Unleashing Flexibility and Interoperability in QKD Networks: The Power of Softwarized Architectures

Blanca Lopez [1,2,*], **Ivan Vidal** [2], **Francisco Valera** [2], **Diego R. Lopez** [3], **Antonio Pastor** [3]
[1]IMDEA Networks Institute, Avda. del Mar Mediterráneo, 22, 28918 Leganés, Madrid, Spain
[2]Telematic Engineering Department, Universidad Carlos III de Madrid, Avda. Universidad, 30, 28911 Leganés, Madrid, Spain
[3]Telefónica, Ronda de la Comunicación, Fuencarral-El Pardo, 28050 Madrid, Spain
[*]Correspondence: blanca.lopez@imdea.org (B.L.)
https://doi.org/10.1109/MNET.2025.3538752

ABSTRACT

Softwarization and disaggregated architectures have transformed traditional communication networks by separating network control functions from the hardware, catalyzing innovation, and dramatically reducing deployment and operation costs. This paper extends these concepts to Quantum Key Distribution (QKD) networks, emphasizing the importance of virtualizing key management functions with advanced cloud-native technologies for enhanced global interoperability and flexibility. Our approach advocates for a fully disaggregated key management plane supported by softwarization and virtualization technologies, without losing sight of the established standards. The proposed model unlocks multiple benefits, including the facilitation of tailored access control mechanisms for QKD network administrators, the ability to apply real-time performance monitoring and base the control and management of the network on the gathered data, as well as conducting different key generation Quality of Service (QoS) admission control mechanisms on the QKD network. Moreover, a disaggregated model of the key management functions facilitates the implementation of different strategies for cross-domain collaboration between QKD network providers, as well as continuous key provisioning even in the midst of quantum infrastructure outages. The model has been validated through experiments in a virtualized environment, leveraging software tools to create customizable digital twins of QKD networks.

1 INTRODUCTION

As Quantum Key Distribution (QKD) networks advance toward providing theoretically unbreakable encryption, scaling them up remains challenging due to, among other things, their inherently rigid architectures. Current QKD network designs make interoperability and flexibilitythe ability to adapt to changesvery difficult to achieve, despite being critical features in any network construction. This paper posits that one of the keys to unlocking the full potential of QKD networks lies in the lessons learned from the evolution of contemporary classical network design, particularly the roles of softwarization and virtualization.

Although QKD networks obviously are, and will be, intrinsically based on hardware devices that take ad-

vantage of quantum properties, nowadays it is accepted that the difficulties of a standalone deployment of quantum networks are considerably high, and it seems to be more appropriate to schedule for integration and coexistence together with existing operator network infrastructure. In this sense, the evolution of the classical communication networks is a testament to the advantages of software-based adaptability over hardware-centric solutions. Softwarization and virtualization have not only enabled unprecedented ductility and pliability in traditional networks, but also fostered innovation and interoperability across diverse platforms and technologies. By abstracting the underlying hardware, they enable more agile and versatile network architectures. This machinery, which is already a reality implemented in our networks, creates dynamic and scalable environments capable of rapidly adapting to fluctuating demands. Drawing inspiration from the transformative impact of these concepts in established communication networks, this paper poses that a similar approach is critical for the evolution of QKD networks. We introduce a novel model where the key management functionalities are completely decoupled from the QKD nodes, departing from the conventional monolithic QKD node paradigm, while adhering to established standards. Well-established virtualization and softwarization technologies support this model. In particular, this work takes advantage of current notorious efforts towards the utilization of the Software Defined Network (SDN) approach to lead the synergistic integration of quantum and classical communication network environments, which is noticeable in the development of both theoretical and experimental work [1–4], as well as in the creation of standards that define a common framework for these implementations [5–7]. The work presented in this article progresses toward the virtualization of all core network functionalities.

First, an analysis focusing on standardization in the field is made, paying particular attention to standards that incorporate SDN technologies in the control layer, which represent a first step towards the softwarization and virtualization of QKD network functions, (Section 2). Then, the proposed model is presented and its advantages are discussed in greater depth (Section 3); to accompany the argumentation, a proof of concept carried out in a virtual environment of digital twins of QKD networks [8] is presented (Section 4), thus validating the proposal and opening the door for future experiments. Lastly, the conclusions of our work are gathered and new lines of research are set out (Section 5).

