Quantum Internet Protocols

Chen Yang cheyan@wustl.edu
(A paper written under the guidance of Prof. Raj Jain) Download

Abstract

To address the fundamental threat posed by quantum computing to classical cryptographic systems and facilitate the transition of quantum key distribution (QKD) from experimental validation to industrial deployment, this paper systematically examines the evolution of QKD technology from Wiesner's 1969 quantum money concept to current commercial implementations, with particular emphasis on recent breakthroughs in discrete variable and continuous variable approaches regarding protocol design, channel transmission, and system integration. The discussion emphasizes interoperability, scalability, and experimental demonstrations leading toward a global quantum internet.

Keywords: Quantum key distribution; Quantum communication networks; Continuous variable QKD; Discrete variable QKD; Quantum-secure communications; Quantum networking; Quantum internet; Entanglement swapping; Quantum routing

Table of Contents

- 0. Introduction
- 1. Technological Research and Industrialization Progress
  - 1.1 Progress in QKD Theoretical Research
  - 1.2 Current Status of QKD Industrialization
    - 1.2.1 Technological Breakthroughs
    - 1.2.2 Demonstration Application
    - 1.2.3 Standardization Trends
  - 1.3 QKDN Deployment Cases
- 2. Standardization Organizations and Standards Progress
  - 2.1 ITU-T Standardization Progress
  - 2.2 ETSI Standardization Progress
  - 2.3 ISO/IEC Standardization Progress
  - 2.4 IEEE Standardization Progress
- 3. QKD Networking Technology Challenges and Future Layout
- References

0. Introduction

The rapid development of quantum computing technology poses a fundamental threat to traditional asymmetric cryptographic systems based on computational complexity, and it is urgent to build a new generation of information security system that can resist quantum attacks [Ladd10]. Quantum

key distribution (QKD) technology utilizes the quantum no-cloning principle and measurement collapse characteristics to achieve information theoretical security of key distribution at the physical level, providing important security support for future communication infrastructure [Gisin07]. Although QKD has the potential to resist quantum computing attacks in principle, its actual promotion and application still faces multiple constraints such as transmission distance, key generation rate, equipment cost and system integration [Langer09].

In recent years, with the breakthroughs in key technologies such as thousand-kilometer-level optical fiber transmission, satellite quantum communication and dynamic quantum networks, QKD is moving from experimentation to initial large-scale application. In this process, standardization has become a key support for promoting technological maturity and industrial interconnection [Chen21]. At present, major international standardization organizations have actively deployed the development of QKD-related standards, forming a multi-level and multi-directional collaborative promotion pattern. Since 2008, the European Telecommunications Standards Institute (ETSI) has systematically promoted the standardization of QKD components, protocols and network architectures, and released the Information Security Skills Competition (ISG)-QKD series of standards [Bennett84].

The International Telecommunication Union (ITU-T) established the Joint Coordination Group for Quantum Key Distribution Networks (JCA-QKDN) in 2022, focusing on the security mechanism of the space-ground integrated quantum network [Dirac81]. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) is committed to building consistent security testing and evaluation standards, and its Subcommittee 27 (SC27) working group has carried out research on QKD security evaluation specifications [Heisenberg85]. In addition, the Institute of Electrical and Electronics Engineers (IEEE), the China Communications Standards Association (CCSA) and other organizations have also promoted the formulation of standards from the perspectives of classical-quantum signal co-transmission, protocol compatibility and industry applications, and jointly promoted the practical application and internationalization of QKD technology [Wootters82, Zhang21].

However, existing standards still fail to fully cover the interdisciplinary challenges and dynamic security issues faced by QKD systems in actual deployment, especially in areas such as device-independent (DI) QKD security authentication, network scaling mechanisms, and compatibility of hybrid quantum-classical protocols [Ekert91, Bennett92]. This paper aims to systematically analyze the current status and development trend of international QKD standardization, summarize the progress and shortcomings of existing standards in terms of technical requirements and security evaluation, and propose standardization paths and implementation suggestions suitable for large-scale quantum network applications for key issues such as QKD system interoperability, security verification system, and space-ground integrated integration, so as to help QKD technology move from demonstration applications to full-scale commercial deployment.

