2024 International Conference on Quantum Communications, Networking, and Computing (QCNC) | 979-8-3503-6677-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/QCNC62729.2024.00044

A Security Plane Architecture for Ultra-low-energy, High-capacity Optical Transport Networks

J.M. Rivas-Moscoso[1], A. Melgar[1], L. Potì[2], K. Krilakis[3], L. Velasco[4],
S. Bahrani[5], M. Svaluto Moreolo[6], I. Tafur Monroy[7], P. Nguyen[8], M. Ruiz[4],
D.K. Syvridis[3], A. Mandilara[3], A. Pagano[9], J. Morales[1], A. Pastor[1], R. Nejabati[5],
R. Wang[5], P. Nadimi Goki[10], A. Sánchez-Macián[11], S. Civelli[12], S. Rommel[7], C. Rubio García[7],
M. Iqbal[6], R. Oliveira[5], J.C. Hernández-Hernández[11], D. Larrabeiti[11] and J. Folgueira[1]
[1]Telefónica Global CTIO, [2]CNIT, [3]Eulambia Advanced Technologies, [4]Universitat Politècnica de Catalunya,
[5]University of Bristol, [6]CTTC/CERCA, [7]Eindhoven University of Technology, [8]Secure IC, [9]Telecom Italia,
[10]Scuola Superiore Sant'Anna, [11]Universidad Carlos III de Madrid, [12]Consiglio Nazionale delle Ricerche
Email: josemanuel.rivasmoscoso@telefonica.com

***Abstract*—The evolution toward agile, ultra-low-energy, high-capacity optical transport networks can benefit from solutions incorporating multi-band, multi-fiber, and point-to-multipoint (P2MP)/sliceable high-capacity transport technologies carefully designed to simplify network hierarchy and minimize optical-electrical-optical (OEO) conversions. To guarantee quantum-secure communications, these networks require a thorough reassessment of their security plane architecture, acting as a transversal plane to the data and control planes. In this paper, we propose a programmable Quantum Key Distribution (QKD) network built upon multi-protocol QKD systems, including entangled QKD for P2MP secure access/metro scenarios, Quantum Random Key Generation (QRNG) modules as alternative entropy sources for links where QKD system deployment is not economically viable, and hybrid classic/QKD/Post-Quantum Cryptography (PQC) primitives for greater flexibility and backward compatibility. Authentication services are performed through physically-unclonable-function (PUF) certification authorities, particularly implementing strong Rayleigh-backscattering-pattern or speckle-pattern-based optical Physically Unclonable Functions (OPUFs). These security technologies leverage on agnostic key management system (KMS) and quantum digital twin (QDT) assisted performance optimization, e.g. for artificial intelligence (AI)-based State of Polarization (SOP) compensation. Key relay between border nodes is realized by means of a combination of a centralized PUF and a procedure to securely exchange keys between KMSs based on ETSI-014 and PQC. The KMS can feed keys to encryptors implemented at the different data-plane layers, but the proposed architecture favors encryption relying on physical-layer security techniques to align with the above design principle aimed at a flatter network and fewer OEO conversions. Examples of this are Light Path SECurity (LPSec) techniques, consisting of two nested physical ciphers ensuring a high-security level, and all-optical steganography. Coexistence of classical and quantum signals is generally feasible in the access and metro segments, whereas in the backbone segment it needs to be evaluated on a case-by-case basis.**

***Index Terms*—QKD, PUF, KMS Relay, Steganography, LPsec, Optical Fingerprint, Optical Transport Network**

1. Introduction

Next-generation packet-optical transport networks must address four essential pillars of telecommunication systems: (1) ultra-high capacity from access to core, (2) power consumption and cost reduction, (3) autonomous network control management, and (4) secure and reliable optical transmission. The ALLEGRO project [1] aims to design, prototype and demonstrate an end-to-end (E2E) network architecture achieving ultra-high capacity leveraging sliceable smart bandwidth-variable transceivers and switching elements for point-to-point (P2P) and point-to-multipoint (P2MP) multi-band (MB) and multi-fiber transmission/switching of up to 32 Tb/s. Power consumption and total cost of ownership are minimized by consolidating network segments into two fundamental structures: the long-reach access and the metro-backbone, enabled by the aforementioned data-plane innovations and the utilization of pervasive telemetry and artificial intelligence/machine learning for autonomous network diagnosing, provisioning and healing. The security of both the data and control planes is ensured by quantum and classical cryptographic methods leveraging Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC) and classical approaches for key distribution and authentication, alongside the development of a quantum digital twin (QDT), for a complete future-proof security solution.

