Journal of Electronic Research and Application, 2025, Volume 9, Issue 5
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Quantum-Secure OTN Framework Integrating QKD-PQC Technologies

Wenliang Zhang[1,2], Jiao Zhao[2]*, Bao Tang[2]*, Wei Huang[1,2], Binbin Xu[1,2], Miao Li[1,2], Linfeng Wang[1,2], Bo Liu[1,2], Gongchong Zhong[1,2]

[1]Xintong Digital Intelligence Quantum Technology Co., Ltd., Beijing 100176, China
[2]CAS Quantum Network Co., Ltd., Shanghai 201315, China

**Authors to whom correspondence should be addressed.*

Abstract: The Optical Transport Network (OTN) is a protocol for sending network messaging over optical fiber networks. Intelligent optical networks provide an ideal solution for high-bandwidth services. Currently, data encryption schemes for OTN typically rely on mathematical problems such as elliptic curve cryptography or discrete logarithms, which are vulnerable to attacks by quantum computers. This paper investigates a quantum-secure OTN Framework that integrates Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) technologies, enabling OTN leased lines to resist quantum attacks. This framework can provide users with highly secure quantum-encrypted OTN leased lines services.

Keywords: OTN leased lines; QKD; Quantum key; Quantum Security Service Platform

Online publication: October 17, 2025

1. Introduction

The Optical Transport Network (OTN) is a transport network that implements the transmission, multiplexing, routing, and monitoring of service signals within the optical domain. It ensures the performance and survivability of service signals [1]. The high-quality OTN-based leased lines have become a key area of competition among operators due to their large capacity, long distance, low latency, and high availability [2].

Currently, operator-provided OTN leased lines typically employ non-encrypted transmission. To meet the practical requirements of enterprises for secure communications, OTN supports encryption technologies to mitigate the risks of data leakage and theft.

Traditional encryption solutions are utilized for achieving customer data protection, including elliptic curve cryptography, large-number factorization mathematical models, and AES block cipher algorithms based on public-key negotiation are employed to encrypt Optical Channel Payload Unit (OPUk) payloads between OTN devices (**Figure 1**).

However, these encryption assumptions are vulnerable to quantum computing threats and incapable of resisting quantum computational attacks using quantum algorithms such as Shor's and Grover's algorithms [3]. With the rapid advancement of quantum computing, addressing threats posed by quantum computational attacks has become an urgent necessity for business applications in highly secure industries, including government affairs, finance, electricity, and data centers.

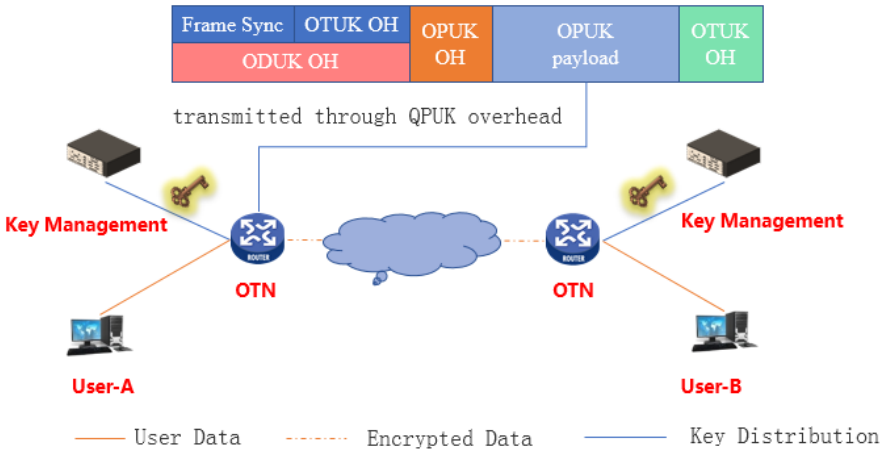

Figure 1. Quantum-secure communication between OTN equipment

To defend against threats posed by quantum computing, two main approaches have gained international recognition: Quantum Key Distribution (QKD), which leverages the principles of quantum physics, and Post-Quantum Cryptography (PQC), which is based on computational complexity.

