S. Wendzel et al. (Hrsg.): SICHERHEIT 2024,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2024 301

Ways for confidential and authenticated hop-by-hop key establishment in QKDN

Johanna Henrich[1]

1 Motivation & Problem

Asymmetric cryptography, specifically key exchange and digital signatures, enables secure digital communication. However, sufficiently powerful Quantum Computers, which could be available within a few years [Eh21], would be able to break classical primitives like Elliptic-Curve Diffie–Hellman (ECDH) and RSA in polynomial time [Sh97]. Moreover, the „harvest-then-decrypt"-attack [Sc16] poses the danger that stored encrypted data can be decrypted later. Thus, alternative approaches are urgently needed. Besides Post Quantum Cryptography (PQC) [Xu23], which is based on mathematical problems, Quantum Key Distribution (QKD) uses quantum effects, to establish keys in an information-theoretically secure way [Me20]. Nevertheless, there are no reliable QKD modules that bridge distances of more than 150 km [Me20]. Therefore, a QKD Network (QKDN) uses a concatenation of QKD links. End users are connected to each other via a series of QKD nodes performing a hop-by-hop key forwarding. All nodes involved have access to the final shared secret. If a node cannot be trusted the security of the system is no longer guaranteed. Physical protection or key hybridization can mitigate this risk, where hybridization refers to the combination of QKD and PQC. By using both schemes appropriately, the security objectives are met as long as at least one of the schemes used has not been compromised [Gi22]. Nonetheless, there is a lack of concrete concepts and analyzes to enable a secure and efficient key forwarding process. In the following, 'secure' implies the security objectives of confidentiality and authenticity. 'Efficient' refers to the time taken to complete the process, the amount of data transferred and the amount of computing required. The analyses available often only consider specific sub-processes, e.g., forwarding between two directly adjacent nodes. The integration into the entire system and its resulting effects are disregarded. A systematic comparison of different options is missing. When implementing a QKDN, it is unclear which variant is suitable for one's own intentions. This PhD project aims to address the problem by defining the key establishment process, analyzing security requirements, designing and implementing corresponding schemes, and evaluating these approaches.

2 Related Work

Numerous research projects on QKDN test beds have been carried out [El07; Eu23; Ló21] and in the field of standardization, various organizations, e.g., International Telecommunication

[1] Darmstadt University of Applied Sciences, Schöfferstr. 3, 64295 Darmstadt, Germany, johanna.henrich@h-da.de

doi: 10.18420/sicherheit2024_024

Union (ITU) [IT20] and European Telecommunications Standards Institute (ETSI) [Le12] have established working groups and released guidelines. [Me20] provide a good overview of projects and current achievements. However, a comprehensive effort towards security on top of the quantum layer is notably absent [Eh21]. Studies such as [Bi19; Bo23; Fi20] describe different theoretical approaches for quantum-safe security schemes in the context of authentication, Authenticated Key Exchange (AKE), confidential data transmission and hybridization. Furthermore, some investigate their practical usage [Go14; Se22]. As part of this scope, [Br23; Ja23] take into account the communication between Key Management Systems (KMS) in a QKDN. KMS form part of the relay nodes. They manage (quantum) keys and specifically carry out the key forwarding. [Br23] outlines a protocol for a hybrid AKE that employs a certificate-based approach with PQC signature algorithms. In [Ja23] the implementation and integration of a KMS in QKDN is discussed from a wider perspective. Section 3 deals with hybridization, including a reference to [Br23]. There is a shortage of a detailed study of the implementation choices and their effect on the system as a whole.

