Demonstration of Classical and Hybrid Solutions for Lightpath Security Using Quantum Keys

Morteza Ahmadian[1], Jaime Buruaga[2], Ruben Mendez[2], Juan P. Brito[2], Antonio Pastor[3], Jose M. Rivas[3], Jaume Comellas[1], Marc Ruiz[1], Vicente Martin[2], and Luis Velasco[1*]

[1] Universitat Politècnica de Catalunya (UPC), Barcelona, Spain; e-mail: luis.velasco@upc.edu

[2] Universidad Politécnica de Madrid (UPM), Madrid, Spain; [3] Telefonica I+D, Madrid, Spain

ABSTRACT

Optical communications have enabled high-speed data transmission over long distances. However, data are transmitted plain unless are encrypted on higher layers, e.g., IP and TCP, precisely because of: *i*) the high data rates; and *ii*) the need of secure key exchange between the end-points of the optical connection. Meanwhile, quantum enabled cryptography has emerged as a promising solution for securing communications by leveraging the principles of quantum mechanics which provides unlimited and unconditional security. Although Quantum Key Distribution (QKD) protocols can deliver quantum keys to distant end-points, there are scenarios where one of them is not within the security perimeter of the quantum network. This demonstration focuses on the intersection of optical communication and quantum security, highlighting the synergies between these two domains and their potential to ensure secure communication networks. We explore the integration of optical communication with quantum technologies and showcase how optical encryption using quantum keys retrieved from QKD and Quantum Random Number Generator (QRNG) systems is performed. Retrieved keys are expanded to the required rate and then used to encrypt the input data at line speed.

1. OVERVIEW

The high capacity and low latency of optical connections are key to support current and future services, including 6G. Traditionally, services requiring secure communications use data encryption at the IP and TCP layers, using standard stream ciphers, like Advanced Encryption Standard and ChaCha. However, secure transmission at the optical layer is still not massively implemented, mainly due to the added delay and the limitations of those cryptographic methods to work at line speeds of 400Gb/s or higher. In our previous paper [1], we proposed Light Path SECurity (LPsec). LPSec is a secure cryptographic solution for optical signals (e.g., 16 QAM) that involves fast bit stream encryption using stream ciphers and key exchange by implementing the Diffie-Hellman protocol through the optical channel. The security level of LPSec is, however, limited by classical Pseudo-Random Number Generators (PRNG), which are used to generate and expand the symmetric keys that are needed for the encryption.

This demonstration showcases the use of quantum-generated keys to improve the security level of LPSec, taking advantage of the random properties of quantum physics. Specifically, two scenarios are targeted where keys are retrieved from: (A) a Quantum Key Distribution (QKD) network, when the two optical transponders (Tp) are inside of the security perimeter of the QKD network; and (B) a Quantum Random Number Generator (QRNG) when only one of the Tps is inside the security perimeter of the quantum network. In both cases, quantum keys feed two nested ciphers that provide a high security level: *i*) the outer cipher is a substitution cipher that relies on a Lookup Table (LUT) used for the substitution of bits before sending them to the optical modulator; and *ii*) the inner cipher is a stream cipher that encrypts data chunks of predefined size based on a cryptographically secure. An optical connection between two Tps will be set up using a software-defined networking (SDN). In Demo A, both Tps will connect to their local Key Manager (KM) to retrieve keys exchanged through a QKD system connecting the premises of Telefónica in Madrid, Spain. In Demo B, the Tp inside the security perimeter retrieves keys from a local key server in a QRNG and exchanges them through the classical optical channel in a secure way. The workflows have been designed in the Horizon Europe ALLEGRO project [2].

2. INNOVATION

QRNGs devices generate randomness by measuring quantum processes and hence, are an ideal resource for cryptographic purposes. QRNGs are usually part of QKD networks that allow for the distribution of symmetric keys with bounded security between parties. In that regard, a QKD network can be seen as a distributed QRNG, where the random keys appear at two ends of the network.

In Demo A, we will showcase encryption of a 16 QAM optical signal using the keys retrieved from a QKD network. Such keys are used in LPSec as input to a key expansion mechanism based on a secure PRNG to encrypt the input bit stream at line rate. Note that the perfect security provided by the QKD network is reduced by the high expansion rate, as QKD systems provide throughputs from hundreds of kb/s to few Mb/s, depending on the system.