QKD refers to the method and process by which two communicating parties generate and distribute cryptographic keys with information-theoretic security through the transmission of quantum states. Its security is guaranteed by fundamental principles of quantum mechanics, notably the indivisibility of single photons and the no-cloning theorem of quantum states [4]. In parallel, software systems and protocol standards supporting QKD have been developed. For example, the Chinese standard YD/T 4303-2023 specifies technical protocols, functional performance requirements, and testing methods for quantum-secure communication gateway and terminal devices based on the IPsec protocol [5].

Another quantum-resistant security technique is Post-Quantum Cryptography (PQC). It builds on well-studied hardness assumptions in mathematics, including lattice-based, code-based, and multivariate polynomial cryptography. These hardness assumptions are widely believed to remain computationally infeasible even for the quantum computer. PQC is mandated by the U.S. National Security Agency (NSA) in its Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) [6]. The U.S. National Institute of Standards and Technology (NIST) has forecasted that quantum computers may pose a realistic threat to existing classical encryption algorithms as early as 2030 [7].

This paper presents a quantum-secure OTN Framework that merges PQC for initialization and QKD for encrypted transmission.

(1) Initialization phase (PQC-based): Legacy OTN devices are provisioned with initial keys using Post Quantum Cryptography (PQC) algorithms. This scheme enables secure device onboarding, authentication, authorization, and quantum key injection.

(2) Encrypted transmission phase (QKD-based): QKD technology is used to establish quantum-secure OTN transmission leased lines. By interfacing with the QKD network, OTN devices can securely and cost-effectively obtain quantum-generated keys. These keys are then used in symmetric encryption algorithms to encrypt the payloads of OPUk. This approach enables OTN leased lines to be resistant to quantum attacks.

2. Challenges on the quantum-secure OTN framework

2.1. Unified interface definition

Traditional OTN equipment manufacturers often use proprietary protocols in OTN networking, resulting in interoperability challenges across devices from different manufacturers. Hardware products from different manufacturers may also vary in their implementation. The key to this technical solution is addressing how to adapt to heterogeneous OTN equipment models, standardize interface types, and unify transmission protocols to enable secure and reliable quantum key distribution across diverse OTN infrastructures.

2.2. Quantum key distribution integrating QKD-PQC

QKD networks offer a secure solution for key distribution between cities. However, within urban areas—such as between an OTN aggregation point and a nearby OTN terminal—deploying a full QKD network for key distribution poses challenges in terms of cost-efficiency and operational convenience. The core challenge for the feasibility of this technical solution lies in how to distribute quantum keys to OTN devices securely and economically, while establishing end-to-end encrypted OTN leased lines. Integrating QKD and PQC technologies plays a crucial role in addressing the "last mile" problem in quantum key delivery and accelerating the large-scale commercialization of quantum-secure communication technologies [8].

3. Methods

3.1. Architecture of quantum-secure OTN framework

Figure 2 shows the overall network architecture, which is divided into three layers: the quantum layer, the key management layer, and the service layer.