2 STANDARDIZATION AND RELATED WORK

The landscape of QKD networks is in a phase of swift evolution, both in terms of technology and standardization. In particular, the establishment of standards plays an essential role in the development and adoption of QKD networks. Significant organizations, such as ITU, ETSI, or IETF, have created specific committees [9–11] to develop standards that serve as a framework for building future quantum networks. Particularly, we will focus on those that discuss the incorporation of softwarized management technologies into such quantum networks. In these terms, two fundamental standards, ITU Y-3805 [5] and ETSI GS

QKD 015 [6], are presented. To contextualize the reader, we first discuss the QKD network architectures that these standards work with.

ITU specifications propose an architecture divided into separate layers, as well as differentiating between two QKD network models depending on whether the network control plane is centralized or distributed [12]. The centralized model can be seen in Fig. 1, where different layers are color-coded.

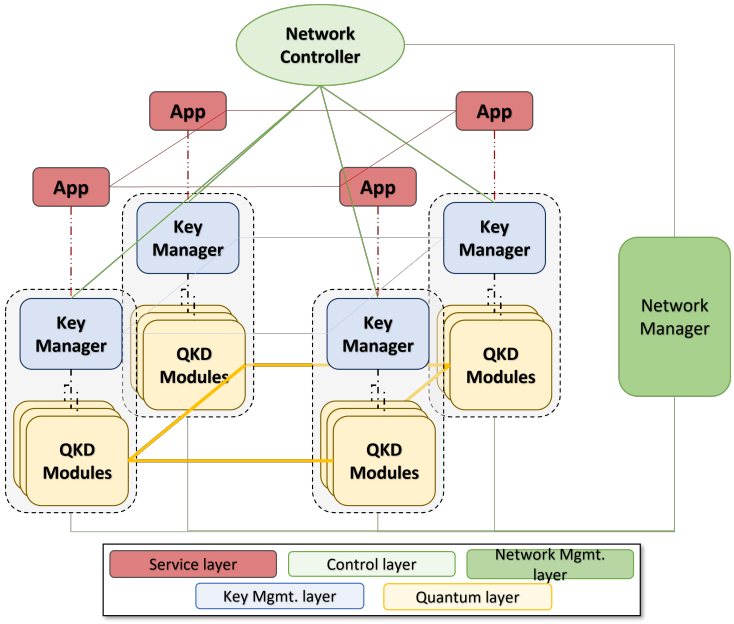

Figure 1: High-level design of centralized QKD network [12].

In line with these architecture proposals, the ITU Y-3805 standard [5] addresses the incorporation of SDN technologies in the control plane of QKD networks to enhance the control and management operations, as well as improve the efficiency of the network functions. The document outlines the functional architecture and various operational procedures of SDN control in QKD networks, such as service requests, key generation, and key supply among others [5].

ETSI has also been working for several years on standardizing QKD networks, publishing specifications that address a range of issues in such networks. The ETSI GS QKD 015 [6] standard extends the scheme presented in ETSI GS QKD 004 [13], where the QKD modules are composed of quantum components and a QKD Key Manager Peer, and adds an SDN-based control agent within the nodes, as well as including a controller for the complete QKD network. This architectural design permits the SDN controller to orchestrate the QKD resources to optimize QKD network functions. Including an SDN controller centralizes network management, allowing for dynamic configuration and enhancement of QKD resources based on network demands.

A more general document from the research branch of IETF, the IRTF, is being produced [7] which intends to describe a consistent reference architecture model for the Quantum Internet that enables agility, sustainability, and pliability. The architecture model is inspired by the separation of concerns, that have

been converging on the trends around open disaggregation strategies in classical network designs. The work already includes a section discussing the use of SDN technology in the control plane of the particular case of QKD networks.

These documents mark the initial shift from hardware-centric networks to more dynamic, software-based structures through softwarization and virtualization. They highlight the crucial roles of programmability and adaptability in responding to evolving network demands. With SDN, these approaches provide centralized control and dynamic resource management, enhancing the capacity of QKD networks to support growth, diverse applications, and optimized key distribution. Representing the first stage in exploiting the full potential of network virtualization, there have already been several QKD deployments that align with these standards [1, 2]. To maximize the advantages of softwarizationlike increased flexibility, scalability, and resource efficiencyfurther development beyond these established standards is essential.