The research leading to these results has received funding from the European Union's Horizon Europe research and innovation programme under G.A. No. 101092766 (ALLEGRO) from the MICINN IBON (PID2020-114135RB-I00) projects and from the ICREA Institution.

979-8-3503-7732-3/24/$31.00 ©2024 IEEE

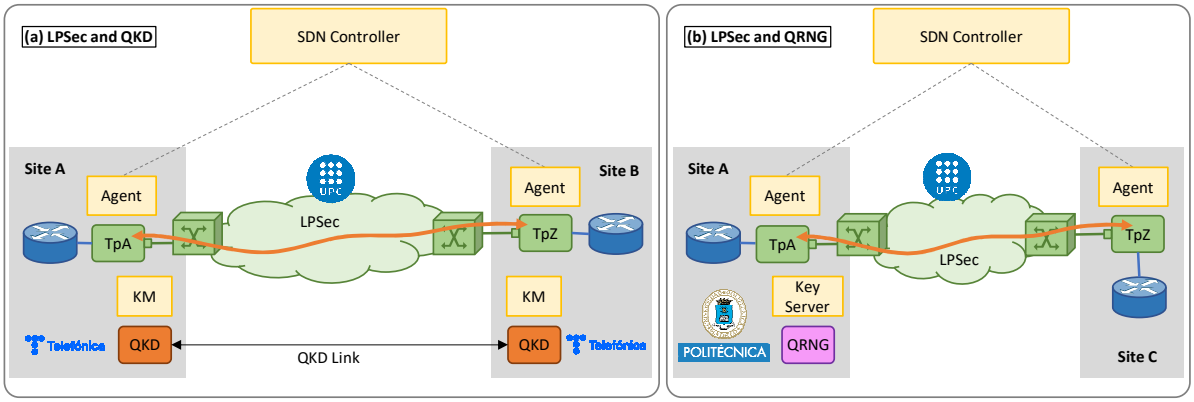

Figure 1. Demonstration scenarios: Lightpath end points are inside QKD security perimeters (a) and only one end point is in a security perimeter.

To achieve the highest security level, however, both Tps need to be within the security perimeter of the QKD network, which is not always possible, e.g., when one of the Ts is in the access network. For this very reason, in Demo B, we will show LPSec using a single QRNG as the entropy source, where keys are: *i*) retrieved by the local Tp; *ii*) used to encrypt the optical signal; and *iii*) distributed to the remote Tp within the optical signal. Therefore, LPSec is used in this case to extend farther the reach of the quantum network security perimeter. In addition, because QRNGs have high throughput (about 1 Gb/s), moderate expansion to reach the desired line rate is needed.

3. DEMO CONTENT

This section describes the workflows of the proposed demonstrations. Details of the workflows have been intentionally omitted due to the space constraints; please refer to [1] for details, especially those related to LPSec, e.g., the use of public/private keys, KxF, LUT, etc.

LPsec extends the standard coherent transponder with optical encryption and decryption blocks, as well as with some key management functionalities; note that cryptographic blocks operate at line speeds, so optical encryption is based on simple operations performed on the input bit stream. The encryption is based on two nested ciphers: *i*) a substitution cipher for scrambling symbols, where a LUT is used to create a ciphered gray map constellation through LUT permutations of incoming bits; and *ii*) a stream cipher that encrypts data chunks of predefined size based on a cryptographically secure PRNG to generate a sequence of stream keys from an input random key *k*. However, the sequence of stream keys generated by the PRNG from a given input key cannot be infinite as this would reduce the security level, and the LUT permutation needs to be periodically regenerated to minimize vulnerabilities. In consequence, we limit the lifetime of keys *k*, e.g., to 1 sec., which entails new keys being periodically made available at the two ends of the lightpath. Because the two Tps needs to communicate among them, we defined a special frame named Key exchange Frame (KxF). The KxF is generated by the Tx and includes a known pattern as header and sent to the Rx periodically.