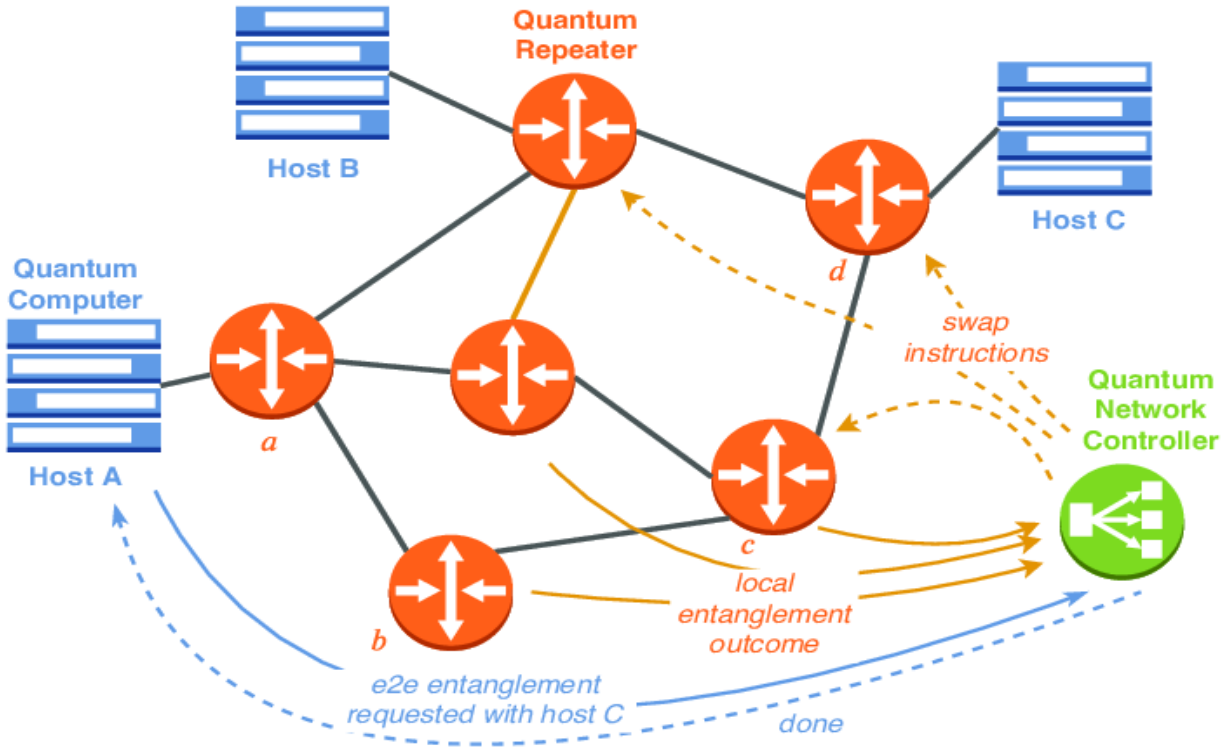


Figure 1: Quantum network architecture. The diagram shows the flow of entanglement requests, local entanglement outcomes, and swap instructions within the quantum network infrastructure [Cicconetti21].

1. Technological Research and Industrialization Progress

1.1 Progress in QKD Theoretical Research

As the core application of quantum cryptography, QKD achieves secure negotiation by transmitting randomly generated candidate keys—this process is only used to confirm the security of the key and does not involve the actual transmission of information. Its theoretical origin can be traced back to the revolutionary idea proposed by Wiesner in 1969: to construct unforgeable "quantum banknotes" using the properties of single quantum states. After nearly 20 years of silence, this pioneering idea made a breakthrough in 1984 through in-depth research by Bennett and Brassard. The two formally proposed the BB84 protocol based on the principle of quantum state information transmission, marking the establishment of the QKD technology paradigm [Bennett84].