3 DISAGGREGATION OF QKD KEY MANAGEMENT FUNCTIONS

The decoupling of the key management layer from the monolithic design of QKD nodes that has prevailed so far represents a step towards QKD networks global interoperability. This section will discuss the several advantages associated with this model, presenting a design in line with current standards. The main idea behind this scheme is the virtualization and disaggregation of the key management layer of the QKD network from the underlying hardware. An illustrated example of the design can be found in Fig. 2, where two applications request cryptographic material from two ends of a network.

The scheme separates the key management plane from the QKD nodes, creating a virtual layer over the physical QKD network. This enables, as will be discussed later, innovative elements of the control layer. The model would use SDN technology to, among other things, choose the most appropriate route once an application makes a request to obtain a key. The change of design would inherit all the advantages already available in standards defined with a centralized control layer thanks to SDN, in addition to achieving new features that would imply a step towards the real deployment of large-scale QKD networks.

Since the QKD networking landscape is a constantly evolving field, it is quite uncertain what the ultimate global framework will be once these technologies take hold. Software-centric solutions, historically more adaptable than hardware-based ones in quickly changing tech environments, motivate a transition. Our model encourages this shift in approach: by separating the key manager from its physical enclave, QKD networks gain the agility needed to cope with future developments. The main advantage of our approach is that it allows QKD networks to quickly and easily adapt to advancing technologies and regulatory standards, without complex hardware revisions. This facilitates innovation in key management functionalities and broadens participation to new stakeholders like application developers and cloud and edge service providers.

All further advantages identified by the authors that the proposed model offers are discussed below.

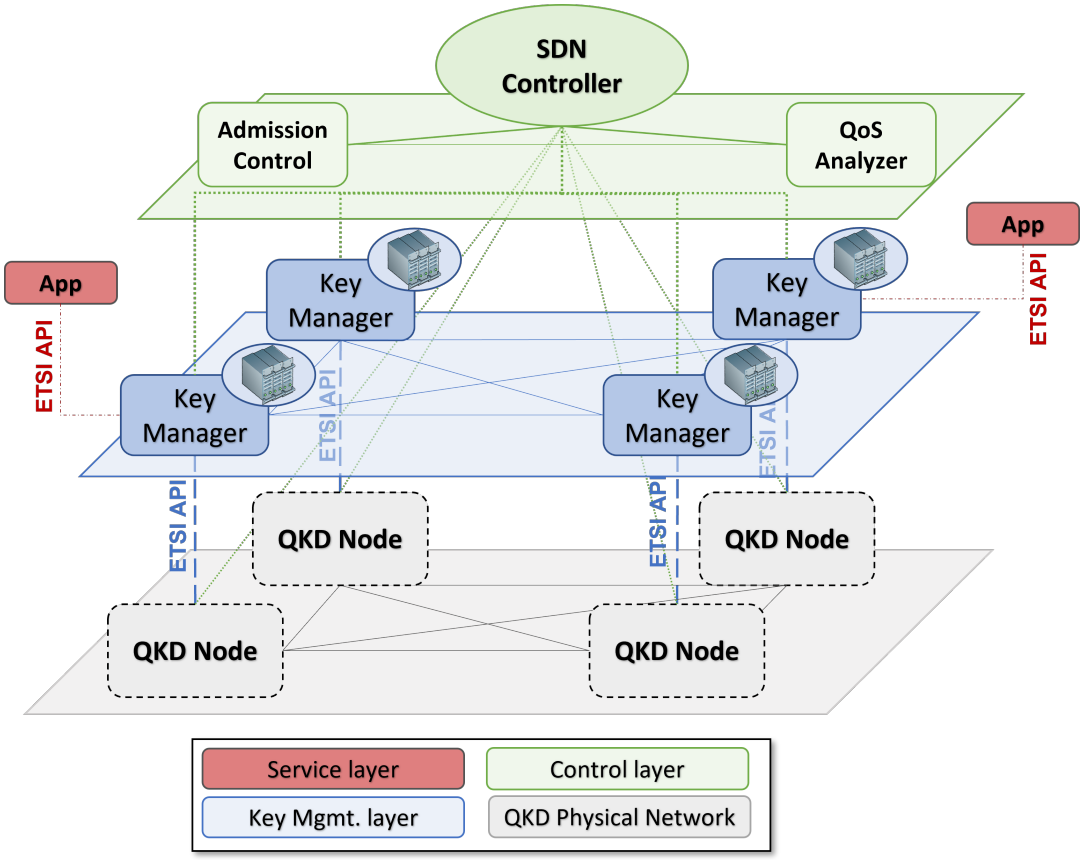

Figure 2: Outline of the proposed model design.