In Demo A, the two Tps are in sites covered by the QKD network, so keys *k* can be retrieved from the local KMs using standard interfaces, we rely on ETSI GS QKD 004 [3], and used as input to the PRNG. In this case, the KxF header is used for synchronization purposes between the two Tps. Figure 1a presents the scenario of this demo. Two QKD systems with their respective KMs are deployed in Telefónica's premises in Madrid, Spain and connected to create a QKD link. Optical transmission and LPSec, including encryption and key exchange is implemented in a simulator running in UPC premises in Barcelona, Spain. An SDN controller is in charge of lightpath provisioning and LPSec configuration. Finally, two Tp agents are on top of the local Tps for configuration purposes and communicate with the SDN controller. Demo A extends case 1 "undefined KSID in a single link scenario" defined in [3], to be used for LPSec connection set-up. Note that case 5 defined in [3] could be also implemented in the case that QKD systems in sites A and B are in the QKD network but not directly connected through a single QKD link. The workflow (see Figure 2) starts after the lightpath has been established (step 0). LPSec requires an initial public key exchange to be carried out during connection set-up through the SDN controller. In this case, the keys are used to generate the particular KxF header pattern that will be used. The SDN collects the public key and the ID of TpZ (1) and sends them to the agent of TpA together with the details of the local KM (2). Both agent A and B use the OPEN_CONNECT function to connect to their local KM indicating the ID of TpA as source and TpZ as destination, and receive the Key stream ID (KSID) to be used for retrieving keys (3, 3'). The KM in site A coordinates internally with the KM in site B to create the association KSID in the two sites and TpA and TpZ send the KM connection confirmation to their agents (4, 4'). Agent A sends the public key, the ID of the local Tp, and the KxF header pattern encrypted with the public key of TpZ to the SDN controller (5), which, in turn, sends them to agent B (6). Agent B decrypts KxF header and both ends are ready to use the optical connection with encryption (7).

Now, the two Tps have to synchronize so they can start using the right keys to encrypt the data stream. To that end, the SDN controller requests the agents of the Tps to start the synchronization (8, 8'). In the case of TpA, the local Tp has to retrieve the first key, and use it to encrypt a known bit stream; the KxF header is inserted periodically and it includes the index of the retrieved key (9-12). In the case of TpZ, the agent retrieves two keys (10', 11), where the first key will be used during the synchronization period while the second key will be used once that period finished. The TpZ should be able to successfully decrypt the known bit stream and find the same index in the KxF header as the one got from the local KM. That is reported to the SDN controller (13, 14). The SDN controller requests agents A and B to start with the real data encryption (15, 17). Then, TpA gets the next key from the local KM (18), sends its index in the KxF header (19) and starts encrypting the incoming bit stream with the new key. Note that TpZ already had the key to use for decrypt the data, so it uses immediately, and retrieves the next key from the local KM (20). Steps 18-20 repeat at every time interval until the optical connection is torn-down, when both agents use the KSID to terminate the association with the KMs.

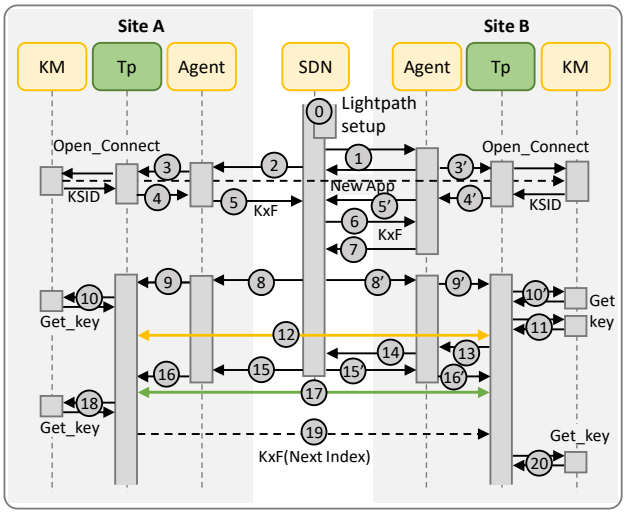

Figure 2. Workflow of Demo A.

In Demo B, only one of the Tps is in a site covered by the QKD network. In this case, keys *k* can be retrieved from a local QRNG through a vendor-proprietary interface. In this case, the KxF header of LPSec is used as well for the distribution of the keys between the two Tps. Note that this is in addition to the synchronization mechanism as in Demo A. Figure 1b presents the scenario, where the QRNG system is used. As in Demo A, the workflow (see Figure 3) starts after the lightpath has been established (step 0). The initial public key exchange is carried out and used to generate the particular KxF header pattern that will be used on the optical channel for synchronization between the two Tps (1-3). Next, TpA retrieves a key from the local key server that will be used for data encryption (4). The retrieved key is sent to the SDN controller encrypted using the public key of TpB, together with the generated KxF header pattern, which are sent to TpB (6-8). Once TpB is able to get synchronized with TpA through the optical channel, a reply is sent to the SDN controller (10, 11). When TpA receive the confirmation that the encryption of the data stream can start (12, 13), it requests a new key from the local key server (15), encrypts it using the previous retrieved key and sends it within the next KxF header (16). Steps 15-16 repeat at every time interval until the lightpath is torn-down.

