Demonstration of Software-defined Key Management for Quantum Key Distribution Network

Joo Yeon Cho[1], Jose-Juan Pedreno-Manresa[1], Sai Patri[1], Andrew Sergeev[1], Jörg-Peter Elbers[1], Helmut Griesser[1], Catherine White[2], Andrew Lord[2]

[1]ADVA Optical Networking, Fraunhoferstrasse 9a, Martinsried, Germany, 82152
[2]BT Labs, Adastral Park, Ipswich, U.K
jcho@adva.com

Abstract: We demonstrate a practical key management scheme for a quantum key distribution network. Multi-vendor QKD systems are interoperated via a standard interface and a key relay is dynamically routed by SDN. © 2021 The Author(s)

1. Overview

Quantum key distribution (QKD) is a method of the secret key establishment between two remote peers, based on the laws of quantum physics. The QKD network is composed of multiple point-to-point QKD links where keys are securely relayed and shared between two parties even though the QKD devices are not directly connected. The QKD protocol may differ for each QKD link and each QKD key may be produced independently by a different vendor. Hence, a key format and its metadata may be different from each other.

We demonstrate a practical key management system for a vendor agnostic QKD network. It can integrate various QKD systems from different vendors into a single network, retrieve their QKD keys in a standard form, and use them to relay an encryption key to the end users in a quantum-secure way.

To support the interoperability of QKD devices from different vendors, a key management agent on a trusted node is functionally decoupled from a QKD network and access QKD keys individually via the ETSI standard key delivery interface. Each agent can collect keys from intermediate QKDs, encrypt them by the one-time pad, and deliver the ciphertext to the destination node. A key is generated at the source node and relayed through a chain of QKD links which are dynamically allocated by an SDN controller. The key is restored at the destination node by XORing all the ciphertexts received from the intermediate nodes [1]. Trusted nodes are mutually authenticated by a quantum-secure authentication method which is immune to retrospective decryption by future quantum computers.

We implement a key management system on commercial products which have multiple network interfaces and a feature of tamper-resistance. We demonstrate a high-speed quantum-secure optical communication based on a dynamic key relay mechanism using multiple trusted nodes as shown in Figure 1.

2. Innovation

The distance limit of the point-to-point QKD can be overcome by using either quantum repeaters or trusted nodes. Among those, the trusted node is so far the most practical solution to build an arbitrary long distance of the QKD link. We demonstrate a flexible key management solution which has the potential to integrate an unlimited number of trusted nodes for a meshed QKD network. Our solution is entirely based on the standard interface and QKD vendor agnostic. A key relay route is dynamically allocated by an SDN controller. By our solution, a complex QKD network can be easily integrated into an existing telecommunication network.

3. OFC Relevance

Even though a large scale of quantum computers has not arrived yet, the deployment of new solutions against quantum threats becomes already an important requirement in optical networks. In this demo, we show that a QKD network can be easily integrated into an existing optical network by introducing a glue layer for a key management. Our solution does not depend on any proprietary interface of QKD vendors and it can be implemented on a commercial product using standard interfaces. Our solution is already deployable in the optical networks.

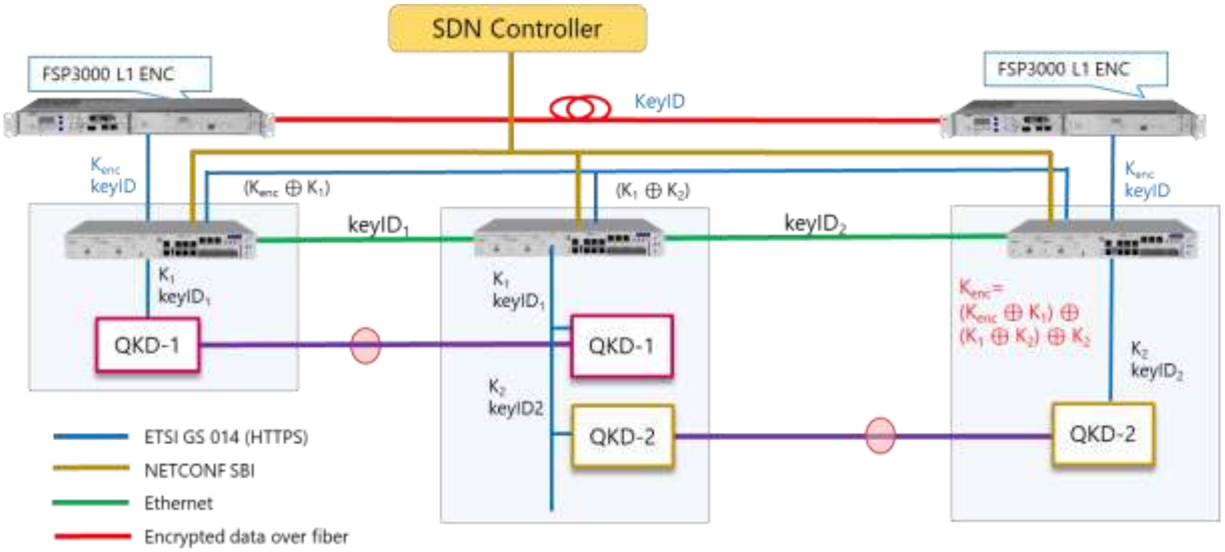

Figure 1. Configuration of the key management system using two QKD links

4. Components of key management system

4.1 Trusted node

Our demo is composed of commercial products available in the market. The key management agent can interact with multi-vendor QKD devices, retrieve their QKD key individually. These keys are OTP-encrypted and delivered to the destination node. The keyID of the 2nd QKD key is sent to the next node via an Ethernet port. The key relay route can be dynamically switched by an SDN controller, depending on the available keys in the QKD network. The key management agent has potential to interconnect more than two QKD links to deal with a meshed QKD network. A user has an option to insert its own key and let it relay over the QKD network.