3.1 Tailored access control mechanism

Until now, the integration of key managers with QKD nodes has been rigid, as they are tightly bound to the manufacturers designs, limiting the adaptability of access control measures. This inflexibility hinders the implementation of alternative or enhanced access controls and modification of predefined ones, a significant constraint in large, commercial-scale networks managed by different service providers aiming to offer QKD services to their own users and between their users (inter-provider). The proposed design shifts access from the QKD nodes to a softwarized layer, allowing network owners to implement customized access control mechanisms. This flexibility ensures that only authorized users, devices, or processes can interact with the QKD network, thereby enhancing its security and operational integrity.

3.2 Real-time performance monitoring

Virtualizing a key management layer over the quantum network would unlock the capability to conduct different real-time diagnostics, thereby continuously monitoring the network operational status. The proposed model enables key managers to function as on-demand configurable applications, facilitating the execution of targeted control experiments. This dynamic scheme enhances agility in assessing and adapting the network QoS in real-time. It makes network administrators able to promptly identify and rectify potential issues and optimize network configurations. The disaggregation and virtualization of the

key management layer ensure that the QoS is not merely a static metric, but a dynamic feature of the QKD network, applicable to make a more responsive, resilient, and efficient network.

3.3 Data-driven control and management

The integration of the virtualized key manager layer with SDN technology, added to the possibility of doing real-time diagnostics of the condition of the network, unlocks great advantages we are starting to explore in detail. With a thorough understanding of the current operational state of the network, a new SDN component, that could be co-located with the SDN controller, would be uniquely positioned to optimize network functions such as selecting the most efficient paths for secure end-to-end quantum key exchange. Our model enables the implementation of these centralized functionalities, without the need to add additional hardware to the already complex QKD nodes, improving efficiency and adaptability in the management and performance of QKD networks.

3.4 QoS admission control mechanisms

Another advantage that is naturally derived from accessing real-time data is the implementation of QoS admission control mechanisms. Virtualizing and decoupling the key manager entity facilitate network administrators to develop admission control mechanisms that dynamically allocate network resources based on the QoS requirements of different cryptographic material requests, such as the size of said material, the required rate, or the request priority [13]. This ensures that critical applications can receive the QoS they need, without being adversely affected by less critical processes. This mechanism could be implemented, for example, by including an Admission Control component (as the one shown in Fig. 2) that has information about the network topology, as well as the updated QoS of the QKD links and the QoS required by the applications. This new element could therefore determine if the QKD network can admit or not a new request, and help to define the path that has to be followed over the key manager network to fulfill the request. The proposed scheme not only enhances the operational flexibility of QKD networks, but also ensures that they can deliver reliable service quality in an increasingly complex digital ecosystem.

3.5 Cross-domain QKD networks

One major issue in the QKD ecosystem is the fragmentation due to a hardware-centric approach. The diversity of manufacturers leads to a variety of QKD nodes, each with unique physical configurations, creating significant interoperability challenges as these nodes generally cannot communicate with each other. Similar to the early days of computing, the reliance on hardware-specific components within QKD nodes restricts innovation and hinders experimentation compared to software-based solutions. By focusing on a software-first approach and abstracting key functions like key management, we facilitate the creation of mechanisms for secure end-to-end key exchanges across a virtual key manager network. This approach enhances interoperability among nodes from different manufacturers and simplifies integration

across various administrative domains, potentially leading to a network of Key Managers networks that ensures seamless key exchange.

3.6 Continous key provisioning

In scenarios where the quantum infrastructure is compromised or unavailable, current QKD network designs have no mechanism to continue fulfilling their role of providing secure keys to the applications that require them. Virtualization of the Key Management layer in QKD networks represents a strategic approach for solving this issue, improving the resilience and adaptability of communications security. The flexibility offered by the model facilitates uninterrupted key provisioning, ensuring that secure communication channels remain operational even during quantum infrastructure outages. Our approach allows for the dynamic integration of auxiliary security mechanisms, for example, the system can seamlessly transition to leveraging post-quantum cryptographic protocols for key exchange in the event of quantum subsystem failure. The model therefore creates a barrier against vulnerabilities that may affect the physical structure, making the network resilient and adaptable. It ensures a trustworthy method of key exchange regardless of the operational state of the quantum network. This scheme not only safeguards against current and emerging threats but also guarantees continuous protection, reinforcing the robustness of secure communications.

