Key Management System for a QKD Network

Guilherme Duarte, Guilherme Andrade, João Rodrigues,
Inês Santos, André Miragaia, Patrícia Cardoso

Oriented by Prof. Armando Pinto, Diogo Matos
Supervised by Prof. José Moreira
anp@ua.pt, dftm@ua.pt, jose.moreira@ua.pt

Universidade de Aveiro

Key Management System for a QKD Network

DETI

Universidade de Aveiro

Guilherme Duarte, Guilherme Andrade, João Rodrigues, Inês Santos, André Miragaia, Patrícia Cardoso

30/11/2023

Abstract

In today's data-driven world, keeping information safe during transmission is crucial. That's where a Key Management System (KMS) for a Quantum Key Distribution (QKD) network comes in. This report is all about the design of a specialized KMS for these types of networks. The big challenge? Creating a way to make, store, synchronize, and share cryptographic keys. It's about retrieving keys securely, keeping them safe, managing their lifecycle, and making sure they are passed along efficiently. Plus, it is crucial to get these keys to the applications that requested them whilst keeping everything super secure. To understand what different users need, we have made detailed profiles for various fields, like genomics and the military.

Additionally, we recognized the vital significance of interaction between KMS units that aren't directly linked by a physical connection. This aspect adds another layer of complexity and importance to the overall functionality and security of the KMS in Quantum Key Distribution Networks.

Keywords: Quantum Key Distribution, Key Management System, cryptographic keys, secure transmission, Inter-KMS communication, Quantum Key Distribution Network (QKDN)

Report contents

Acronyms

UA Universidade de Aveiro

IT Instituto de Telecomunicações

LECI Licenciatura em Engenharia de Computadores e Informática

QKD Quantum Key Distribution

KMS Key Management System

QKDN Quantum Key Distribution Network

SMC Secure Multiparty Computation

ETSI European Telecommunications Standards Institute

KML Key Management Layer

OTP One Time Pad

SDN Software-Defined Networking

ITS Information-Theoretic Security

QoS Quality of Service

Chapter 1

Introduction

In an era defined by the relentless advancement of technology, the security and privacy of sensitive information exchanged over communication channels has become an ever-growing concern. In response to this challenge, cryptography has emerged as a crucial solution. Cryptography involves transforming readable data (plaintext) into unreadable data (ciphertext) using keys generated by mathematical techniques and algorithms.

Cryptographic keys are a vital part of any security system and the compromise of any cryptographic key can lead to the collapse of an organization's entire security infrastructure, allowing the attackers to decrypt sensitive data, authenticate themselves as privileged users and give themselves access to other sources of classified information. Cryptography can be symmetric if it uses a single cryptographic key to encrypt and decrypt the information or it can be asymmetric if it uses two cryptographic keys, a public to encrypt and a private to decrypt.

Symmetric cryptography requires less computational overhead when compared to asymmetric cryptography. But if there is an eavesdropper in the communication channel, the key will be compromised and all communications encrypted with that key become vulnerable. Asymmetric cryptography is not affected by this, since only the public key is exchanged but, as previously mentioned, it is computationally more intensive and requires much more computational resources.

The algorithms used in classical cryptography based in mathematical techniques are currently secure against classical computers but may be in risk due to the imminent evolution of quantum computing. Quantum cryptography emerges as a solution to mitigate this risk, since it uses quantum mechanics to perform cryptographic tasks. Quantum Key Distribution (QKD) is an example of quantum cryptography which enables the negotiation of cryptographic keys in a theoretically secure manner, in other words, without relying on computational complexity to be secure.

A Quantum Key Distribution Network (QKDN) is a set of Quantum Key Distribution nodes. These nodes contain one or more modules that generate keys and implement QKD

protocols, and can be linked through quantum communication channels to each other at the physical layer. As opposed to classic cryptography, an eavesdropping attempt through these channels is noticed by both end-points, since it disturbs the system.

On top of that, a Key Management Layer (Key Management Layer (KML)) needs to exist in order to mediate the key provisioning to cryptographic applications. It basically receives keys and key material generated by the physical layer and supplies them upon request to cryptographic applications, that need keys to ensure security and privacy of its communications.

1.1 Context

This project is being done in University of Aveiro (Universidade de Aveiro (UA)) in the scope of the graduating project for our course in Computer and Informatics Engineering (Licenciatura em Engenharia de Computadores e Informática (LECI)), and focuses on the development of a Key Management Layer for a Quantum Key Distribution Network that is being developed by the Optical Quantum Communications group in Instituto de Telecomunicações (Instituto de Telecomunicações (IT)). The system will follow International and European standards specified by institutions/groups such as European Telecommunications Standards Institute (ETSI) and ITU-T.

1.2 Motivation

As mentioned earlier in this chapter, classical cryptography may be in risk due to the advancements of quantum computers, which have substantially larger processing abilities. Quantum Key Distribution networks offer a solution to secure communication using symmetric keys and to Secure Multiparty Computation (SMC) using oblivious keys. Secure Multiparty Computation is a cryptographic technique that allows multiple parties (entities) to jointly compute a function without knowing each others information. Oblivious keys are asymmetric keys used in Oblivious Transfer which is very resource demanding and not very efficient with traditional computation. For the QKD networks to work, a Key Management Layer needs to exist to supply those keys upon request from the cryptographic applications.