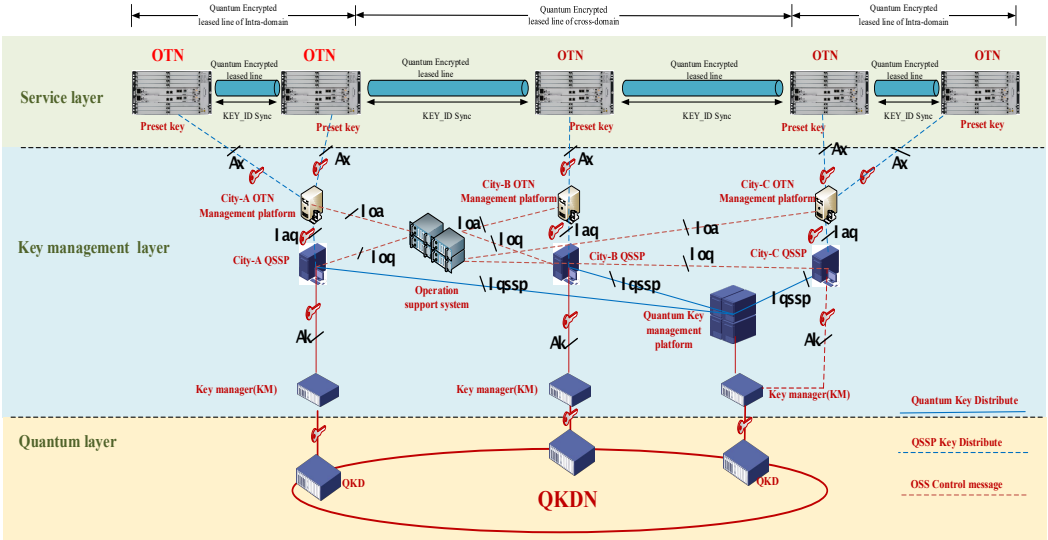

Figure 2. Architecture of quantum-secure OTN framework

3.1.1. Quantum layer

This layer leverages an integrated ground-satellite quantum key distribution (QKD) network to facilitate quantum key agreement and distribution between OTN devices across city-level, provincial, and cross-provincial domains.

3.1.2. Key management layer

This layer is organized into two levels—provincial and municipal (**Table 1**).

Table 1. Levels of key management layer

Locations	Platform	Shortcuts
Provinces	Operation support system	Responsible for user accounts opening, management, etc., and distribute control information to the OTN management platform and the QSSP.
Provinces	Quantum key management platform	Manage the QSSP of each city, and synchronize quantum keys among the QSSP through QKDN.
Cities	QSSP	Distribute quantum keys among OTN equipment through the OTN management platform.
Cities	OTN management platform	Management authentication and authentication for OTN equipment in each city, distribute quantum keys from the QSSP to OTN equipment.

3.1.3. Service layer

OTN-CPE devices are deployed at the user end. User-side OTN devices obtain quantum session keys through the municipal-level quantum security service platform. During the initialization phase, PQC algorithms are employed to securely inject pre-distributed quantum keys into the secure cryptographic modules of the OTN devices via the municipal platform. During the secure communication phase, the OTN devices establish quantum-encrypted leased lines using quantum session keys distributed by the QKD network.

3.2. Unified interface

The unified interface is defined as follows (**Table 2**).

Table 2. Unified interfaces

NUM	Interfaces	Shortcuts
1	AK	Reference point between the APP and the KSA of the QKDN, whose main functions include key request and provision between the APP and the KM, etc. [9]
2	Iqssp	Reference point between the QSSP and the OTN management platform. Be responsible for the operation maintenance, authentication, and authorization, distributed quantum keys from the QSSP to OTN equipment.
3	Ioq	Reference point between the operation management platform and the QSSP, provides authentication, and the management of encrypted services, such as leased lines establishment and deletion, etc.
4	Ioa	Reference point between the operation management platform and the OTN management platform. provides authentication and management of encrypted services, such as establishment, deletion, and billing, etc.
5	Iaq	Reference point between the OTN management platform and the QSSP, and the logical interface between the OTN CPE and the QSSP. Provide authentication management and distribution of quantum keys, etc.
6	Ax	Reference point between the OTN equipment and the OTN management platform. Exchange information between OTN equipment based on the specific protocol of the OTN manufacturer.

3.3. Methods of the initialization of OTN CPE

The initialization of OTN CPE mainly includes authentication and authorization between OTN equipment and municipal quantum security service platforms, as well as the injection of quantum keys into OTN CPE. The transmission protocol from the provincial OTN management platform to the OTN equipment of the user layer is private for each equipment manufacturer (**Figure 3**).