The theoretical foundation of QKD is rooted in the basic principles of quantum mechanics, namely the Heisenberg uncertainty principle and the quantum no-cloning theorem. These principles guarantee the non-copyability of qubits; any eavesdropping will disturb the quantum state and thus be detected by both parties in the communication [Zhang21]. Since the BB84 protocol was proposed, the QKD protocol system has continued to evolve. In 1991, Ekert proposed the E91 protocol based on Einstein-Podolsky-Rosen (EPR) entangled particle pairs, whose security relies

on the Bell inequality test; in the same year, the Bennett team simplified the design and proposed the B92 protocol which only requires two non-orthogonal states.

With the development of technology, new generation protocols such as coherent state continuous variable (GG02) protocol, measurement device independent (MDI)-QKD protocol and twin-field (TF)-QKD protocol have emerged one after another. They not only have provable security in theory, but have also been verified in experiments [Lucamarini18, Wang19]. Building upon this foundation, QKD has gradually diverged into two main technical routes: discrete-variable (DV)-QKD and continuous-variable (CV)-QKD. The former uses single-photon or weakly coherent light as the signal source, transmitting bit information through polarization or phase encoding; the latter uses Gaussian modulation and demodulation based on the amplitude and phase of quantum states.

Representative DV-QKD protocols include BB84, E91, B92, MDI-QKD, and the recently developed TF-QKD, possessing high fault tolerance and long-distance transmission capabilities, but requiring high device performance and presenting significant system integration challenges. In contrast, CV-QKD, represented by the GG02 protocol, uses coherent states as the signal source, employing homodyne or heterodyne detectors to measure continuous variables, and performing security parameter analysis through covariance matrix estimation. CV-QKD is naturally compatible with classical optical communication systems and has advantages such as simple structure, high spectral efficiency and easy chip integration. In recent years, it has shown great potential for application in short-distance high-density networks and silicon photonics platforms [Zhang24].

In terms of specific implementation, early QKD systems relied on high-performance single-photon sources and single-photon detectors. Due to the maturity of devices, existing systems mostly use weak coherent light sources as substitutes, but such light sources will introduce security risks of photon number separation attacks. To this end, schemes such as decoy state protocol and measurement device-independent architecture have been proposed. By improving the system's anti-interference and anti-side channel attack capabilities, the practicality and deployment feasibility of QKD have been significantly enhanced.

QKD can be implemented through two channels: free space and optical fiber. Among them, optical fiber has become the mainstream carrier due to its wide coverage and low loss characteristics. To achieve co-fiber transmission of quantum signals and classical optical signals, wavelength division multiplexing and time division multiplexing technologies have been widely adopted: early experiments used the O-band (1260–1360 nm) to transmit quantum signals and the C-band (1530–1565 nm) to transmit classical signals; subsequent research has gradually developed a multi-channel multiplexing scheme in the C-band to improve spectral efficiency and alleviate transmission distance limitations [Bahrami20].

1.2 Current Status of QKD Industrialization

As QKD technology moves from theory to practical application, its industrialization process exhibits a development trend of integrated advancement through “scientific research breakthroughs—pilot deployments—ecosystem building.” Table 1 compiles representative quantum key distribution network (QKDN) cases worldwide.