3.7 Integration with classical designs

Last but not least, the virtualization of key management functions in QKD networks represents a strategic alignment with the dominant trends of virtualization and softwarization in current communication networks. This approach improves compatibility and simplifies the processes of integrating quantum networks into classical infrastructures. QKD networks could leverage some existing and widely adopted frameworks and standards of classical networks, paving the way for a smooth transition to quantum-enhanced security within classical infrastructures.

4 PROOF OF CONCEPT

An experiment was designed using a synthetic environment to better analyze the proposed model and test its feasibility. This setting utilizes Quditto [8], a service that allows deploying tailored digital twins of QKD networks in virtual machines or, as in our particular case, in virtualization containers. Quditto enables the design of digital twins of QKD networks that implement a standardized ETSI API, the one defined in [13], creating an ideal environment for the development of experiments and tests on models such as ours. In our scenario, a QKD network consisting of three nodes was deployed. Each of the Quantum Nodes had a virtualized Key Manager associated with it, implementing the ETSI 004 API [13]. In addition, two external Applications were created that made HTTP requests to their corresponding Key Manager, in line with the ETSI 014 standard model [14]. The possibility of using different standardized interfaces underlines the flexibility the environment offers. An outline of the experiment design can be seen

in Fig. 3. Note that this experiment is a basic proof of concept to show how our proposal works, but the framework used would allow for much more complex tests to be implemented.

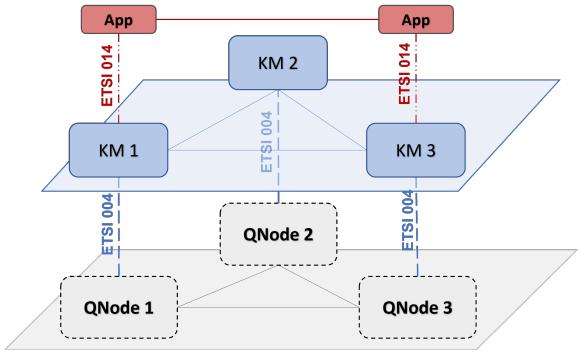

Figure 3: Topology of the conducted experiment.

Since the QKD network has a triangle topology, there are two possible paths for the applications to gain a symmetric key shared by two vertexes: one direct route and one indirect route. In Fig. 3, the indirect path corresponds to going through QNode 2.

To exemplify a more general case, we chose the indirect path to perform our proof of concept, emulating the behavior of a network with a trusted node. To provide both applications with a symmetric key, Key Manager 1 generates an end-to-end key which returns to the application, and after establishing enough shared quantum cryptographic material with QNode 2, encrypts it using Advanced Encryption Standard (AES) and said quantum cryptographic materialit should be noted that the choice of this protocol was discretionary, as any other could have been selected. This encrypted key is then sent to Key Manager 2, which can decrypt it due to having the same quantum cryptographic material. Key Manager 2, having also established shared cryptographic material with QNode 3, re-encrypts the key using AES and sends it to Key Manager 3. Key Manager 3 decrypts the key and forwards it to the application, ensuring both applications receive a secure symmetric key protected by quantum encryption throughout their network journey. This mechanism can be seen schematically in Fig. 4.

4.1 Results

Under the described design of the experiment, we take time measurements of the different events that occur in the process from the time applications request a key until they obtain it. The graph included in Fig. 5, shows the results. In our case the key managers were configured to store three extra keys, so after the first request and consequent response, the manager stores three extra keys to speed up the process in the following requests. It should again be noted that this implementation has been chosen as any other could have been selected, highlighting the flexibility offered by digital emulation for the verification and testing of proposals such as ours.