The security of a network is described in terms of three main aspects: confidentiality, integrity, and authenticity. Confidentiality involves protecting sensitive information from unauthorized access through techniques such as data encryption and access control. Integrity ensures that information remains intact and unaltered, safeguarding it from unauthorized or accidental modifications. This is achieved

979-8-3503-6677-8/24/$31.00 ©2024 IEEE
DOI 10.1109/QCNC62729.2024.00044

through access control mechanisms and digital signatures, which verify that data have not been tampered with during transmission or storage. Authenticity verifies the genuineness of data or individuals, ensuring that they have not been forged. Strong authentication protocols, such as two-factor authentication and digital signatures, are used to verify the identity of users and devices, as well as the authenticity of transmitted data. A security plane architecture must address these critical aspects, while accommodating the specific requirements dictated by the network architecture, infrastructure and involved entities.

Ultra-low energy, high-capacity networks such as the one proposed in the ALLEGRO project require the design of a new security plane architecture that integrates existing solutions and other innovative technologies. Currently, several connectivity planes are utilized to provide the flexibility required by the different network segments. Optical Transport Network (OTN) encryption, for instance, is used for connections with datacenters or special demands from clients such as governments, the defence sector, or large corporations. Higher-level connectivity planes are better suited for services in existing 4G/5G mobile networks, where the connections between base stations and the operator's point of presence (PoP) are protected with IPSec via a security gateway before accessing the network core services. Ultra-high capacity networks will also take advantage of this flexibility, but will mainly rely on Physical Layer Security (PLS) for encryption, which enhances security and contributes to power consumption savings by reducing the amount of optical-electrical-optical (OEO) conversions required by higher-layer encryption. This aligns with the trend toward less hierarchical and compartmentalized architectures that favor transparent E2E transport by bypassing unnecessary aggregation IP routers. Moreover, PLS supports operation at the high line speeds required by the Optical Transport Network through key augmentation techniques at the expense of reducing security, which will be acceptable for non-critical connections. Various PLS implementations will be presented in the paper.

For quantum-safe security, the proposed architecture incorporates QKD for distributing cryptographic keys. QKD ensures, through fundamental principles of physics, key distribution for encryption at different layers. In the proposed security architecture, we explore multi-protocol QKD systems that enable switching between Discrete-Variable QKD (DV-QKD) and Continuous-Variable QKD (CV-QKD) protocols, enhancing the network flexibility to address various user requirements in terms of reach, secret key rate (SKR), and complexity. Additionally, entanglement-based QKD systems are considered for P2MP scenarios, resulting in reduced overall costs and power consumption as fewer QKD modules are required compared to protocols inherently designed for P2P communications, such as CV-QKD and DV-QKD. The proposed solutions aim to achieve key distribution over the same fibers used for classical communications [2], which is of paramount importance for network operators [3]. However, MB transmission introduces notable challenges that need to be addressed. Hybrid QKD and PQC solutions are envisioned to ensure secure and resilient authentication mechanisms, such as for key relay between key management systems (KMSs) belonging to different network domains. Finally, the network makes use of novel authentication mechanisms leveraging optical Physically Unclonable Function (OPUF) systems. These systems exploit the inherent randomness and unique characteristics of optical components to generate fingerprints, which serve as robust authentication tokens for verifying the identity of network entities. OPUF offers enhanced security against various attacks, including cloning and spoofing attempts.

The rest of the paper is structured as follows: Section 2 gives an overview of the technologies and solutions enabling the design of the innovative security plane architecture proposed in the ALLEGRO project. Section 3 offers a detailed description of how these technologies are integrated and synergize to achieve a quantum-safe security plane architecture. Finally, in Section 4, we present our conclusions.

2. Enabling Technologies for an Innovative Security Plane Architecture

In this section, we provide a concise overview of the technologies explored for secure key distribution, authentication, and encryption. These technologies contribute to the innovative security plane architecture detailed in Section 3.