1.3 Goal

The main goal of this project is to implement a Key Manager System that is capable of receiving and sending keys from the physical layer to cryptographic applications, storing, maintaining, synchronizing, deriving and relaying keys.

Chapter 2

Related Work and State-of-The-Art

2.1 Background, Related Work and State-of-The-Art on Quantum Key Distribution and Key Management Systems for QKD Networks

To deepen our understanding of what has been previously attempted and explored in the area of Quantum Key Distribution and Key Management Systems, we searched for related scientific papers and made a selection of eight of them that we figured provided relevant context for the system we are currently developing. In this section, an overview of the articles is provided in the following table, along with their presentation and key topics explored in them in the subsequent subsections.

2.1.1 Papers and Articles

Tables 2.1, and 2.2 chronologically pinpoint the main achievements in every article, along with who conducted that investigation or project. In the next subsections, a more careful explanation of each of this papers is provided.

Year	Researchers/Organizations	Achievements/Findings	Distance (km)	Key Rate	Additional Details
1991	John Rarity, Paul Tapster, Artur Ekert	Demonstrated secure form of quantum key distribution based on mathematical theorems and (quantum) physical laws			UK Defense Research Agency in Malvern and Oxford University
2008	University of Cambridge and Toshiba	Exchange of secure keys at 1 Mbit/s (20 km of optical fiber) and 10 kbit/s (over 100 km of fiber)	20/100	1 Mbit/s 10 kbit/s	BB84 protocol with decoy states
2008	System Platforms Research Laboratories and Nano Electronics Research Laboratories, NEC Corporation. Quantum Computation and Information Project, JST ERATO-SORST	Novel key-management technique that uses on-demand crypto-key supply using 'Repeat' and 'Remote' nodes	Key Relay: functional QKD network irrespectively of physical link configurations		Developed and tested for a five-node QKD network
2014	University of Geneva and Corning Inc. (New York)	Longest distance for optical fiber QKD (307 km)	307	12.7 kbit-s/s	Highest bit rate over distances of 100 km

Table 2.1: Synthetic comparison and explanation of the main studies referred in this chapter (Part 1).

Year	Researchers/Organizations	Achievements/Findings	Distance (km)	Key Rate	Additional Details
2019	Shanghai Jiaotong University	Demonstrated polarization qubit states	Extended the distribution distance of CV-QKD to 50 km over commercial fiber	Comparable to discrete-variable QKD systems key rate in metropolitan areas	Quantum communication pilot over existing telecommunication fiber
2019	Ririka Takahashi, Yoshimichi Tanizawa, Alexander Dixon, Corporate Research and Development Center, Toshiba Corporation	High-speed quantum encryption method			The local key manager, the OTP tunnel manager, the global key manager and key providing web API reached 414 Mb/s, 185 Mb/s, 85 Mb/s and 971 Mb/s respectively
2021	Joo Yeon Cho, Jose-Juan Pedreno-Manresa, Sai Patri, Andrew Sergeev, Jörg-Peter Elbers, Helmut Griesser, Catherine White, Andrew Lord ADVA Optical Networking, Fraunhoferstrasse 9a, Martinsried, Germany. BT Labs, Adastral Park, Ipswich, U.K	Interoperability of multi-vendor QKD systems through a standard interface			Key relay routes dynamically managed by Software-Defined Networking (Software-Defined Networking (SDN))
2023	Paul James, Stephan Laschet, Sebastian Ramacher, and Luca Torresetti. 2023. In The 18th International Conference ARES 2023	KMSs for Large-scale Quantum Key Distribution Networks			Integration of Post Quantum Cryptography techniques

Table 2.2: Synthetic comparison and explanation of the main studies referred in this chapter (Part 2).

2.1.2 Quantum Cryptography Based on Bell's Theorem (1991) [1]

The paper explores the practical application of the generalized Bell's theorem in quantum key distribution (QKD) for cryptography.

Quantum Cryptography's Basis: The paper emphasizes the inseparability of cryptographic mathematical structures from the physical laws governing computation. It showcases how quantum mechanics significantly extends computational possibilities beyond classical Turing machines, as exemplified by quantum cryptography initiated by Bennett and Brassard.

Quantum Key Distribution Scheme: Ekert presents a method where the security of key distribution in cryptography relies on the completeness of quantum mechanics. The proposed scheme involves the Bohm version of the EPR experiment and the Clauser-Horne-Shimony-Holt inequalities (generalized Bell's theorem) to test for eavesdropping.

Shift from Classical to Quantum Channels: Traditional cryptography depended on the secrecy of the entire encryption and decryption process. In contrast, quantum channels, as described by Ekert, distribute keys without any "element of reality" associated with them, thus protected by the completeness of quantum mechanics.

Implementation and Testing: The paper describes a quantum channel consisting of source emitting pairs of spin-1/2 particles in a single state towards two users, Alice and Bob. After transmission, Alice and Bob can publicly announce their analyzer orientations for each measurement, allowing them to establish a secret key string from their results.

Eavesdropping Detection and Security: The system is secured against eavesdropping because any intervention by an eavesdropper is detectable. It is shown that the generalized Bell's theorem can attest the safety of key distribution, with the security of the system protected by fundamental physical laws as long as quantum theory remains valid.