As can be seen in Fig. 5 two different quantum keys have to be created before the key manager can send a response to the application. Once they successfully obtain that material, they generate the response for

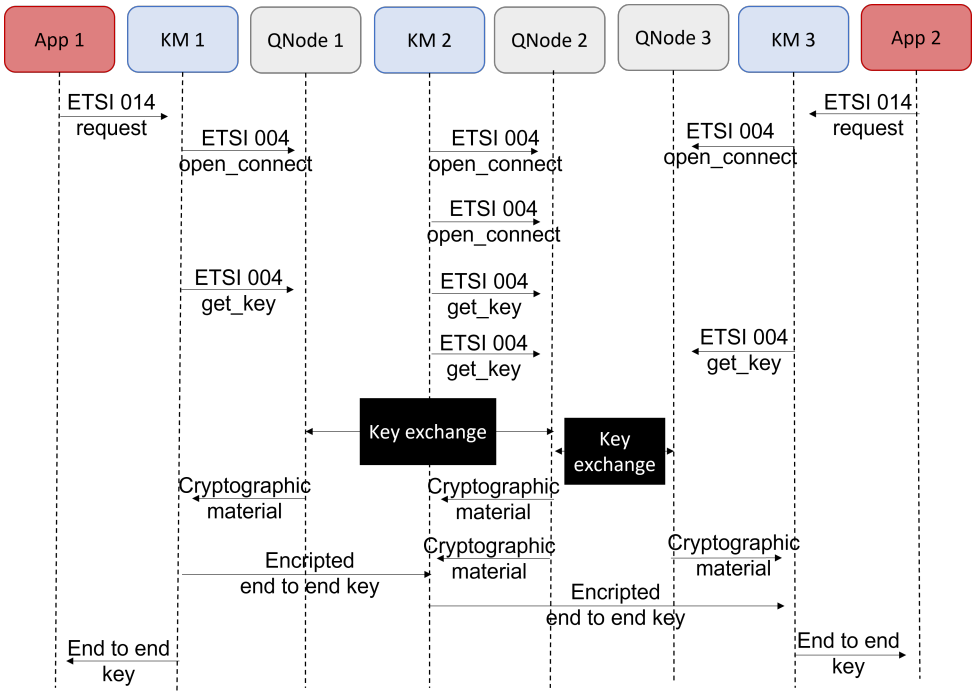

Figure 4: Flow diagram of the conducted experiment.

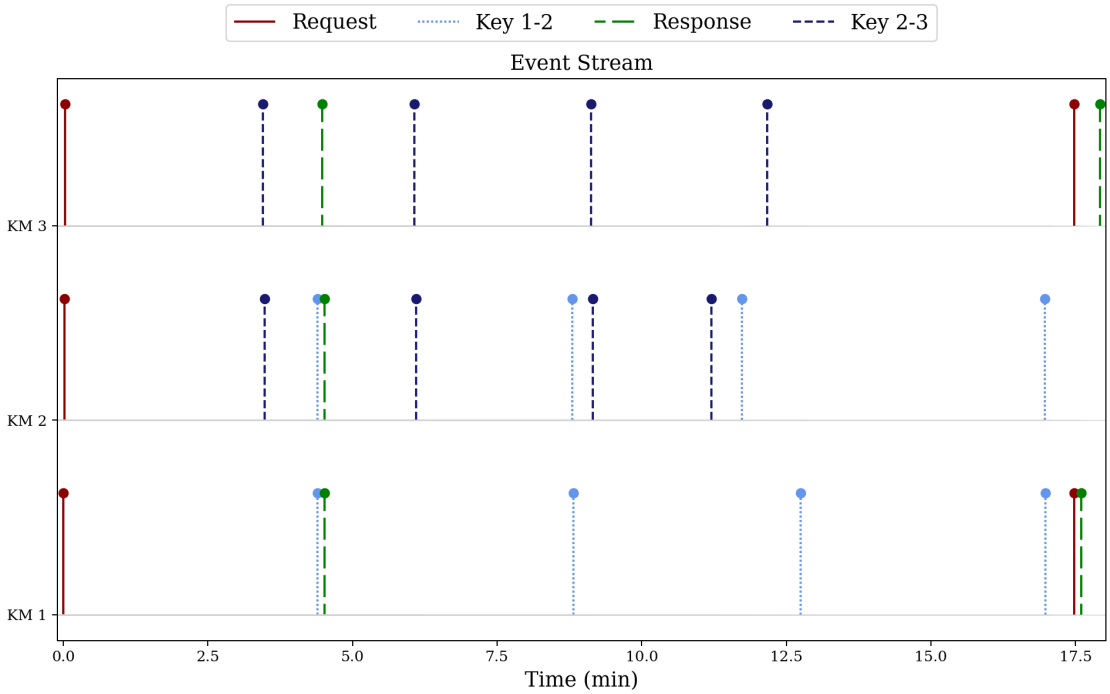

Figure 5: Time measurements of the conducted experiment.

the application and continue to store three more keys so that, when the next request is received, the response generation is much faster. It is worth mentioning that the cryptographic material formation times should not be taken as reliable, since they depend on the computational implementation and do not correspond to the real case.