2.1. Key Distribution Technologies

The security architecture proposed in this work primarly relies on QKD as the key distribution approach for achieving the highest level of security. The architecture considers two commercially leading QKD technologies: DV-QKD [4], and CV-QKD [5]. While DV-QKD excels in key distribution over longer distances, simplicity, and robustness against eavesdropping due to its reliance on single-photon states, CV-QKD presents advantages in terms of SKR and seamless integration with existing optical communication infrastructure. Transmission of both the quantum channel (QC) and classical channels, including synchronization and other QKD auxiliary channels, over the same optical fiber is of great interest to operators. In the case of CV-QKD, co-propagating classical channels with the QC at different wavelengths through Dense Wavelength Division Multiplexing (DWDM) requires careful considerations of suitable channel power levels and spacing to address coexistence and optimize the performance of both classical and quantum channels [9]. Recent results, obtained using VpiPhotonics simulation software (SW) [10], demonstrate that CV-QKD can coexist in the C-band with 8×200 Gb/s channels, with degradation in the performance of the QC observed as the classical channel power increases (up to a total of 9 dBm) [11]. However, this degradation can be mitigated by increasing the guard-band to more than 100 GHz [12].

The architecture design incorporates the concept of multi-protocol systems [13], ensuring the flexibility to seamlessly transition between different QKD technologies with-

out the need for hardware (HW) changes. It is relevant for the deployment of networks interfacing segments using different QKD protocols and for incorporating trusted nodes. Moreover, a QKD device that supports multi-protocol allows for combining the benefits of different protocols within one device and adapts to a specific task.

Furthermore, the proposed security architecture includes entanglement-based QKD systems, leveraging broadband polarization-entangled photons and supporting protocols like BBM92 [6], to enable P2MP communication. Recently, researchers have demonstrated an entanglement-based quantum network with dynamic reconfiguration capabilities, utilizing a novel quantum-enabled reconfigurable optical add-drop multiplexer (q-ROADM) [7], [8].

2.2. Authentication Technologies

Like human beings, each chip possesses a unique fingerprint created during manufacturing. This intrinsic characteristic can be revealed by incorporating a specific circuit architecture onto the chip, known as a physically-unclonable-function (PUF) circuit, which serves to verify the identity of network entities. PUF circuits take a sequence of bits (referred to as *challenges*) as input and produce a sequence of bits (known as *responses*) as output, with the property that no two chips generate identical responses to a specific challenge. The pairing of a challenge with its corresponding response is known as a challenge-response pair (CRP). For a PUF implementation to be effective, it must exhibit characteristics such as uniqueness, reliability (over time and environmental changes), and uniformity (random response). One such option is the Static Random Access Memory (SRAM) PUF, which leverages the behavior of standard SRAM memory available in digital chips. Another variant is the OPUFs, wherein challenges and responses are derived from the distinctive properties of optical components. In the proposed architecture, we explore two OPUF implementations: one exploiting the speckle patterns when a coherent light beam propagates through the random optical medium [14], and another based on the Rayleigh backscattering pattern (RBP) of an optical fiber [15].

2.3. Encryption Technologies

Although the proposed security architecture also considers conventional cryptography, the novelty lies in PLS. The concept of PLS within telecommunication systems is based on encrypting information at the lowest layer of the transmission system, i.e. the physical layer, or in the context of this study, the optical layer. PLS supplements and enhances conventional cryptography employed at higher layers. In contrast to higher layer cryptographic schemes, PLS exploits physical transmission characteristics such as the channel, modulations, and other unique transceiver attributes. The architecture explores two approaches: Light Path SECurity (LPSec) encryption [16], [17], and steganography.

LPSec requires extending coherent transponders with optical encryption and decryption blocks, as well as incorporating key management functionalities. Additionally, cryptographic blocks must operate at line speeds without introducing significant delays to data transmission, for which key expansion techniques are commonly used.

In contrast to bit substitution algorithms used to encode sensitive data, steganography focuses on covert communication by concealing the existence of the message. The architecture considers two steganography implementations: digital [18] and all-optical [19]. These approaches differ in their impact on security, complexity, cost, HW requirements, and network constraints.

3. Design of an Innovative Security Plane Architecture

The architecture of the security plane typically consists of three layers: 1) the physical layer; 2) the key management (or KMS) layer; and 3) the application layer.

The physical layer includes all HW, SW, and firmware components, along with the links facilitating the generation, distribution of keys, and authentication of network entities through optical signals. The physical layer also includes the components used for transmitting/receiving different optical signals allocated in different wavelengths (DWDM), the optical switching devices, e.g. ROADM, etc.