3 Objectives and Goals

The aim of this work is to enable an secure and efficient establishment of shared secrets between two distant parties, Alice and Bob, in a QKDN. Given the variety of QKD technologies, QKDN architecture designs and use cases, as well as the corresponding boundary conditions within a QKDN, it appears that there is no single solution that can fully meet all requirements. Thus, the objective is not a 'one-fits-all' solution, but to identify overarching concepts and to evaluate and classify them. Therefore, the key exchange in the overall system is divided into generic sub-processes, which can be combined into a complete process at a later stage. In this context, classical symmetric cryptographic methods, PQC algorithms as well as alternative approaches, which, e.g., offer information-theoretic security (ITS), are considered. In principle, the work should be divided into three main aspects. Firstly, the *Identification* of the process steps involved in key forwarding within a QKDN as well as the definition of respective *Requirements* for each step. Secondly, the specification of various *Design*s, focusing on the previously defined security requirements, followed in part by their *Implementation*. Finally, the *Evaluation* of the previously designed approaches by analyzing security and performance.

4 Expected Contributions

Based on the fundamental question of how to achieve a secure and efficient key establishment in a QKDN, we investigate the following research questions:

R1 *(Identification & Requirements) Which communication steps, including interfaces and protocols, need to be considered when establishing a key between two end-users in a QKDN and how can these be characterized? What functional and non-functional (security and performance) requirements should they meet?*

R2 *(Design & Implementation) How can interfaces and underlying communication processes be designed and implemented and which cryptographic schemes and protocols can be used?*

R3 *„(Evaluation) How does the design (R2) impact security and performance of the key forwarding in a QKDN?“*

5 Approach

Concerning *Identification & Requirements*, the procedure for establishing keys in a QKDN, including the components involved and their interfaces, is first defined. It is then broken down into generic sub-processes. Already published concepts and recommendations, such as the ITU-T Y.3800 series [IT20], are incorporated. As a basis for the *Design & Implementation* phase, existing approaches for the individual sub-processes are analyzed. If these methods fail to meet the relevant criteria, they must be extended or entirely novel ones must be developed. The outcomes of [Br23; Ja23] can form a starting point. During the *Evaluation*, the aforementioned aspects security and performance are considered. To evaluate the security of existing schemes, evaluations and formal proofs from the literature are used and categorized. When designing protocol schemes, a self-contained cryptographic analysis is conducted. To ensure confidentiality and authenticity of the exchanged key, aspect such as ITS and hybridization must be considered. The performance evaluation can be made by referencing existing literature or investigating performance within a QKDN testbed.

6 Current Findings and Contributions

Based on the research project DemoQuanDT [Fe22] as well as technical standards from ITU-T and ETSI [Me20], a basic system architecture was developed. It defines the connection between two users in a QKDN as described in [He23a]. Figure 1 illustrates a breakdown into the different sub-processes labelled with blue numbers. Step 1 involves the initial communication request from Alice to Bob. In Step 2 Alice contacts her QKDN access node. Step 3 involves forwarding a secret platform key k_p between adjacent QKD nodes. Step 4 utilizes k_p acquired in Step 3 to exchange the final user key k_u between Alice and Bob over an arbitrary network connection. This approach allows to pre-establish keys between major traffic hubs (in later, more developed networks) and thus bypass hop-by-hop forwarding at the time of a request. Additional security mechanisms, e.g., hybridization, can also be implemented at this stage. In Step 5, k_u is forwarded from the access nodes to Alice and Bob. Finally, Step 6 involves exchanging user data between Alice and Bob, using k_u.

An initial hybrid AKE design was constructed for steps 3 to 6. It is shown in Figure 2. It combines a QKD key with a PQC key, using an HMAC-based Key Derivation Function (HKDF) [Kr10]. The authentication of the PQC key is accomplished through use of pre-shared public Key Encapsulation Mechanism (KEM) keys beforehand, as delineated