2.1.3 Gigahertz Decoy Quantum Key Distribution with 1 Mbit/s Secure Key Rate (2008) [2]

The paper reports on the first gigahertz clocked decoy-protocol Quantum Key Distribution (QKD), achieving record key rates due to the use of self-differencing InGaAs avalanche photodiodes designed for high-speed single-photon detection. It marks a significant advance in QKD by achieving a secure key rate of 1.02 Mbit/s for a fiber distance of 20 km and 10.1 kbit/s for 100 km, using compact non-cryogenic detectors.

Decoy QKD Protocol: The system uses a decoy QKD protocol where a subset of signal pulses is replaced with weaker decoy pulses to prevent photon number splitting (PNS) attacks, enhancing the security of the key distribution.

Experimental Setup: The QKD system uses a 1.55 µm pulsed laser operating at 1.036 GHz, with phase encoding/decoding optics based on an asymmetric fiber Mach-Zehnder interferometer. The setup also includes a fiber-optic intensity modulator to create the required intensity levels for signal, decoy, and near-vacuum pulses.

Results and Discussion: The protocol was implemented with three different intensity levels for the signal and decoy pulses. The experiment achieved a remarkable secure key rate of 1.02 Mbit/s over 20 km of fiber, significantly higher than previous records for unconditionally secure QKD protocols.

Conclusion: The paper concludes that the demonstrated high key rate QKD using gigahertz-clocked InGaAs APDs and the decoy protocol makes QKD practical for high-bandwidth, information-theoretically secure communication. This advancement is significant both for the field of cryptography and quantum information science.

Implications and Future Applications: The paper presents a practical and low-cost approach to QKD systems, potentially enabling secure broadband communication in the future. The results indicate a significant step towards practical implementation of QKD in real-world applications, such as secure video links and other forms of high-speed secure communication.

2.1.4 Scalable QKD Network Using Simple Key-Management Technique with On-Demand Crypto-Key Supply (2008) [3]

The paper introduces a novel key-management technique for Quantum Key Distribution (QKD) networks, focusing on simplicity and efficiency. It highlights the critical importance of secure key distribution in network security, acknowledging the potential of QKD as a highly secure method. The study reports on the development and testing of a five-node QKD network utilizing this new technique.

Key-Management Technique: The paper proposes a key-management technique that uses on-demand crypto-key supply, addressing the dynamic nature of quantum key quantities in multi-node QKD networks. This technique classifies QKD nodes into 'repeat nodes' and 'remote nodes'. Repeat nodes centrally manage and control quantum key generation, responding to the quantum key amounts, while Remote nodes request and supply these keys for network communication.

Network Architecture: The research delineates an architectural vision for integrating a QKD network with an optical network. It emphasizes the importance of quantum key relay, vital for achieving a functional QKD network irrespective of physical link configurations.

Practical Implementation and Testing: The technique was implemented in a five-node QKD network, comprising both point-to-point and optical switched QKD setups. Key generation and storage were continuously managed, with a quantum key relay operation conducted every five minutes among the nodes.

2.1.5 Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre (2014) [4]

This paper presents a compact and autonomous Quantum Key Distribution (QKD) system capable of distributing provably secure cryptographic keys over 307 km of ultra-low-loss optical fiber. It demonstrates the practicality of long-distance QKD using standard telecom components and addresses the challenge of high background noise from commonly used semiconductor single-photon detectors.

Key Contributions: Extended Operating Distance: The system significantly extends the operating distance of practical fiber-based QKD systems, previously limited to about 150 km, to 307 km. This is achieved through the use of indium gallium arsenide (InGaAs) single-photon detectors (SPDs) with record low background noise.

Coherent One-Way (COW) QKD Protocol: The QKD system is based on the COW protocol, where the bit string is encoded in the time of arrival of weak coherent laser pulses, and channel disturbances are monitored by measuring the visibility of the interference between neighboring pulses.

Security Framework: The security of the QKD system adheres to a universally composable security framework. This framework assures that the output secret key is distinguishable from an ideal secret key with a high probability and ensures a high probability that Alice and Bob have identical secret keys.

Conclusion: The work showcases that a practical, robust, and autonomous QKD over very long distances is feasible even with standard telecom components in a rack-mounted architecture, setting a new benchmark for QKD system performance.

2.1.6 Continuous-variable QKD over 50km commercial fiber (2019) [5]

The paper focuses on continuous-variable Quantum Key Distribution (CV-QKD), highlighting its advantages over discrete-variable systems, particularly higher secret key rates in metropolitan areas and the use of standard telecom components that operate at room temperature.

Key Contributions: CV-QKD Protocol

- The CV-QKD protocol is based on coherent states with Gaussian modulation, proven secure against arbitrary attacks. The paper aims to demonstrate practical CV-QKD systems that maintain automatic operation and stabilization in real-world environments while achieving moderately secure key rates.

Field Test Achievements: The field tests achieved secure key rates significantly higher than previous demonstrations, realized through the development of an efficient calibration model and a fully automatic control system. This system effectively stabilized system noise and applied a rate-adaptive reconciliation method to maintain high efficiency in fluctuating environments.

Experimental Setup: The experimental setup includes two legitimate users (Alice and Bob), where Alice generates Gaussian-modulated coherent states sent to Bob. The setup features a strong local oscillator, dynamic polarization control, and a balanced pulsed homodyne detector for signal processing.

Field Test Environments: The field tests were conducted in two different cities with varying channel losses and physical network types. The research team developed automatic feedback systems to calibrate time, polarization, and phase of the quantum states transmitted, addressing the challenge posed by changing environmental conditions.