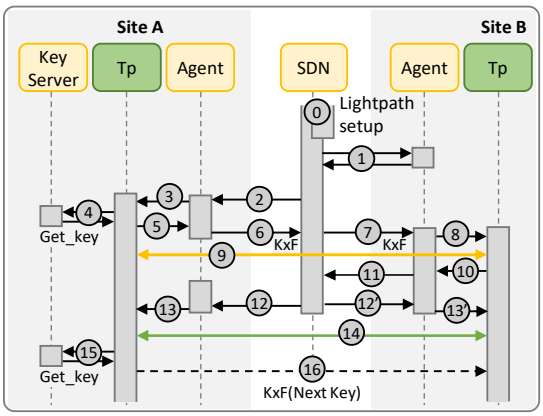

Figure 3. Workflow of Demo B.

4. IMPLEMENTATION

For the demos, real QKD and QRNG systems will be used. In the case of, Demo A will rely on experimental HWDU continuous-variable QKD devices [4]. The link spans 15 km and connects two Telefonica's facilities; it provides 8.4 Kb/s key rate through an ETSI GS QKD 004 interface. Regarding Demo B, a QuSIDE QRNG system will be used as quantum entropy source. The QRNG implements a proprietary phase-diffusion technology and has embedded randomness metrology capabilities [5], [6] to produce very high-quality random bits at 4 Gb/s. The system exposes a proprietary REST API interface to deliver the random bits.

A video streaming service will be used to demonstrate the connectivity and an eavesdropper will show data encryption. Iteration of the attendees with the system will be facilitated with a Web interface, so they can define the scenario to be demonstrated and change parameters.

For illustration purposes, we show how the development of the workflows is performed. The agents, Tps and SDN controller exchange massages implementing the workflows described in the previous section and they can be run through different terminals, as shown in Figure 4. The lightpath setup is triggered through an interface shown in the SDN controller terminal; agents' terminals show that the agents exchange their public keys to encrypt the KxF header. Then, Tps ask the QKD KMs to get the KSID, which is shown in the QKD KM terminals. Next, the SDN controller asks Tps to start synchronization and Tps retrieve the keys that will be used for data encryption and decryption. Then, the SDN controller ask Tps to start data transmission so the video server can start sending

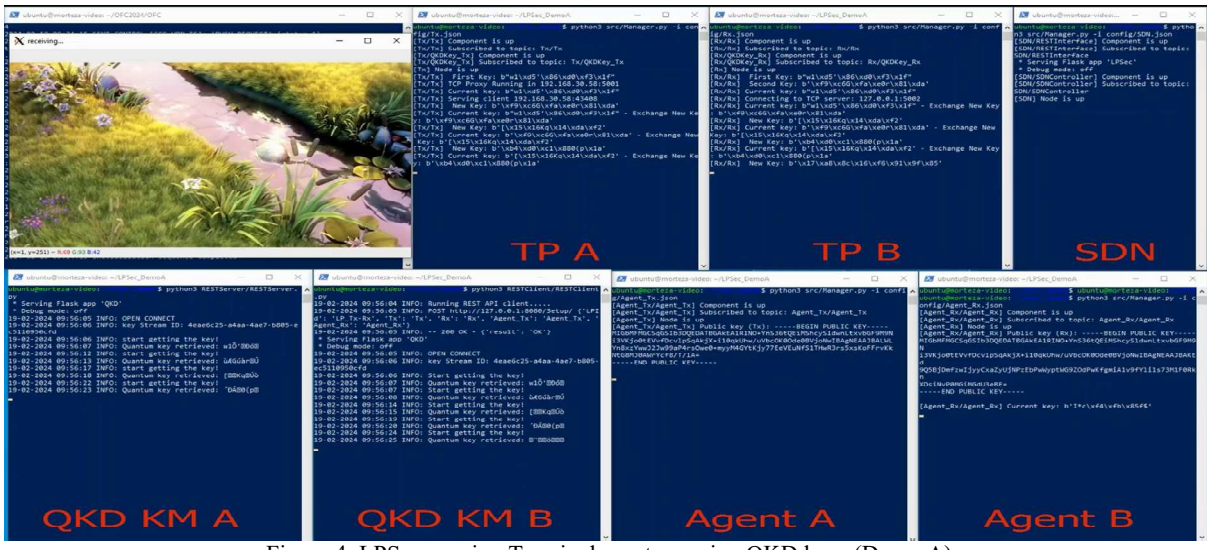

Figure 4. LPSec running Terminals capture using QKD keys (Demo A)