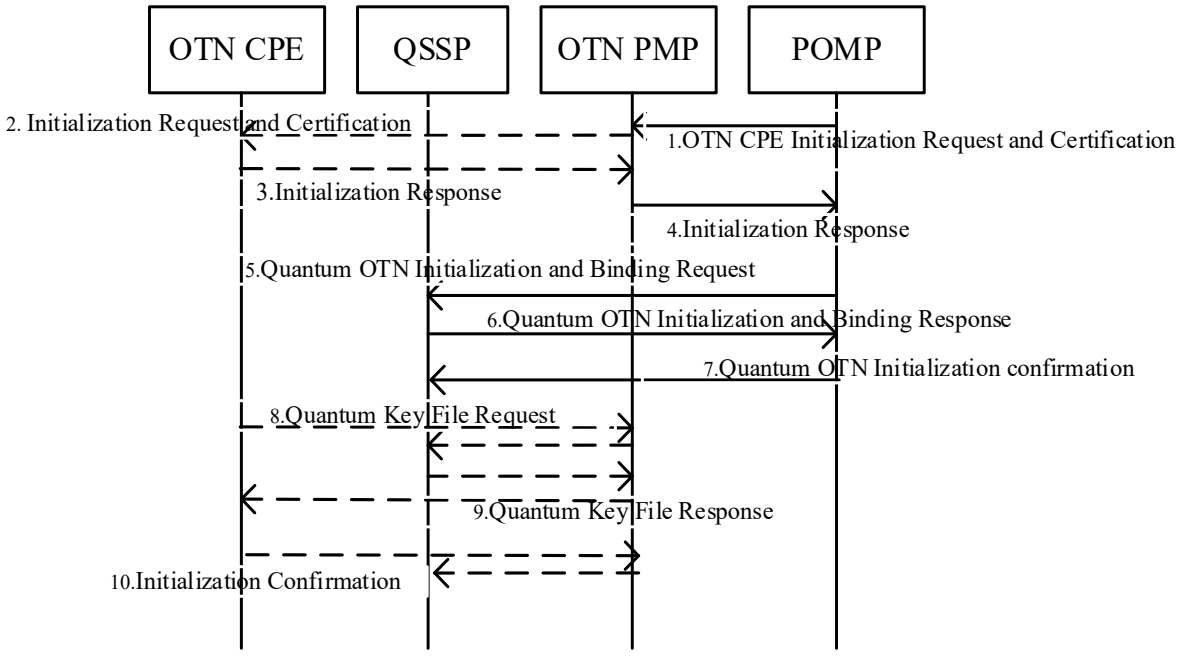

Figure 3. Initialization process of OTN CPE

(1) The provincial operation management platform (POMP) initiates the message "OTN CPE Initialization Request and Certification" to the OTN provincial management platform (OTN PMP). This message carries the unique identifier of the OTN CPE, which requires quantum encryption.

(2) The OTN PMP forwards the message "Initialization Request and Certification" to the OTN CPE according to the unique identifier.

(3) The OTN CPE replies with the message "Initialization Response" to the OTN PMP, and completes authentication and registration within the OTN PMP.

(4) The OTN PMP forwards the "OTN CPE Initialization Response" to complete authentication and registration within the POMP.

(5) The POMP initiates the message "Quantum OTN Initialization and Binding Request" to QSSP, carrying the OTN CPE identification information required for quantum encryption. QSSP prepares the quantum key file if it receives the message successfully.

(6) The municipal QSSP responds to the POMP with a message "Quantum OTN Initialization and Binding Response," when OTN CPE identity authentication and OTN CPE binding is finished.

(7) The POMP responds to QSSP with "Quantum OTN Initialization confirmation," and records the results of identity authentication and binding.

(8) The OTN CPE initiates a "Quantum Key File Request" to the municipal QSSP, which is forwarded by the OTN PMP, carrying the unique identifier of the OTN CPE.

(9) The municipal QSSP responds to the OTN CPE with "Quantum Key File Response," which is forwarded by the OTN PMP.

(10) The OTN CPE initiates a message "Initialization Confirmation" to the municipal QSSP, which is forwarded by the OTN PMP, carrying the Initialization results.