Reconciliation Efficiency and Secret Key Rate: The paper discusses the importance of high reconciliation efficiency and low Frame Error Rate (FER) for achieving high secret key rates. A rate-adaptive reconciliation protocol was used to maximize the secret key rate by balancing efficiency and FER.

24-Hour Continuous Test Results: Over 24 hours in Xi'an and 3 hours in Guangzhou, the CV-QKD system demonstrated stable operation with an average excess noise of 4% and secret key rates of 7.57 kbps (asymptotic limit) and 5.91 kbps (finite-size regime) in Xi'an, and 7.43 kbps (asymptotic limit) and 5.77 kbps (finite-size regime) in Guangzhou.

Conclusion: The field tests extended the distribution distance of CV-QKD to 50 km over commercial fiber, achieving secret key rates comparable to discrete-variable QKD systems in metropolitan areas. This progress moves CV-QKD towards more practical applications, indicating the potential for building secure metropolitan networks with current technology.

2.1.7 A High-Speed Key Management Method for Quantum Key Distribution Network (2019) [6]

The paper introduces a high-speed key management method for Quantum Key Distribution (QKD) networks, addressing the critical need for increased processing speed in key management essential for modern QKD systems. It emphasizes the importance of secure communication in the context of rapidly growing communication data volumes and the necessity of safeguarding against interception and eavesdropping.

High-Speed Key Management Method

The proposed method consists of four main modules:

- Local key manager: Handles keys generated by QKD.
- One-time pad (One Time Pad (OTP)) tunnel manager: Establishes transparent encryption links.
- Global key manager: Generates keys for application communication.
- Web API: Provides keys to applications.

These modules collectively enable efficient handling of encryption keys at high speeds (414 Mb/s for the local key manager, 185 Mb/s for the OTP tunnel manager, 85 Mb/s for the global key manager, and 971 Mb/s for the web API).

Addressing Key Sharing Limitations: The paper discusses the limitations of traditional QKD, including the limited spread of key sharing and the challenge of achieving high-speed key sharing. It references several notable QKD field trials and projects, like the DARPA Quantum Network and the SECOQC project, which have contributed to overcoming these challenges.

QKD Network Architecture: The QKD network architecture described in the paper includes QKD nodes, key management nodes, and applications. It outlines how these components interact within the network, ensuring security at various levels, including operational and physical levels.

2.1.8 Demonstration of Software-defined Key Management for Quantum Key Distribution Network (2021) [7]

The paper presents a practical key management scheme for Quantum Key Distribution (QKD) networks. It emphasizes the interoperability of multi-vendor QKD systems through a standard interface, with key relay routes dynamically managed by Software-Defined Networking (SDN).

QKD Network Concept: It explains the concept of QKD as a method for establishing secret keys between remote peers based on quantum physics. The network consists of point-to-point QKD links, allowing secure key relay and sharing even when devices are not directly connected.

Vendor-Agnostic Key Management System: The paper demonstrates a key management system that is vendor-agnostic, capable of integrating various QKD systems into a single network. The system retrieves QKD keys in a standardized form and relays encryption keys to end-users in a quantum-secure manner.

Interoperability and Trusted Nodes: The system uses a key management agent on a trusted node, decoupled functionally from the QKD network. This agent accesses QKD keys via the ETSI standard key delivery interface, collects keys from intermediate QKDs, encrypts them, and delivers the ciphertext to the destination node.

SDN Controller Role: A centralized SDN controller in the meshed QKD network dynamically provisions and reroutes key relay routes, enhancing the robustness and efficiency of the QKD service.

2.1.9 Key Management Systems for Large-Scale Quantum Key Distribution Networks (2023) [8]

The paper focuses on the development of Key Management Systems (KMSs) for large-scale Quantum Key Distribution Networks (QKDNs), discussing the challenges and solutions in scaling from link-to-link key generation to extensive key distribution networks. It addresses the integration of Post Quantum Cryptography (PQC) hybridization techniques at the KMS level to enhance security against quantum computer-driven attacks.The paper also evaluates existing standards and proposes new Application Programming Interfaces (APIs) for unstandardized interfaces within QKDNs.

KMS Architecture in QKDNs: The KMS plays a vital role in scaling up quantum key distribution. It connects to QKD modules, receiving keys from directly connected nodes and distributing them across the network.

Core KMS Functions: These include key forwarding, key management, database synchronization, bootstrapping, and communication interfaces. KMS is essential for establishing end-to-end keys using intermediate trusted nodes and managing key states.

Key Forwarding Methodology: The process involves generating a random value at the source KMS, encrypting it with the QKD-generated key of the next node, and forwarding it through the network.

Security Algorithms: The paper emphasizes the use of information-theoretic security (Information-Theoretic Security (ITS)) primitives in QKD networks, such as One Time Pad (OTP) encryption and message authentication codes based on universal hashing functions.

Hybridization with Post Quantum Cryptography: It addresses the integration of PQC to enhance security, especially for end-to-end authentication, and reduce reliance on trusted nodes.

Security Infrastructure Considerations: This includes controls for access, audits, tamper response, and security by design. The paper outlines the need for effective management and technical measures to secure QKDNs.

Network Technology and Standards: Discusses RESTful network APIs, like CoAP and HTTP(S), and reviews QKD standards like ETSI GS QKD 004, 014, 015, and ITU-T Y.3803, highlighting their role in the operability and design of QKDN components.