Table 1. Typical QKDN Deployments and Performance Achievements

Time / Publisher	Protocol / Technology Type	Distance (km)	Key Rate	Features / Breakthroughs
2023 / Shanxi University, China	DV-QKD	80	2.11 Mb/s	Enhanced 16-APSK modulation
2023 / USTC Joint Team, China	DV-QKD	10	115.8 Mb/s	Single-channel world record
2023 / USTC, China	SNS-TF-QKD	1,002	0.0034 b/s	Broke PLOB limit, longest distance record
2023 / Beijing Quantum Institute, China	PMP-QKD	508	42.64 b/s	Simplified system design
2024 / Swiss Applied Physics Team	DV-QKD	10	64 Mb/s	Multi-channel superconducting detector readout
2021 / University of Padova, Italy	Integrated silicon photonics platform	0.145	30 kb/s	Free space, all-day testing
2023 / University of Geneva + IDQ, Switzerland	Silicon photonics platform	200.2	1.3 kb/s	Error control optimization
2023 / Cambridge University, UK	III–V materials + silicon hybrid integration	50	1.82 Mb/s	Bidirectional on-chip transmitter and receiver
2023 / Amazon Web Services, USA	CV-QKD	16	Not disclosed	Edge computing integrated VPN
2023 / China Telecom, China	DV-QKD	100.96	2.7 kb/s	Co-fiber transmission supporting 1 Tb/s data
2023 / IDQ, Switzerland	CV-QKD	Tens	Not disclosed	Collaboration with Nokia, Brussels data centers
2023 / LuxQuanta, Spain	CV-QKD	Metropolitan	Not disclosed	World's first CV-QKD system “NOVA LQ”
2024 / Swisscom + Quantum Optics Jena	Entanglement-based QKD	Not disclosed	Not disclosed	Entangled photon pair scheme in commercial network

2025 / France Telecom + Toshiba Europe	QKD + PQC hybrid	20–80	10–100 kb/s	Multi-layer defense-in-depth

1.2.1 Technological Breakthroughs

From core performance to engineering availability, the QKD protocol continues to make progress in theoretical optimization and system integration, driving the technology towards longer transmission distances and higher key generation rates. CV-QKD, with its advantage of high key generation rates over short distances, dominates metropolitan area quantum communication applications; DV-QKD, through continuous optimization of protocols and devices, continues to break through performance limits. Shanxi University [Tian23] used an improved 16-constellation point amplitude-phase joint keying (16-APSK) modulation to achieve a key rate of 2.11 Mb/s in an 80 km fiber optic link; the USTC joint team [Li23] based on the decoy state BB84 protocol set a world record of 115.8 Mb/s in a single channel in a 10 km fiber optic link; the Swiss Institute of Applied Physics [Hajomer24] used a multi-channel superconducting nanowire (SNS) single-photon detector (PD) array to achieve a key rate of 64 Mb/s at the same distance, marking that QKD technology is moving towards high bandwidth and long distance application scenarios. TF-QKD breaks through the limitations of point-to-point communication with its "dual-end preparation-central measurement" architecture. The USTC team [Liu23] adopted the SNS-TF-QKD protocol to achieve a key generation rate of 0.0034 b/s in a 1002 km fiber link. The Beijing Academy of Quantum Information Science [Zhou23] proposed an open phase matching protocol (PMP)-QKD architecture to achieve a key generation rate of 42.64 b/s in a 508 km fiber link, which significantly reduced the system complexity. As an important evolution direction of QKD system hardware, the integrated optical platform is gradually realizing the on-chip integration of core components such as modulators, light sources and detectors. In 2021, the University of Padua team in Italy [Avesani21] developed a free-space QKD transmitter chip with a wavelength of 1,550 nm based on an integrated silicon photonics platform, achieving a key rate of 30 kb/s in a 145 m free-space link all-day test; in 2023, the University of Geneva, together with the IDQ team [Sax23], constructed a high-speed QKD system based on silicon photonics chips, achieving a key rate of 1.3 kb/s in a 200.2 km optical fiber link, with the bit error rate controlled within 0.9%; in the same year, the University of Cambridge [Dolphin23] proposed a hybrid integrated QKD transceiver chip, which integrates a high-speed electro-optic modulator of III-V group materials with a silicon optical waveguide, achieving a key rate of 1.82 Mb/s in a 50 km optical fiber link, with a bit error rate of less than 1%, and a chip area of only 10 mm^2.