A node-to-node communication is performed using the ETSI GS 014 interface. An OTP-encrypted key is delivered to the destination node via an HTTPS-based secure channel. Trusted nodes are mutually authenticated by verifying their PKI certificates before the key is delivered. The PKI certificate is produced under the post-quantum PKI. For maximum strength against any computational attack or capability, the node authentication can be done using a symmetric pre-shared key. A fraction of the exchanged secret key can be used to refresh the pre-shared secret between nodes which require secure communication.

A built-in key database provides the capability of buffering the OTP-encrypted QKD keys to speed up the key relay and reduce the latency. Note that it can be configured not to buffer any key if required. A block diagram of the key management agent is shown in Figure 2.

4.2 Standard key interface

An HTTPS-based secure key delivery interface between a QKD system and an encryptor has been standardized by ETSI [2]. In our demo, this standard interface is extensively applied for the interaction among key relay nodes as well. Note that the standard key delivery interface relies on the classical public-key cryptography such as RSA or ECC. However, it can be extended to a hybrid key interface including post-quantum cryptography.

The interface can be in one of two different phases: registration and key delivery. In the registration phase, every node creates a public/private key pair and installs a PKI certificate which is signed by the certificate authority. In the key delivery phase, a secure channel between two parties is established based on their certificates and a key delivery is performed via RESTful APIs over the secure channel.

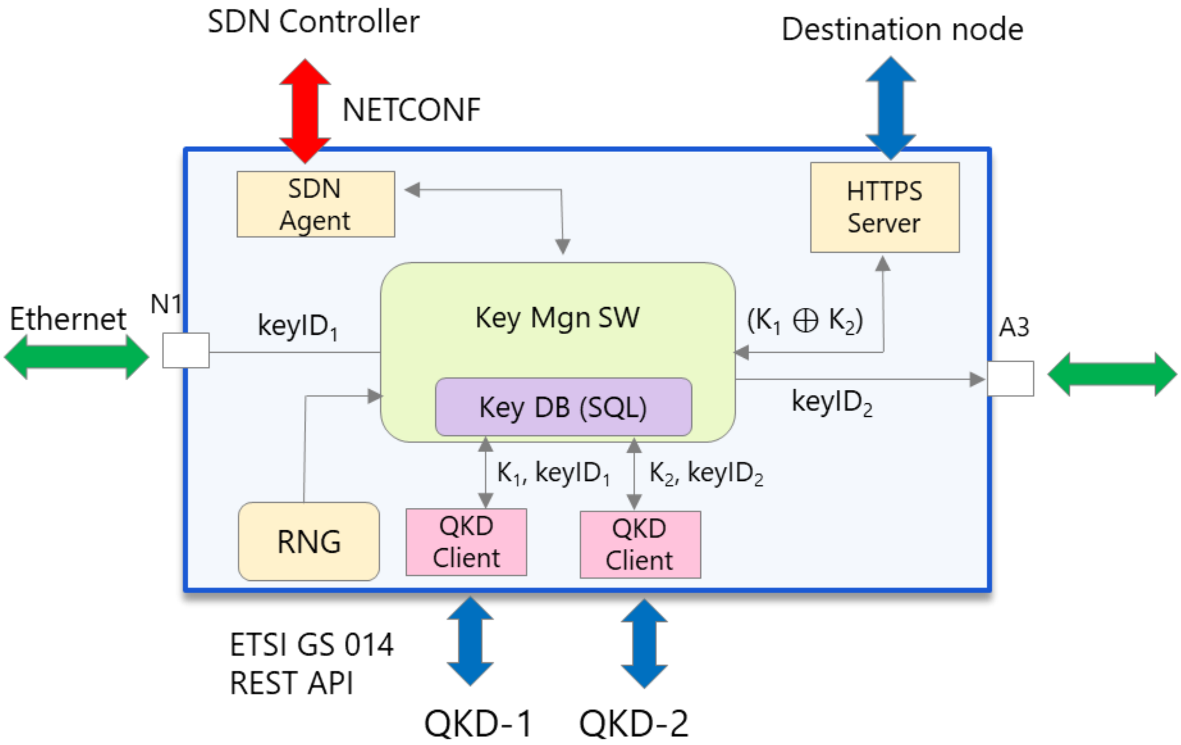

Figure 2. A block diagram of the key management agent on ADVA FSP150

4.3 *SDN controller*

In a meshed QKD network, a centralized SDN controller oversees dynamically provisioning and rerouting key relay routes, thus fulfilling the QKD service or network robustness requirements. The controller can poll key relay information from trusted nodes using NETCONF as a south bound interface (SBI) in conjunction with proprietary YANG models.

5. Acknowledgements

This research is co-funded by OpenQKD project under the Horizon 2020 Framework Program of the European Union (Grant agreement No 857156).

6. References

[1] ETSI, "Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications," GS QKD 014, V1.1.1 (2018).

[2] ITU-T, Y.3803, "Quantum key distribution networks – Key management," (2020).