Proposed Interfaces: The paper proposes new APIs for KMS to KMS and KMS to SDN Agent interfaces, addressing gaps in standardization and enhancing the functionality and security of the network.

KMS Prototype Development: A prototype KMS is developed within the EuroQCI framework, showcasing the practical application of the proposed principles and techniques, including a PQC hybrid approach and ITS algorithms.

2.2 State-of-The-Art takeaways and relevant points

Considering the Background and Related Work presented, our system takes inspiration from some of the tools and concepts previously showcased, and we were able to identify related technologies that will also be useful (and used) in our system.

For example, taking advantage of Physical and Quantum-Mechanics' laws is beneficial for a more secure key distribution in cryptography.

We also concluded that Key Relay is of vital importance for achieving a functional QKD network, regardless of the physical distance between the nodes of a system, since there is an increased importance of secure communication in the context of rapidly growing communication data volumes and a necessity for safeguarding against interception and eavesdropping.

In our system, to guarantee security in communications between KMSs, OTP encryption (a simple XOR of the encryption data, as long as a different key is always used and its size is the same as the data to encrypt) between nodes will be used.

It will become necessary to generate keys according to the needs of eventual applications, and providing those keys to those apps.

Similar approaches to QKD Networks, with a QKD network architecture described in a previous paper, our approach will also include QKD nodes, Key Management nodes, and applications, along with their interactions. Furthermore, SDN Agents will also be needed to coordenate information about the network, and provide Quality of Service (QoS) parameters to the KMS from the apps.

As presented in the last article ([8]), our solution will, similarly, hold some key functionalities such as:

- Connection to QKD modules
- Receiving keys from directly connected QKD nodes and distributing them as requested
- Key Forwarding
- Establishing end-to-end keys using intermediate trusted nodes (Key Relay)
- Communication interfaces (the use of QKD standards like ETSI GS QKD 004)
- The use of information-theoretic security algorithms (ITS), such as One Time Pad (OTP) encryption

Seeing these recent successful approaches to KMS design and development, we conclude that a solution like ours is achievable. With that in mind, in Chapter 4 (KML Architecture), we provide and explain the system architecture and modules with which our KML will be interacting with.

Chapter 3

Requirements Elicitation

Information security stands as a foundational element in digital systems, and the evolving cyber-threats demand constant innovations in data protection practices. Within this landscape, Quantum Key Distribution (QKD) has emerged as a revolutionary technology, enabling the secure generation of cryptographic keys to be immune to traditional computational threats.

This project aims to develop a Key Management System (KMS) for a QKD Network, aligned with standards set by Discretion and ETSI, to provide a secure environment for key generation and distribution. Besides just getting quantum keys from QKD devices, the system needs to become more flexible and better at adapting to what other systems/applications need.

Requirements elicitation plays a crucial role in understanding the needs of users and applications that will interact with the system. This extends beyond obtaining cryptographic keys. It also involves consideration for specific key characteristics, predefined Quality of Service (QoS) requirements, and integration capacity with existing networks.

The elicitation of requirements for the next iteration of the Key Management Layer(KML) aims not only to provide quantum keys but also to expand its functionality to supply classical, post-quantum, and quantum keys, offering a more comprehensive and flexible approach to clients.

This chapter will explore the methods and strategies used to identify, document, and analyze the fundamental requirements for the evolution of this Key Management System. It will consider end-users demands, established standards, as well as emerging needs at the forefront of cybersecurity.

3.1 Personas and Scenarios

We took the necessary steps to establish Personas and Scenarios. We developed two personas that are involved in a work setting that could use our KMS. This approach allows us to create a system that accommodates users of diverse industries and needs, ensuring usability for everyone that needs it. Each persona symbolizes a different industry and has motivations for using the KML, all aligned with the objective of ensuring the security of encryption keys, which are essential for protecting sensitive data. This prevents unauthorized access to information, even if the underlying cryptographic algorithm is compromised. To illustrate the potential applications of our interaction system, we elaborate specific scenarios. These scenarios show the different ways in which individuals need our system. Our goal is to build a system that can serve a wide range of industries, covering diverse collective groups. By developing two personas that represent a community, we can effectively meet the diverse needs of our potential user groups.

3.1.1 Personas

Carlos, 42

- **Description:** Carlos, a military communications officer, plays a vital role in securing sensitive communications between military bases. His focus is on ensuring the security and longevity of these communications.
- **Motivation:** Regular messages lose importance over time, but military information stays valuable. Public key encryption has risks, while symmetric keys work better. Carlos focuses on safeguarding important data by using symmetric keys and good key management. This choice is crucial for long-term security in military settings.

Ana, 27

- **Description:** Ana, a computational genetics researcher at a medical clinic, contributes to the analysis of phylogenetic trees. The clinic collaborates with another. Therefore, there is a need for strong security for genetic data protection.
- **Motivation:** Security is crucial in computational genetics to safeguard valuable data. Collaborative efforts highlight the need for secure data transfer with a strong emphasis on ensuring data privacy. Genetic information exchange must prioritize confidentiality to prevent compromising sensitive data. To achieve this, the clinic is implementing robust security measures, including the utilization of oblivious or symmetric keys in the communications between the two applications.