1.2.2 Demonstration Application

Industry-university-research collaboration drives implementation. On the basis of continuous improvement of key performance, global QKD systems have gradually entered the pilot deployment and industry verification stage. In 2023, the Amazon Quantum Network Center completed the deployment of a dual-node quantum secure network in Singapore, innovatively integrating QKD with Amazon Web Services (AWS) edge computing hardware to build a virtual private network (VPN) tunnel; the China Telecom team broke through the bottleneck of few-mode fiber (FMF) transmission, achieving 100.96 km FMF and classical optical communication co-fiber transmission, with a key generation rate of 2.7 kb/s under 1 Tb/s classical bandwidth [Dou23]. In

Europe, IDQ in Switzerland, together with Nokia, completed the quantum key distribution experiment between Brussels and Mechelen data centers; LuxQuanta in Spain launched the world's first commercial continuous variable QKD system "NOVA LQ" [IDQ23]. In 2024, Swisscom, the largest telecommunications operator in Switzerland, together with the German startup Quantum Optics Jena, completed the verification test of the QKD system based on entangled photon pairs in the existing fiber optic environment [Heise24]. The system generates entangled photon pairs to achieve stable key exchange in the Swisscom commercial network. Compared with traditional DV-QKD or CV-QKD, entangled QKD has a natural physical security advantage in terms of anti-eavesdropping ability. In 2025, French telecommunications operator Orange Business, together with Toshiba, officially launched the "Orange Quantum Defender" quantum security network service in Paris, marking the official launch of the first commercial QKD network in France [Toshiba25]. The system adopts the high key rate QKD technology developed by Toshiba and combines it with the post-quantum cryptography (PQC) algorithm to build a multi-layer defense-in-depth architecture, which has been connected to the core sites of several financial enterprises in France.

1.2.3 Standardization Trends

Building a sustainable development ecosystem, the QKD industry chain has formed a complete closed loop: "upstream core components—midstream equipment and network solutions—downstream industry applications." Upstream, with optical fibers, optical chips, and signal processors as the core, Chinese companies such as Fiberhome and Hengtong Optic-Electric have achieved independent control over key components such as optical fibers, optical cables, and sensors. Midstream focuses on QKD terminals and network deployment, with leading companies such as QuantumCTek deeply engaged in quantum terminal R&D, and emerging forces such as Kyushu Quantum driving breakthroughs in multi-node networking technology. Downstream applications cover high-security areas such as government affairs and finance, meeting graded security requirements through multi-protocol compatible design. Internationally, companies such as MagiQ in the US and IDQ in Switzerland continue to lead the technological iteration of quantum random number generators and quantum switches; Toshiba in Japan and SoftBank jointly built a quantum technology center; and SK Broadband in South Korea launched a dedicated line service integrating QKD and PQC. The global industry chain presents a trend of collaborative evolution from "technological breakthroughs—scenario verification—commercial implementation." As the practical application of QKD technology accelerates, standardization and cross-domain integration become crucial. Future technologies will focus on three main directions: first, improving long-distance transmission efficiency by optimizing the co-fiber transmission performance of quantum classical optical signals using wavelength division multiplexing (WDM) technology; second, deepening multi-protocol compatibility by promoting the integration of QKD with encryption systems such as PQC and IPSec; and third, improving the global standards system by leveraging the leading role of international organizations such as ITU-T and ETSI, and referencing cross-organizational coordination mechanisms such as JCA-QKDN, to promote international consensus on quantum networks in terms of architecture, interface protocols, interoperability, and performance evaluation.