The KMS layer is responsible for tasks such as key generation, key storage, key distribution (transport) and key delivery. The goal of this layer is to improve the quality and usability of keys generated by the QKD modules. Some QKD modules can also provide basic key management functionality by themselves. However, additional components or protocols may be needed to enhance the performance of the key management layer, and therefore this proprietary basic functionality is not considered as part of the KMS layer in the frame of this work, where the aim is to develop agnostic KMS capable of interoperating with multi-vendor, multiprotocol QKD technologies, as well as other security technologies such as PUF. The KMS plays an important role in the security plane architecture as they receive keys from physical layer modules (such as QKDs or Quantum Random Key Generations (QRNGs)), manage them, and distribute them to key application consumers upon request. Additionally, a KMS is entrusted with ensuring the security and availability of keys used for encrypting and decrypting sensitive data. It can enforce policies and procedures for key usage, including expiration dates, access control, and auditing. Concerning the distribution of keys from the KMS to the application layer, there are currently two standardized key delivery APIs: ETSI GS QKD 004 [20] and 014 [21]. The KMS also registers incoming applications and their Quality of Service (QoS) and monitors the real demands of each of them. It also exposes the parameters needed to monitor the key utilization per link. This information allows optimizing the planning of the QKD network [22].

Finally, the application layer encompasses applications that require keys to deliver security services throughout the network, providing confidentiality, authentication, and integrity. Examples of applications within this layer include

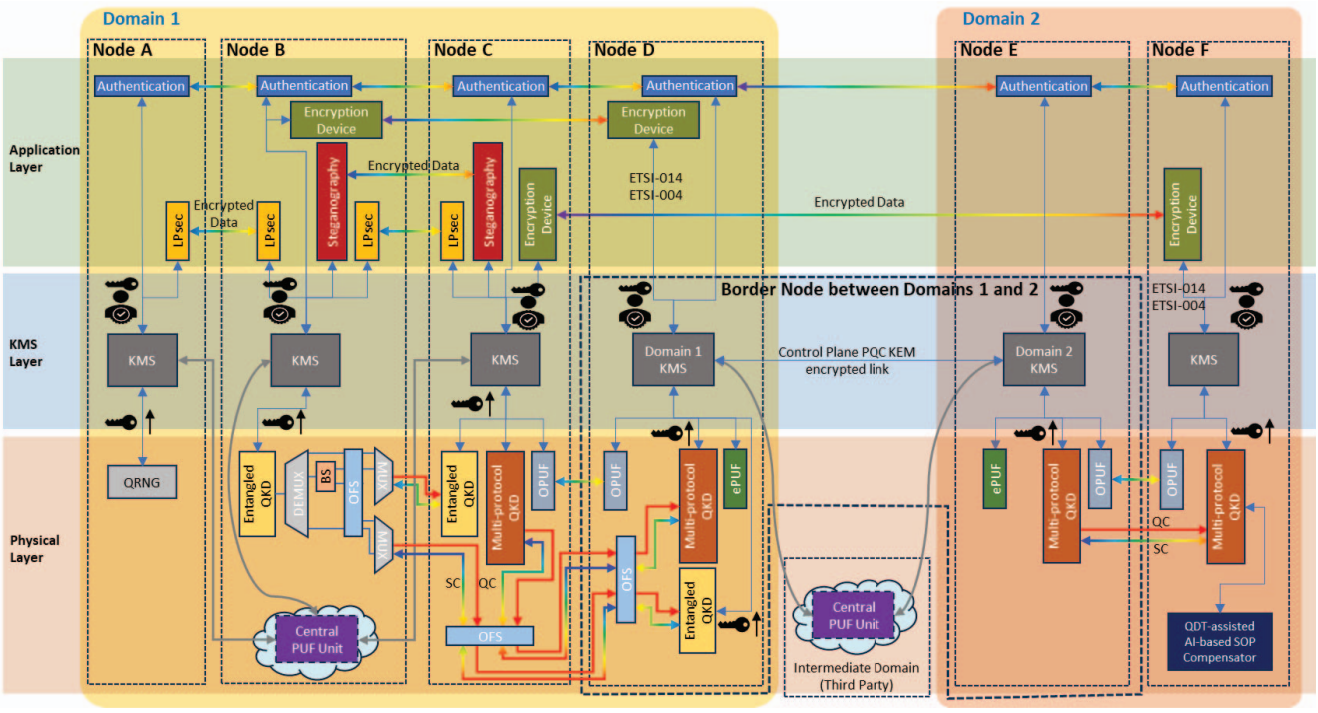

Figure 1: General overview of the proposed security plane architecture.

HW-based encryptors (such as OTN encryptors, MacSec, IPsec, LPsec, etc.), Hardware-Security Modules (HSMs) designed for secure key storage, authentication devices, and, more broadly, any application needing keys.