3.1.2 Scenarios

3.1.2.1 Carlos

Robust communication security: In recent times, the military has witnessed an evolution in the nature of information warfare, with an increasing need for robust communication security. Carlos understands the ephemeral nature of public key encryption, especially in high-stakes military operations where the significance of information persists long after it's transmitted. In response to these challenges, Carlos has chosen to prioritize symmetric key cryptography, recognizing its effectiveness and efficiency in the context of military communication. Carlos, a seasoned military communications officer, finds himself at the forefront of a critical initiative known as Operation Sentinel Secure Communication Upgrade. This operation aims to enhance the security and longevity of sensitive communications between multiple military bases. Carlos's dedication to securing military communications goes beyond routine tasks; it involves a strategic and forward-thinking approach. Operation Sentinel Secure Communication Upgrade reflects Carlos's commitment to long-term security, leveraging symmetric key cryptography, advanced key management practices, and proactive measures to safeguard military information in an ever-changing digital landscape.

3.1.2.2 Ana

Robust communication in Computacional Genetics: In the real world of computational genetics, the significance of security cannot be overstated. Ana's work involves the analysis of intricate phylogenetic trees, requiring collaboration with another medical institution. This collaboration necessitates a robust approach to secure data transfer, with a particular focus on ensuring the privacy of genetic information. The exchange of genetic data demands a high level of confidentiality to prevent any compromise of sensitive information. To address this need, the clinic is actively implementing strict security measures, including the use of oblivious and symmetric keys in the communication channels between the two or more applications. Ana, a computational genetics researcher at a medical clinic, is deeply involved in the analysis of phylogenetic trees — a critical component in understanding genetic relationships. The medical clinic collaborates with another institution, emphasizing the importance of strong security measures to protect valuable genetic data. This scenario showcases Ana's commitment to the security and privacy of genetic information in the collaborative research setting. The implementation of robust security measures, including symmetric and oblivious keys, reflects a comprehensive approach to safeguarding valuable genetic data throughout the collaborative research process. Two apps, one from each clinic, come into contact to create phylogenetic trees with their patients' data, but the data from Clinic A cannot be decrypted by Clinic B and vice versa. In other words, a way needs to be found for them to perform the calculations without having direct access to each other's data, and that's where Secure Multi-Party Computation (SMC) comes in.

3.2 Requirements

To address the scenarios outlined earlier and align with the project's initial conditions, a set of functional and non-functional requirements has been collated. These requirements are shown in tables (3.1, 3.2), offering a detailed overview of their descriptions and intended purposes. Furthermore, thorough explanations for each requirement are provided in the accompanying textual content below the tables.

3.2.1 Functional requirements

Requirement	Description
FR-1	The KMS should request and retrieve keys from physical layer.
FR-2	The KMS should be capable of storing the keys.
FR-3	The system must ensure key synchronization.
FR-4	The system should implement NIST-standard key life cycle.
FR-5	The system must ensure secure key relay.
FR-6	The KMS must give keys to the apps.

Table 3.1: Functional requirements defined for our system.

- FR-1: The KMS is connected to a physical layer that provides keys to it. These keys can be symmetrical or oblivious and can be generated in distinct manners - classical, post-quantum or quantum (our main goal).
- FR-2: All keys reside within a Database, accessible to the key manager for key creation and retrieval. Key material obtained from the physical layer isn't internally classified as a pre-existing key. Instead, it's designated for future key generation upon application request.
- FR-3: The keys stored by peer KMSs must align, not necessarily be identical, to properly supply them to the applications. Synchronization occurs when both peers have received and acknowledged the key.
- FR-4: All keys created within the KMS have a life cycle defined by the NIST standard, where keys have an associated state determined by an expiration timestamp and creation timestamp linked to the key and stored in the database.
- FR-5: As QKD devices generate key material only between directly connected devices, but matching keys are needed across two arbitrary nodes, there's a necessity for a method to transfer keys from one KMS to another (from one node to another node) that are not directly connected.

- FR-6: The application requests keys from the KMS, which then sends them in response to the request. This process facilitates the distribution of keys.

3.2.2 Non-functional requirements

Category	**Requirement**	**Description**
Security	NFR-1	The communication between KMSs should be encrypted.
Performance	NFR-2	KMS delivers requested keys efficiently.
Maintainability	NFR-3	Modular system for easy maintenance.
Reliability	NFR-4	Validate ETSI parameters and manage errors.

Table 3.2: Non-functional requirements defined for our system.

- NFR-1: The communication between KMS should be encrypted (XOR or One Time Pad), always using a different key, with the same size of the data to encrypt.
- NFR-2: The KMS should be able to send the requested keys to the apps with the requested key rate (effective_key_rate parameter in the QoS Provider module).
- NFR-3: The system is organized in various modules, which facilitates maintainability.
- NFR-4: The system should verify the correction of parameters (according to the ETSI protocol), and handle errors (i.e: in OPEN_CONNECT requests from an app).

Chapter 4

KML Architecture

4.1 Introduction

Quantum Key Distribution (QKD) enables the negotiation of cryptographic keys in a secure manner without relying on computational complexity to achieve its security. On top of the QKD systems, a Key Management Layer (KML) needs to exist in order to mediate the key provisioning to the applications. The key manager provides keys with characteristics requested by the apps and bonds to a pre-negotiated quality of service. The proposed system follows Discretion's and ETSI standards. The system differentiates itself in the fact that mostly (or only) receives quantum oblivious keys from the QKD devices. A future version of the KMS should be able to offer classical, post-quantum and quantum keys, facilitating its integration into existing networks and providing more flexibility to its clients. In this Chapter we present the Architecture we need to implement for the KML.