1.3 QKDN Deployment Cases

Although point-to-point QKD has made significant progress, its large-scale application still relies on networked deployment. Since the TOWNSEND P team proposed a multi-user extension scheme based on passive optical networks in 1994, the construction of global QKDN has been continuously promoted: the first prototype of optical node quantum communication network was realized in 1997; in 2002, the quantum network led by the US Defense Advanced Research Projects Agency (DARPA) deployed a cross-agency 10-node system [Elliott02]; in 2008, the EU's Secure Communication Based on Quantum Cryptography (SECOQC) project integrated a multi-node trusted relay architecture in Vienna and completed long-distance networking verification [Peev09]; China has made significant achievements in this field - between 2016 and 2019, the "Micius" quantum science experimental satellite was successfully launched, and quantum secure communication trunk lines such as Beijing-Shanghai and Shanghai-Hangzhou were opened one after another. The Guangzhou-Foshan-Zhaoqing quantum communication demonstration network innovatively integrated high-precision time synchronization technology and became the first quantum communication backbone network in the Guangdong-Hong Kong-Macao Greater Bay Area. Meanwhile, many countries around the world are actively building QKD test platforms to verify their performance in real environments: the SwissQuantum network in Geneva, Switzerland [Stucki11], the Durban quantum network in South Africa [Mirza10], and the Cambridge quantum network in the UK [Yuan05] have achieved long-term stable operation and analysis through trusted relay technology; Japan and Europe have cooperated to build a transnational QKD test network in Tokyo [Sasaki11]; China's Wuhu metropolitan area quantum communication network [Xu09] and Beijing Netcom commercial fiber backbone quantum network have provided important verification scenarios for industry applications. With the breakthrough of quantum signal and classical optical signal co-fiber transmission technology, QKDN is gradually moving towards practical application. In 2017, China successfully achieved more than 2,000 km of quantum link connection in cities such as Beijing, Jinan, Hefei, and Shanghai. Many companies have launched dedicated QKD services based on this infrastructure, providing quantum encryption protection for key data of governments and enterprises. Related technical standards and testing methods are also being improved in sync, covering core processes such as key establishment, resource allocation, and trusted relay communication. Currently, global quantum communication networks are transitioning from the technology verification stage to a new era of deep integration with multiple industries. Leveraging policy support and abundant application scenarios, the quantum field is accelerating the construction of a fully independent and controllable industrial chain system, encompassing core components, key equipment, and network applications, providing an important practical paradigm for the development of global quantum-secure communication networks.

2. Standardization Organizations and Standards Progress

2.1 ITU-T Standardization Progress

To promote the deep integration of QKD technology with information and communication technology (ICT) networks, the ITU-T has established a multi-level, phased standardization mechanism. In 2019, the ITU-T established the Quantum Information Technology Networks Focus Group (FG-QIT4N), which clarified the key technological directions of QKD in wide-area networking and high-security scenarios, effectively promoting interdisciplinary and inter-

organizational collaborative research. Its results laid the foundation for the subsequent construction of the standards system. Currently, QKD standardization work is mainly promoted by ITU-T Study Groups 11 (SG11), 13 (SG13), and 17 (SG17), focusing on key areas such as protocol testing, network architecture, and security mechanisms. SG11 is responsible for the Q series recommendations, focusing on protocol design, interface definition, and interoperability testing, and has led the development of a series of QKDN interface standards, including Q.4160–Q.4164. SG13 systematically defined the overall architecture and functional model of QKDN through the Y series recommendations (such as Y.3800 "QKD Network Fundamentals" and Y.3801 "Functional Requirements"). SG17 promotes quantum security standardization through the X series recommendations, covering key technologies such as the security framework (X.1710), key combination methods, and quantum noise random number generator architecture (X.1702). To improve the efficiency of organizational collaboration in the standards development process, ITU-T launched JCA-QKDN in 2023 as a coordination hub between its internal research groups and external standards organizations (such as ETSI, ISO/IEC, and IEEE). Although JCA-QKDN does not directly formulate standards, it promotes resource sharing, progress synchronization, and standard alignment through institutionalized collaboration, effectively driving mutual recognition and consistency within the global QKDN standards system.