Figure 1 provides a comprehensive overview of the security plane architecture proposed in this work. In the physical layer, our focus is on QKD modules used for key generation and secure quantum key distribution. Each QKD module can be either CV-QKD or DV-QKD, with these technologies differing in the implemented encoding scheme, implementation complexity, tolerance to channel attenuation, and application scope. Alternatively, entangled QKD can be employed, particularly beneficial for P2MP applications. E.g., in Node B, the QKD module leverages on a broadband entangled photon source, capable of generating entangled photons in different frequencies, which can be transmitted to QKD modules located in several nodes (e.g. Nodes C and D in the figure). The use of beam splitters (BSs) enables sharing QC in a given frequency among different users, this being particularly interesting in scenarios involving access networks, where technology-deployment cost reduction is of paramount importance. In P2MP security scenarios, the integration of optical components, such as (de-)multiplexers, BSs, and optical fiber switches (OFS) provides the flexibility required to implement a programmable QKD network. Key generation and distribution are not exclusive to QKD systems; QRNG modules are also proposed as alternative entropy sources (e.g., Node A). The generated keys are securely distributed to Node A's counterpart (Node B) through a dedicated secure interface between KMSs. Moreover, authentication services are performed by means of PUF, which in this architecture will be mainly implemented as centralised PUF formations. Decentralised electronic Physically Unclonable Function (ePUF) modules are also considered as backup. The PUF module can take the form of either an ePUF, such as an SRAM-based PUF, or the speckle-pattern-based optical PUF (OPUF). Centralised PUF, together with the implementation of a procedure to securely exchange keys between KMS based on ETSI-014 and PQC, is proposed for relaying keys in border nodes. Finally, in node F, we represent an AI-based State of Polarization (SOP) compensator capable of optimising QKD systems by adjusting the tuneable parameters of the optical components to improve on the key distribution. This requires an interface with a quantum digital twin in the control plane, capable of providing the intelligence required to carry out that optimisation. Within the KMS layer, KMS units demonstrate the capability to interoperate with various QKD technologies and protocols (CV-QKD, DV-QKD, and entanglement-based QKD), along with other security technologies, such as PUF. These KMS units receive keys from QKD, QRNG and PUF modules, subsequently distributing them to key application consumers upon request. Finally, the application layer integrates application modules requiring keys to perform the encryption and authentication functions, which they retrieve from the KMS layer. This architecture contemplates the utilization of conventional encryptors executing standard protocols like TLS. However, it also focuses on innovative encryption modules such as those based on LPSec, implementing two nested ciphers ensuring a high-

security level. Authentication services (mainly based on PUF) facilitate the authentication of each node within the network.

The security plane architecture integrates notable advancements leveraging on cutting-edge technologies such as optical fingerprinting based on Rayleigh backscattering, indicated in the figure as OPUF between nodes C-D and E-F; multiprotocol QKD systems, and steganography applications as an encryption technique. These technologies, contingent upon their maturity level and their potential impact on existing networks, can be classified as disruptive. In the realm of multi-protocol QKD, having a QKD device with versatile protocol options provides an advantage in adapting to different users with varying QKD protocols, without the requirement for HW changes. This feature is especially important for applications such as satellite QKD, where access to the HW is difficult, making it impractical to reconfigure equipment for each specific protocol demand, as well as for trusted-node implementations.

4. Conclusions

The security plane architecture proposed in this work encompasses three layers, integrating various enabling technologies to address network security challenges. At the physical layer, multi-protocol QKD offers secure key generation and distribution, as well as flexibility in adapting to different user requirements, leveraging on AI-based SOP compensation for QKD performance optimization. Both DV-QKD and CV-QKD are inherently designed for P2P communication, while entangled-based QKD is proposed for P2MP scenarios. Additionally, QRNG modules provide an alternative entropy source for key generation. Authentication services are performed by PUF modules, mainly in centralized formations, supplemented by decentralized ePUF modules as a backup. These centralized PUF modules may take the form of SRAM-based PUF or OPUF, using speckle pattern or RBP approaches. Centralised PUF, together with the implementation of a procedure to securely exchange keys between KMSs based on ETSI-014 and PQC, is proposed for relaying keys in border nodes. At the KMS layer, KMS units demonstrate interoperability with various QKD technologies and protocols, along with other security technologies like PUFs. Finally, the application layer incorporates traditional upper layer encryptors alongside PLS using LPSec, complemented by cutting-edge technologies such as steganography. These advancements represent disruptive technologies that will have a significant impact on existing networks, offering adaptability and robust security tailored to evolving network landscapes.