4.2 System Overview

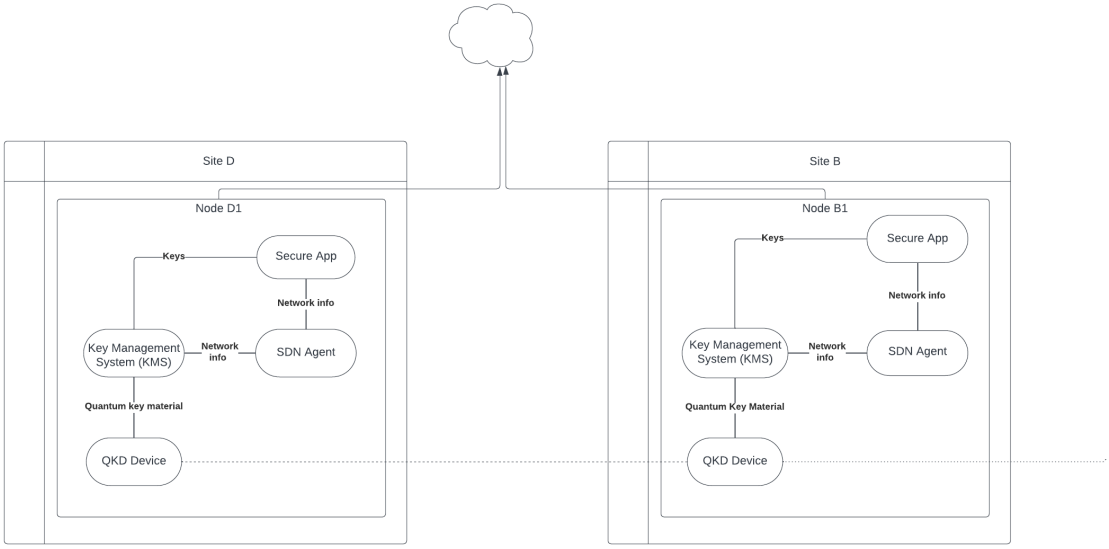

Figure 4.1: System Architecture.

In the diagram above (Figure 4.1), a simple overview of the whole system in a two node scenario where the Key Management System (KMS) is integrated can be seen. The dashed line represents a quantum link and the cloud is the black network where, for example, the Software Defined Network (SDN) Controller is located. Each secure site hs one or more SD-QKD nodes each identified by its qkdn_id. The KMS is connected to a physical layer that provides keys to it. These keys can be symmetrical or oblivious and can be generated in distinct manners - classical, post-quantum or quantum (our main focus). Multiple applications are connected to it in order to retrieve keys. Both interfaces (to the applications and to the QKD devices) are based on ETSI QKD 004 standard. Each KMS is connected to at least one KMS that is considered to be its peer since they receive matching keys from the physical layer. Also, the SDN Agent (SDN Controller representative inside the node) is connected to the KMS and is used, from the KMS perspective, to retrieve information about the network, provide QoS parameters and to receive command orders. The type of key sources connected to the KMS might limit the keys that this one can provide. The connection to an oblivious key source is enough to provide both symmetrical and oblivious keys and even random numbers. Though the key rate might be lower because in order to generate a symmetrical key using oblivious keys, twice the size of the wished key will be used.

Apart from just receiving and sending keys through its South and North bound interfaces, respectively, the KMS needs to store, maintain, synchronize, derive and relay (forward) keys. The KMS is divided into various logical modules (Figure 4.2), namely:

- **KMS interface (north bound interface)** -> ETSI QKD 004 based interface to the applications. Interface to the SDN Agent (to be defined) and to its peer KMSs.
- **QoS Provider** -> Gathers and provides all QoS parameters to be used to negotiate with the applications and to send them to the SDN Agent when requested.
- **Synchronization manager** -> Handles the synchronization protocol.
- **Security component** -> Implements all cryptographic algorithms used during the operation of the KMS.
- **Key relay module** -> Handles the key relay (forwarding) process.
- **Key manager** -> Maintains and handles keys. It is mainly used for key material retrieval, storage, etc. It's involved in almost any activity related with keys.
- **Base functionality** -> Handles several quality-of-life features such as logging and configuration.
- **Device handler** -> Handles devices connected to the KMS (such as the QKD devices).

This is the base structure we will implement on our project. At this state, we haven't started building the architecture yet, since we are still trying to understand how we are going to implement all of these modules and how the KML will interact with the other components.