2.2 ETSI Standardization Progress

As a core organization for global information and communication technology standardization, ETSI effectively promotes rapid technological innovation through its unique "Industry Standard Group (ISG)" mechanism. ETSI brings together over 700 member organizations, including enterprises, universities, and research institutions. Its standard-setting process adheres to the principle of open consensus, and all results are publicly released in a free and open-source manner. To balance intellectual property protection and technology sharing, ETSI implements a strict intellectual property rights (IPR) policy, requiring core patents to be open to all members under fair, reasonable, and non-discriminatory conditions. To adapt to the need for simultaneous advancement of R&D and standardization in the ICT industry, ETSI innovatively established the ISG mechanism: a special working group can be established with the initiation of just four member organizations, and the standardization process can be quickly launched after signing relevant agreements. ISGs are open to all members and external partners, and participants are required to sign confidentiality agreements and comply with IPR management regulations. The final output of this mechanism is the "Group Specification (GS)," which, as an open standard, provides a unified technical specification framework for the global ICT industry. As the first industry standardization group within ETSI focusing on quantum communication standardization, ISG-QKD has established a technical standard system covering the entire industry chain. From basic documents (such as the "Glossary Group Specification" GS QKD 002 [ETSI10a]) to core technical specifications (such as the key extraction process GS QKD 004 [ETSI10b] and security protocol verification GS QKD 011 [ETSI16]), from security attack and defense analysis ("QKD Security Implementation White Paper") to device characteristic standardization (GS QKD 003 [ETSI18]), the group has released more than 20 GS specifications. Currently, ISG-QKD's work focuses on the standardization of extended interfaces that support the construction of large-scale quantum networks, including the key supply interface (GS QKD 014 [ETSI19]) and the network orchestration protocol (GS QKD 018 [ETSI22]), aiming to break through the technical bottleneck from laboratory verification to cross-domain large-scale networking. Through the efficient ISG

mechanism, ETSI has not only accelerated the process of QKD technology moving from theoretical research to practical application, but also provided a scalable and interoperable standard foundation for the construction of a global quantum communication network.

2.3 ISO/IEC Standardization Progress

Working Group WG3, SC27, "Security Assessment, Testing and Specification," under the Joint Technical Committee 1 (JTC1) of ISO/IEC, focuses on the security requirements analysis, testing methods, and assessment system construction of QKD systems. It is committed to optimizing the design security and implementation reliability of QKD devices and establishing a security verification mechanism for QKD modules. This working group leads the standardization work of quantum technology within the ISO/IEC framework, and has published two core standards to improve the security assessment and certification process for QKD systems. It is also responsible for developing and maintaining ISO/EN 15408, "General Guidelines for Security Assessment of Information Technology," providing standardized support for the security of QKD technology throughout its entire lifecycle, from R&D to deployment.

2.4 IEEE Standardization Progress

IEEE is advancing two key standards in the field of quantum communication standardization: The P1913 standard working group is dedicated to proposing a dynamic management framework based on the YANG model, supporting the flexible configuration, modification, and removal of quantum protocols and applications in communication networks. Its defined standardized interface for QKD modules can capture key parameters such as device transceiver rate and QKD protocol type in real time. However, it needs to address the risk of technological fragmentation in the co-evolution of classical communication and quantum technology, as well as interoperability conflicts caused by insufficient coordination across standards organizations. The other standard, P7130, focuses on defining quantum technology-specific terminology, improving consistency in technical understanding by building a unified conceptual system, and laying the foundation for interoperability of multi-vendor systems. Furthermore, the P1913 standard innovatively defines a "Software-Defined Quantum Communication (SDQC)" application layer protocol, which, based on the Transmission Control Protocol/Internet Protocol (TCP/IP) architecture, enables dynamic configuration of quantum endpoints, supports agile development and iteration of quantum protocols and application modules, and further expands the flexibility and scalability of quantum communication networks.

