientific reports 9 (1), p. 3045. DOI: 10.1038/s41598-019-39454-1. https://www.nature.com/articles/s41598-019-39454-1

[ZAW-2019] Zawadzki, Piotr (2019): Quantum identity authentication without entanglement. In Quantum Inf Process 18 (1). DOI: 10.1007/s11128-018-2124-2. https://link.springer.com/article/10.1007/s11128-018-2124-2

[ZEB-2018] Zebboudj, Sofia; Omar, Mawloud (2018): Deterministic MDI QKD with two secret bits per shared entangled pair. In Quantum Inf Process 17 (3). DOI: 10.1007/s11128-018-1813-1. https://link.springer.com/article/10.1007/s11128-018-1813-1

[ZHA-2010] Zhao, Yi; Qi, Bing; Lo, Hoi-Kwong; Qian, Li (2010): Security analysis of an untrusted source for quantum key distribution: passive approach. In New J. Phys. 12 (2), p. 23024. DOI: 10.1088/1367-2630/12/2/023024. https://iopscience.iop.org/article/10.1088/1367-2630/12/2/023024

Glossary

COO	Chief Operating Officer
CV	Continuous-Variable
dB	decibel
DDoS	Distributed Denial-of-Service
DI	Device-Independent
DV	Discrete-Variable
EB	Entanglement-Based
ECC	Elliptic-Curve Cryptography
ETSI	European Telecommunications Standards Institute
EuroQCI	European Quantum Communication Infrastructure
FG-QIT4N	Focus Group on Quantum Information Technology for Networks
FTTB	Fibre-to-the-Building
FTTD	Fibre-to-the-Desk
HPC	High Performance Computing
ICT	Information and Communications Technology
ID	Identification
ISG	Industry Specification Group
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KM	Key Manager
KMS	Key Management System
MDI	Measurement Device Independent
ML	Machine Learning
NLPQT	National Laboratory for Photonics and Quantum Technologies
NREN	National Research and Education Network
NSA	National Security Authorities
OGS	Optical Ground Stations
OTP	One-Time-Pad
PM	Prepare-and-Measurement
PNS	Photon-Number Splitting
PoP	Point of Presence
PQC	Post Quantum Cryptography
QBER	Quantum Bit Error Rate
QCI	Quantum Communication Infrastructure
QEA	Quantum Entity Authentication
QIA	Quantum Identity Authentication
QITs	Quantum Information Technologies
QKD	Quantum Key Distribution
QKDN	QKD Network
QMA	Quantum Message Authentication
QoS	Quality of Service
QSS	Quantum Secret Sharing
R&D	Research and Development

RSA	Rivest–Shamir–Adleman cryptosystem
NatQCI	National Quantum Communication Infrastructure
NISR	National Industrial Security Regulation
SAB	Security Advisory Board
SD	Secure Digital
SDN	Software-Defined Networking
SKR	Secure Key Rate
SPD	Single Photon Detectors
SSN	Secure Storage Network
TF	Twin-Field Quantum Key Distribution
USB	Universal Serial Bus
WP	Work Package