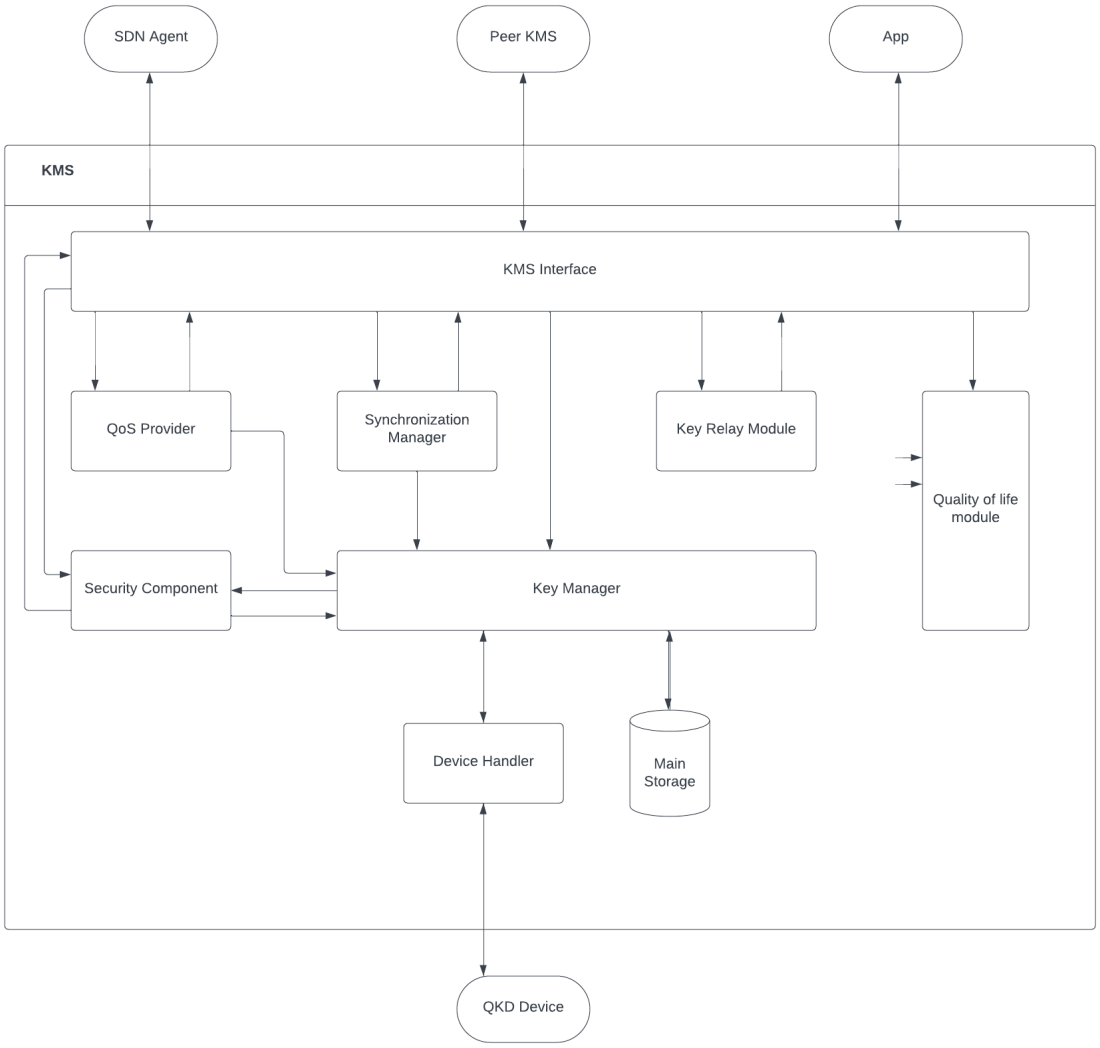

Figure 4.2: KMS Architecture.

Chapter 5

Conclusion

5.1 Conclusions

In this project, we propose a Key Management System for a Quantum Key Distribution Network that aims to provide a secure environment for key generation and distribution. Besides just getting quantum keys from Quantum Key Distribution devices, the system needs to become more flexible and better at adapting to what other systems/applications need.

In this report, we went over the background, the related work and the State-of-the-art, and detailed the Functional and Non-Functional Requirements that will guide our development. Additionally and ultimately, we demonstrated the main modules of the system architecture and their broad interactions. Previous projects displayed their modules with similar main functionalities, but we intend to implement and arrange them in a slightly different way, according to our architecture defined in Chapter 4.

Bibliography

[1] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 6 Aug. 1991. DOI: 10.1103/PhysRevLett.67.661. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

[2] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," *Opt. Express*, vol. 16, no. 23, pp. 18 790–18 797, Nov. 2008. DOI: 10.1364/OE.16.018790. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-16-23-18790.

[3] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Scalable qkd network using simple key-management technique with on-demand crypto-key supply," in *2008 34th European Conference on Optical Communication*, 2008, pp. 1–2. DOI: 10.1109/ECOC.2008.4729256.

[4] B. Korzh, C. Lim, R. Houlmann, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, Jul. 2014. DOI: 10.1038/nphoton.2014.327.

[5] Y. Zhang, Z. Li, Z. Chen, *et al.*, "Continuous-variable qkd over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, p. 035 006, May 2019. DOI: 10.1088/2058-9565/ab19d1. [Online]. Available: https://dx.doi.org/10.1088/2058-9565/ab19d1.

[6] R. Takahashi, Y. Tanizawa, and A. Dixon, "A high-speed key management method for quantum key distribution network," in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, 2019, pp. 437–442. DOI: 10.1109/ICUFN.2019.8806052.

[7] J. Y. Cho, J.-J. Pedreno-Manresa, S. Patri, *et al.*, "Demonstration of software-defined key management for quantum key distribution network," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, 2021, pp. 1–3.

[8] P. James, S. Laschet, S. Ramacher, and L. Torresetti, "Key management systems for large-scale quantum key distribution networks," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES '23, Benevento, Italy:

Association for Computing Machinery, 2023, ISBN: 9798400707728. DOI: 10.1145/3600160.3605050. [Online]. Available: https://doi.org/10.1145/3600160.3605050.