3.4. Method of quantum OTN leased line

The establishment of a quantum OTN leased line primarily involves mutual identity authentication, service authentication, and confirmation between the OTN equipment and the OTN PMP, POMP, and municipal QSSP. The two QSSPs can synchronize relevant business information and obtain quantum session keys from the QKD network. The quantum session keys are encrypted and distributed to two OTN CPEs, which require quantum encryption through the OTN PMP. The transmission protocol from the OTN PMP to the OTN equipment of the user layer is private for each equipment manufacturer (**Figure 4**).

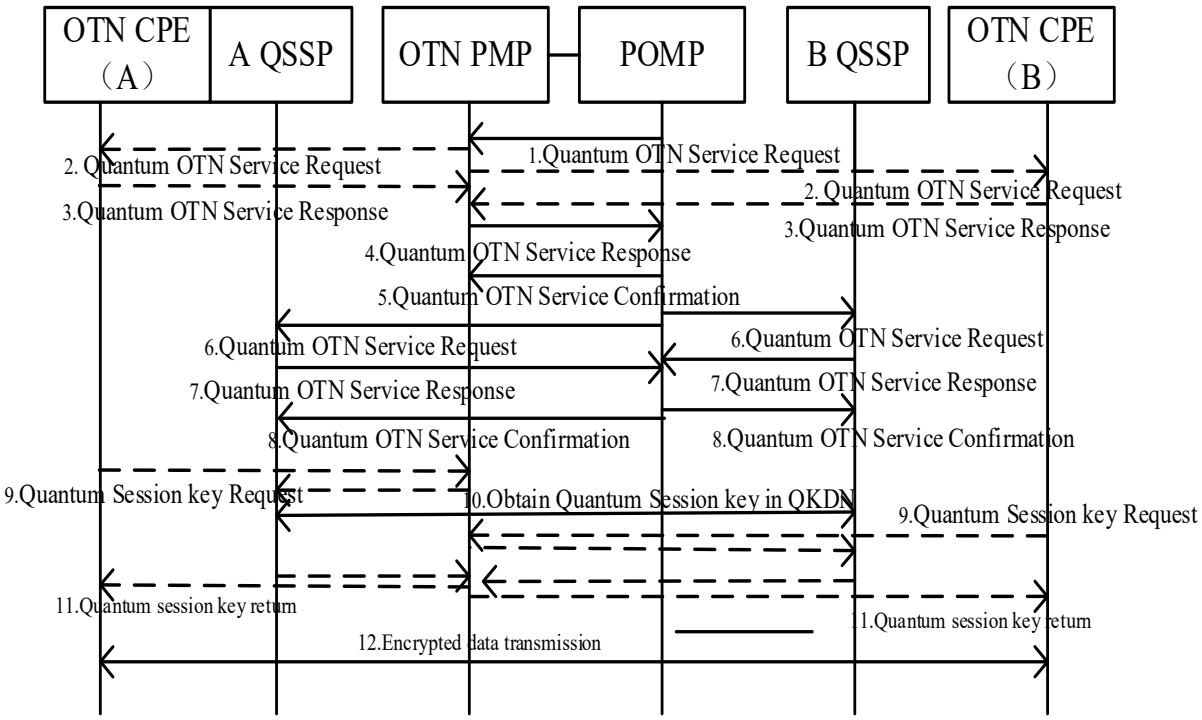

Figure 4. Quantum OTN dedicated line establishment

(1) The POMP initiates the message "Quantum OTN Service Request," with QOS and authentication information to the OTN PMP, carrying the unique identifier of two OTN CPEs to establish a quantum OTN dedicated line.

(2) The OTN PMP forwards the "Quantum OTN Service Request" message to the OTN CPEs at both ends, notifying both OTN CPEs ready for service.

(3) The OTN CPE replies with the message "Quantum OTN Service Response" to the OTN PMP and completes the identity authentication process.

(4) The OTN PMP forwards the message "Quantum OTN Service Response" to the POMP, and completes the identity authentication of the OTN CPE to the POMP.