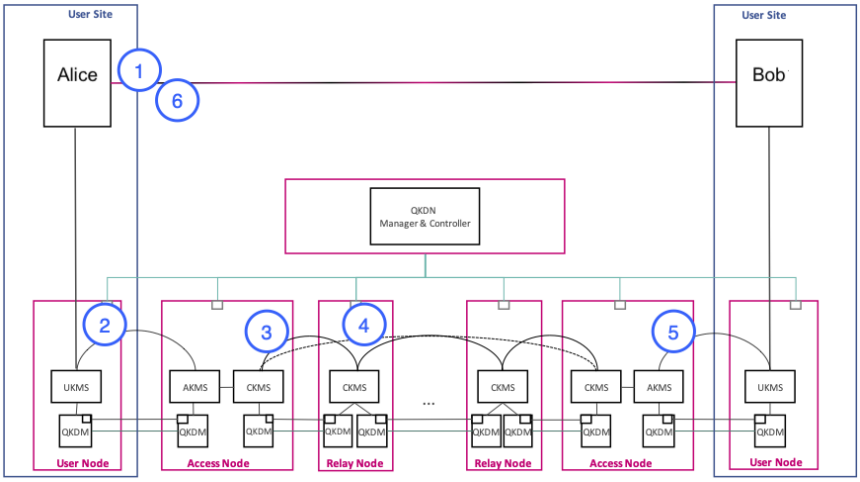

Fig. 1: Simplified QKDN Architecture:Alice and Bob connected via QKDN

in [Bo23]. The resulting hybrid key can be employed for encryption, e.g., via TLS 1.3 with pre-shared keys.

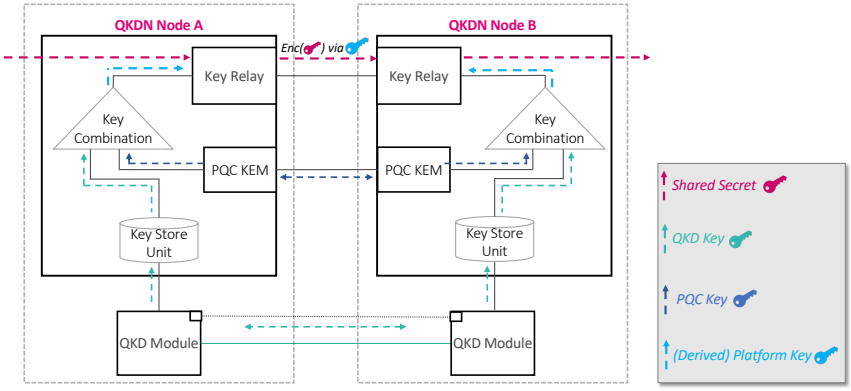

Fig. 2: Hybrid Key Establishment combining QKD and KEM-based AKE for PQC

A performance evaluation of TLS 1.3 using various KEM showed that the use of PQC is generally possible without major delays, even under hybrid use and inadequate network conditions [He23b]. Thus, TLS 1.3 via PQC has the potential to enable hybrid key forwarding in QKDN. The evaluation of FrodoKEM [Bo16], which is recommended by the BSI [Eh21], showed that it generally underperforms compared to other PQC variants or classical schemes, especially at higher security levels. However, these shortcomings can be partially mitigated by appropriate network configuration as described in [He23b].

7 Next Steps

Firstly, clear definitions of the sub-processes outlined in Section 6 need to be established and individual requirements should be identified. Furthermore, conducting a comprehensive literature review, particularly in relation to authentication, AKE, key combination and symmetric encryption in the context of QKDN, will enable the identification of potential security schemes. A mapping will be made after comparing the interface requirements with the scheme conditions. It is then possible to decide whether an extension or a completely new scheme implementation is necessary. E.g., the hybrid AKE outlined in Section 6 will serve as a first illustration for a final key forwarding scheme. The new and old schemes will be theoretically analyzed and practically evaluated in a testbed. Moreover, evaluating PQC algorithms in-depth concerning their performance in the context of TLS and additional protocols is also planned.

References

[Bi19] Bindel, N. et al.: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In: Post-Quantum Cryptography. Springer International Publishing, pp. 206–226, 2019.

[Bo16] Bos, J. et al.: Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.