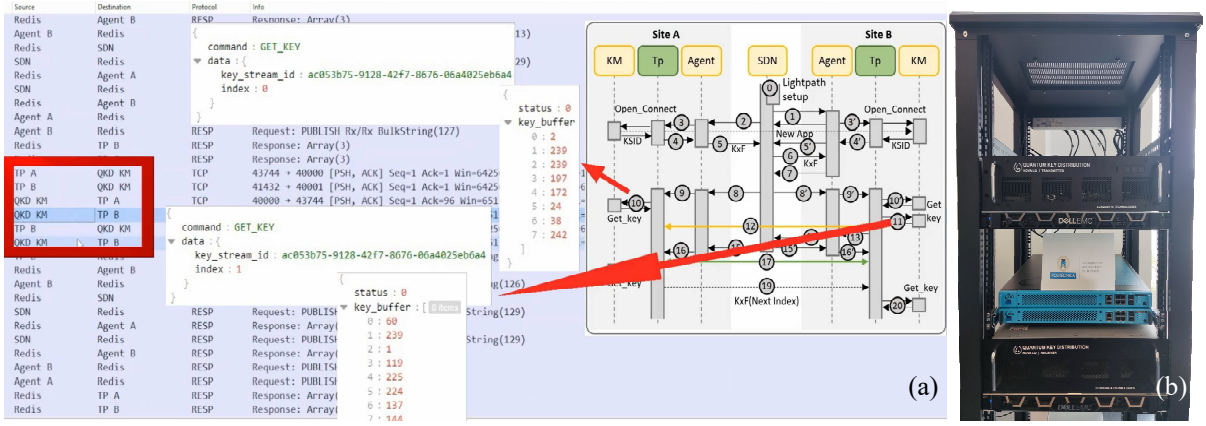

Figure 5. (a)Wireshark Capture when keys are being retrieved (Demo A) (b) QKD endpoints

the video stream to the video client. Here, standardized interfaces are used to retrieve keys from the real QKD systems (Figure 5b). Terminals of QKD KM A and QKD KM B are also showing the retrieved keys. Tps terminals show the current keys and the new keys once they receive them. Keys can be tracked to ensure that the keys are correctly retrieved. The video played by the video client is also shown after decrypting the received data stream.

We use Wireshark to track the messages exchanged between the components. Figure 5a, shows a Wireshark capture when the keys are being retrieved from the QKD endpoints in Demo A. Tps asks keys using the KSID they have retrieved beforehand and the index of the keys. We see that TpA asks for one key with index 0 (step 10) while TpB asks for two keys with 0 and 1 indexes to avoid the delay in the decryption steps in site B by having one key ahead of time.

5. CONCLUSION

LPSec has shown its ability to provide bit stream encryption at line speed, while introducing noticeable low processing delay. The combination of LPSec and quantum security represents another step to secure classical optical communications, as it allows upgrading technologies currently deployed in operators' network with quantum security, thus saving costs by extending their lifespan.

REFERENCES

[1] M. Iqbal *et al.*, "LPsec: A Fast and Secure Cryptographic System for Optical Connections," JOCN, 2022.
[2] HORIZON-CL4-2022 "Agile ultra-low energy secure networks" (ALLEGRO) [On-line] https://www.allegro-he.eu/
[3] "Quantum Key Distribution (QKD); Application Interface," ETSI GS QKD 004 v.2.1.1, 2020.
[4] H. Brunner *et al.*, "Demonstration of a switched CV-QKD network," EPJ Quantum Technology, 2023.
[5] A. Mitchell *et al.*, "Strong experimental guarantees in ultrafast quantum random number generation," Physical Review, 2015.
[6] C. Abellán *et al.*, "Generation of fresh and pure random numbers for loophole-free Bell tests," Physical review letters, 2015.