Acknowledgments

This paper has received EU funding under grant agreement ALLEGRO No. 101092766.

References

[1] ALLEGRO project website: https://www.allegro-he.eu/

[2] P. Mehdizadeh et al., "Quantum-Classical Coexistence in Multi-Band Optical Networks: A Noise Analysis of QKD," in IEEE Communications Letters, vol. 28, no. 3, pp. 488-492, March 2024.

[3] J. P. Fernández-Palacios et al., "A Multi-technology/Multi-domain QKD Deployment over a Telco Production Network: Practical Issues and Outcomes," Optica Advanced Photonics Congress 2022, paper NeTh2C.4.

[4] C.H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science," (2014).

[5] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle security and implementations," Entropy, vol. 17, no. 9, pp. 6072-6092, 2015.

[6] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem, Phys. Rev. Lett. 68, 557-559 (1992).

[7] R. Wang et al., "A Dynamic Multi-Protocol Entanglement Distribution Quantum Network," 2022 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 2022, pp. 1-3.

[8] R. Wang et al., "AI-Enabled Large-Scale Entanglement Distribution Quantum Networks," 2021 Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA, USA, 2021, pp. 1-3.

[9] M. Svaluto Moreolo, Masab Iqbal, Laia Nadal, R. Muñoz, "Efficient solutions for quantum secure communications in future optical networks," (Invited), ICTON 2023, Bucharest, July 2-6, 2023.

[10] VPIphotonics (https://www.vpiphotonics.com/index.php).

[11] M. Iqbal et al, "SDN-Enabled Continuous-Variable QKD in Coexistence with 8×200 Gb/s 16-QAM Classical Channels," ONDM 2024, 6-9 May 2024, Madrid, Spain.

[12] M. Svaluto Moreolo, M. Iqbal, A. Villegas, L. Nadal, R. Casellas, R. Muñoz, "Continuous-Variable Quantum Key Distribution for Enabling Sustainable Secure 6G Networks," ONDM 2024, 6-9 May 2024, Madrid, Spain.

[13] A. Grebenchukov et al., "Prospects of Chip-Based Multi-Protocol Quantum Key Distribution Transceivers", 23rd International Conference on Transparent Optical Networks, ICTON 2023.

[14] M. Akriotou, A. Fragkos, D. Syvridis. Photonic physical unclonable functions: From the concept to fully functional device operating in the field, Proceedings of SPIE - The International Society for Optical Engineering (2020).

[15] P. Nadimi Goki, S. Civelli, E. Parente, R. Caldelli, T. Teferi Mulugeta, N. Sambo, M. Secondini, and L. Potì, "Optical identification using physical unclonable functions," in Journal of Optical Communications and Networking, vol. 15, no. 10, pp. E63-E73, October 2023.

[16] M. Iqbal, L. Velasco, N. Costa, A. Napoli, J. Pedro, and M. Ruiz, "LPsec: A Fast and Secure Cryptographic System for Optical Connections," IEEE/OPTICA Journal of Optical Communications and Networking (JOCN), vol. 14, pp. 278-288, 2022.

[17] T. Nikas, E. Rousas, M. Mylonakis, G. Pekridis, S. Karabetsos, A. Mandilara, D. Syvridis, "Physical layer security based on scrambling of the telecommunication system parameters driven by a quantum key distribution system," Next-Generation Optical Communication: Components, Sub-Systems, and Systems XIII, vol 12894, 2024.

[18] E. Wohlgemuth et al., "A Field Trial of Multi-Homodyne Coherent Detection Over Multi-Core Fiber for Encryption and Steganography," in Journal of Lightwave Technology, 41 (9), pp. 2723-2735, 2023.

[19] E. Wohlgemuth , Y. Yoffe , P. Nadimi Goki, M. Imran, F. Fresi, L. Potì, and D. Sadot, "Demonstration of Stealthy and Encrypted Optical Transmission Below Adjacent 50 GHz DWDM Channels," in IEEE Photonics Technology Letters, 32 (10), pp. 581-584, 2020.

[20] ETSI GS QKD 004, "Quantum Key Distribution (QKD); Application Interface", V2.1.1 (2020-08).

[21] ETSI GS QKD 014, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API", V1.1.1 (2019-02).

[22] ETSI GS QKD 015, Quantum Key Distribution (QKD); Control Interface for Software Defined Networks, V2.1.1 (2022-04).