(5) The POMP initiates the "Quantum OTN Service Confirmation" message to the OTN PMP, verifies the

QOS information, and the Token information corresponding to the OTN CPEs.

(6) The POMP initiates the message "Quantum OTN Service Request" to the municipal QSSP, which the OTN CPE belongs to.

(7) The municipal QSSP replies with the message "Quantum OTN Service Response" to the OTN PMP and completes the identity authentication process.

(8) The POMP returns "Quantum OTN Service Confirmation" message to the municipal QSSP, and completes bidirectional quantum OTN service authentication and confirmation.

(9) The OTN CPE (A) initiates the message "Quantum Session key Request" to the home QSSP, which is forwarded by the OTN PMP.

(10) After the identity authentication is performed by the municipal QSSP, relevant management information is synchronized between the two QSSPs, and quantum session keys are obtained from the QKD network.

(11) The QSSP distributes the quantum session keys, which are encrypted to two OTN CPEs, and this distribution is forwarded by the OTN PMP.

(12) After obtaining the quantum session keys, the OTN CPE encrypts and transmits the OPUk payload using the quantum session keys..

4. Retrospect and prospects

This paper presents a Quantum-Secure OTN Framework integrating QKD-PQC technology, enabling OTN devices to obtain quantum keys from the QKD network safely and at low cost. Then, quantum keys are used to encrypt the payload of OTN OPUk frames, making the OTN secure communication achieve the security capability of resisting quantum attacks. On the one hand, the unfiled interface definitions have been unified to address the issue of interface types and transmission protocol adaptation for different models of OTN devices from various manufacturers. On the other hand, by integrating QKD and PQC technologies, it simplifies the processes of key issuance and subsequent usage and management, breaks through the "last mile" problem of key transmission, and thus promotes the implementation of the OTN quantum encryption technology solution.

One of the practical goals of quantum encryption technology is to achieve large-scale commercial deployment. Therefore, by leveraging the existing classic OTN optical fiber network infrastructure, co-fiber transmission of OKD and classic signals is an important approach to achieving large-scale deployment of OKD. Due to the weak strength and susceptibility of quantum signals, as well as the single function of the OTN terminal equipment on the user side. The co-fiber transmission technology of QKD and OTN still faces challenges. Research on the co-fiber transmission technology of QKD and OTN networks needs to be continued [10].

Funding

National Development and Reform Commission (NDRC) New-Generation Information Infrastructure Construction Project: National Wide-Area Quantum Secure Communication Backbone Network Construction Project (0747-2260SCCSHV90(001))

Disclosure statement

The authors declare no conflict of interest.

References

[1] Fang C, 2012, Research on Key Technologies of Optical Transport Network (OTN), dissertation, Beijing University of Posts and Telecommunications.

[2] Zang Y, Yin Z, Wang L, 2023, Discussion on Interoperability Application of OTN-CPE Multi-Vendors. Telecommunications Design Technology, 2023(4).

[3] Shor PW, 1999, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Sci. Statist. Comput.

[4] Tang B, Ying J, Li J, 2025, The Technology and Networking Strategy of the Quantum Secure Communication Bearer Network with Space-Integrated-Ground. Communications Technology, 58(3): 232–240.

[5] YD/T 4303-2023 Technical Specifications for Quantum Secure Communication Application Equipment Based on IPsec Protocol, 2023, https://www.chinesestandard.net/PDF/English.aspx/YDT4303-2023

[6] National Security Agency, 2022, Announcing the Commercial National Security Algorithms.

[7] Chen L, Jordan S, Moody D, et al., 2016, Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

[8] Wang LJ, Zhang KY, 2020, Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography. arXiv. https://arxiv.org/abs/2009.04662

[9] YDT 4301-2023 Quantum Secure Communication Network Architecture, 2023, https://www.gb-gbt.com/PDF/Related.aspx/YDT4301-2023

[10] Gong J, 2022, Research on Quantum Key Distribution System for Classical-Quantum Co-Fiber Transmission, dissertation, University of Science and Technology of China.