[Bo23] Boyd, C. et al.: Modular Design of KEM-Based Authenticated Key Exchange, Cryptology ePrint Archive, Paper 2023/167, 2023.

[Br23] Bruckner, S. et al.: Muckle+: End-to-End Hybrid Authenticated Key Exchanges, Cryptology ePrint Archive, Paper 2023/653, 2023.

[Eh21] Ehlen, S. et al.: Kryptografie quantensicher gestalten, tech. rep. BSI-Bro21/01, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021.

[El07] Elliott, C. et al.: DARPA Quantum Network Testbed./, July 2007, URL: https://apps.dtic.mil/sti/tr/pdf/ADA471450.pdf, visited on: 11/30/2023.

[Eu23] European Commission: European Quantum Communication Infrastructure (EuroQCI), 2023, URL: https://digital-strategy.ec.europa.eu/de/policies/european-quantum-communication-infrastructure-euroqci, visited on: 11/02/2023.

[Fe22] Federal Ministry of Education and Research (BMWF): DemoQuanDT. Quantenschlüsselaustausch im deutschen Telekommunikationsnetz für höhere IT-Sicherheit, 2022, URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt, visited on: 11/15/2023.

[Fi20] Fischlin, M. et al.: Information-Theoretic Security of Cryptographic Channels. In: Information and Communications Security. Springer, pp. 295–311, 2020.

[Gi22] Giron, A. et al.: Post-quantum hybrid key exchange: a systematic mapping study. Journal of Cryptographic Engineering/, 2022.

[Go14] Goorden, S. A. et al.: Quantum-secure authentication of a physical unclonable key. Optica 1/6, pp. 421–424, Dec. 2014.

[He23a] Henrich, J. et al.: Crypto-Agile Design and Testbed for QKD-Networks. In: Proceedings of the 2023 European Interdisciplinary Cybersecurity Conf. ACM, Stavanger, Norway, 2023.

[He23b] Henrich, J. et al.: Performance Impact of PQC KEMs on TLS 1.3 under Varying Network Characteristics. In: Proceedings of the 2023 Int. Security Conf. Vol. 14411. Lecture Notes in Computer Science, Springer, Groningen, Netherlands, 2023.

[IT20] ITU-T: Overview on networks supporting quantum key distribution, tech. rep., July 2020, URL: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1, visited on: 09/24/2021.

[Ja23] James, P. et al.: Key Management Systems for Large-Scale Quantum Key Distribution Networks. In: Proceedings of the 18th Int. Conf. on Availability, Reliability and Security. ARES '23, ACM, Benevento, Italy, 2023.

[Kr10] Krawczyk, H. et al.: HMAC-based Extract-and-Expand Key Derivation Function (HKDF), RFC 5869, 2010, URL: https://www.rfc-editor.org/info/rfc5869.

[Le12] Lenhart, G.: QKD standardization at ETSI. In: AIP Conf. Proceedings. Vol. 1469. 1, American Institute of Physics, pp. 50–57, 2012.

[Ló21] López, D. et al.: Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks. In: Optical Fiber Communications Conf. and Exhibition (OFC) 2021. IEEE, 2021.

[Me20] Mehic, M. et al.: Quantum Key Distribution: A Networking Perspective. ACM Comput. Surv. 53/5, 2020, URL: https://doi.org/10.1145/3402192.

[Sc16] Schanck, J. et al.: Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography, tech. rep., IETF, 2016, URL: https://datatracker.ietf.org/doc/html/draft-whyte-select-pkc-qsh-02.

[Se22] Seok, S. K. et al.: A Design of Secure Communication Architecture Applying Quantum Cryptography. Journal of Information Science Theory and Practice 10/spc, pp. 123–134, June 2022.

[Sh97] Shor, P. W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26/5, Oct. 1997.

[Xu23] Xu, G. et al.: An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography. In: 2023 57th Annual Conference on Information Sciences and Systems (CISS). Pp. 1–6, 2023.