5 CONCLUSIONS

This paper delineates a pioneering step towards adopting a software-first approach in QKD networks, which will significantly influence the evolution and adaptability of quantum networks on a global scale. It introduces a model that detaches the key management layer from its hardware constraints, which enhances network flexibility, interoperability, and performance. The benefits highlighted include customized QoS mechanisms, real-time monitoring, and continuous key provisioning.

Future work will focus on the study of the integration of the model with SDN elements, aligning the model with existing SDN standards, and evaluating their collective impact on network efficiency. These advancements aim to develop a flexible key management ecosystem that leverages both quantum and classical network technologies, setting the stage for a more adaptable and robust quantum communications infrastructure.

ACKNOWLEDGMENT

This research is part of MADQuantum-CM project, funded by the Regional Government of Madrid, the Spanish State through the Recovery, Transformation and Resilience Plan, and the European Union through the NextGeneration EU funds; it is also part of the project 6GINSPIRE PID2022-137329OB-C42, funded by MCIN/AEI/10.13039/501100011033/. Authors have also been supported by the European Unions Horizon Europe research and innovation programme under projects QSNP (grant agreement No 101114043) and PQ-REACT (grant agreement No 101119547).

REFERENCES

[1] Obada Alia, Rodrigo Stange Tessinari, Emilio Hugues Salas, George Kanellos, Reza Nejabati, Dimitra Simeonidou, *Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks*, Journal of Lightwave Technology, vol. 40, no. 17, pp. 5816-5824, 1 Sept.1, 2022, doi: 10.1109/JLT.2022.3183962

[2] Vicente Martin et al., *Quantum Aware SDN Nodes in the Madrid Quantum Network*, 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 2019, pp. 1-4, doi: 10.1109/ICTON.2019.8840338

[3] R. S. Tessinari, R. I. Woodward, and A. J. Shields, *Software-Defined Quantum Network Using a QKD-Secured SDN Controller and Encrypted Messages*, Optical Fiber Communication Conference (OFC) 2023, Technical Digest Series (Optica Publishing Group, 2023)

[4] Hua Wang, Yongli Zhao, and Avishek Nag, *Quantum-Key-Distribution (QKD) Networks Enabled by Software-Defined Networks (SDN).* Applied Sciences. 2019; 9(10):2081. https://doi.org/10.3390/app9102081

[5] ITU-T, *Quantum key distribution networks Software-defined networking control*; ITU-T Y.3805 (2021) Amd. 1 (11/2023); ITU: Geneva, Switzerland, 2023.

[6] ETSI, *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks*; ETSI GS QKD 015 V2.1.1 (2022-04); ETSI: Sophia Antipolis, France, 2022.

[7] Diego Lopez, Vicente Martin, Blanca Lopez, and Luis Miguel Contreras, *A Multiplane Architecture Proposal for the Quantum Internet*. Internet Engineering Task Force, 2023. Work in Progress. Available online: https://datatracker.ietf.org/doc/draft-lopez-qirg-qi-multiplane-arch/.

[8] Raul Martin, Blanca Lopez, Ivan Vidal, Francisco Valera, and Borja Nogales *Service for Deploying Digital Twins of QKD Networks*. Appl. Sci. 2024, 14, 1018. https://doi.org/10.3390/app14031018

[9] ETSI Industry Specification Group (ISG) on Quantum Key Distribution (QKD). Available online: https://www.etsi.org/committee/1430-qkd.

[10] IETF Quantum Internet Research Group (QIRG). Available online: https://datatracker.ietf.org/group/qirg/about/.

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

[12] ITU-T, *Quantum key distribution networks Functional architecture*; ITU-T Y.3802 (2020) Amd. 1 (11/2023); ITU: Geneva, Switzerland, 2023.

[13] ETSI, *Quantum Key Distribution (QKD); Application Interface*; ETSI GS QKD 004 V2.1.1 (2020-08); ETSI: Sophia Antipolis, France, 2020.

[14] ETSI, *Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API*; ETSI: Sophia Antipolis, France, 2019.