3. QKD Networking Technology Challenges and Future Layout

Currently, QKD networking faces two core challenges: First, network interoperability. This requires addressing the deep integration of QKD with existing fiber optic infrastructure, standardization of key transmission interfaces, and the integration of quantum keys with classical encryption protocols. ETSI is leading network layer technology research, promoting optimized co-fiber transmission of quantum signals and traditional optical communication systems. However, in practical deployments, issues such as insufficient equipment compatibility and fragmented key

negotiation mechanisms remain. For example, incompatibility between quantum switches from different manufacturers and classical router interface protocols necessitates the deployment of additional intermediate conversion equipment during networking, increasing system complexity and construction costs. Furthermore, the lack of unified standards for data interaction between QKD terminals and existing network management systems may lead to risks of key call delays or even failures. Second, network security authentication challenges. Although ITU-T SG17 has promoted QKDN security research, the end-to-end security authentication framework for multi-node dynamic networking scenarios still needs improvement. The security capabilities of QKD keys are continuously expanding, with applications extending from early point-to-point encryption at the link layer to more complex and diverse network environments, including cloud-edge collaboration, cross-domain connections, and dynamic key services for mobile users. In July 2025, the South Korean delegation submitted a draft technical report, "TR.QKDN-nqZTA," to ITU-T SG13, proposing a deep integration of QKDN with a zero-trust architecture based on trust enhancement mechanisms to build a quantum-secure network system for 6G. This aims to overcome the trust boundary limitations of traditional QKDN in complex networks and create a future network security architecture that supports dynamic authentication, scalable trust, and combinable services.

Looking towards the goal of a fully quantum internet beyond 2025, QKD networking needs to construct a new architecture that supports quantum computer interconnection and direct quantum information transmission. This requires overcoming the technical bottlenecks of quantum repeaters to achieve lossless transmission and efficient entanglement distribution of quantum states over long distances. Currently, quantum repeaters are limited by entanglement swapping efficiency and noise interference, with transmission distances generally below 100 kilometers. There is an urgent need to develop new repeater solutions based on superconducting quantum bits and photonic integrated chips. Simultaneously, hybrid networking standards compatible with classical network protocols should be developed, such as embedding the QKD key management protocol into the SDN architecture to achieve unified scheduling of quantum and classical network resources. Standardization of satellite quantum communication modules is also increasingly urgent, including performance parameters of optical ground stations (such as single-photon detection sensitivity and dark count rate) and satellite optical terminal interface protocols (such as encoding formats and modulation methods). For example, low-Earth orbit satellite networking needs to solve the key synchronization problem during dynamic switching of inter-satellite quantum channels, while high-Earth orbit satellite quantum repeaters need to overcome satellite-to-ground link delay compensation and Doppler frequency shift correction technologies. All of these require industry-academia-research collaboration to accelerate technology transfer and ecosystem building.

At the standardization strategy level, priority should be given to improving the fundamental standards system, including developing unified QKD equipment performance indicators (such as ITU-T Y.3827), key management protocols (such as the BB84-based key negotiation process), and network control interface standards (such as ETSI GS QKD 018 [ETSI22]). International organizations such as ETSI and ITU-T should strengthen cooperation to promote global consensus on key technologies such as quantum network architecture and key transmission efficiency optimization. For example, they could jointly develop the "Quantum Key Distribution Network Interoperability Framework," clarifying core specifications such as device access authentication

and key routing strategies. Simultaneously, a cross-platform interoperability testing framework should be established, and an automated testing toolchain should be developed, covering the entire process of quantum state preparation, transmission, and measurement, providing technical support for multi-vendor device access. The European OPENQKD project has built a multi-vendor QKD equipment testbed, verifying the interoperability of the BB84 and E91 protocols in metropolitan area networks. Such practices can provide important references for the standardization process. Future deployments should focus on the standardized construction of satellite quantum communication networks, with key breakthroughs in technologies such as low-Earth orbit satellite constellations and seamless switching of quantum signals between satellites and ground stations. For example, building a global quantum communication network by deploying a distributed low-Earth orbit satellite constellation requires addressing challenges such as optimizing satellite orbital parameters and rapidly establishing inter-satellite quantum links. Simultaneously, the standardization of a hybrid quantum-classical network architecture should be promoted to achieve dynamic bandwidth allocation between QKD and classical data transmission.

List of Acronyms

- APD — Avalanche Photodiode
- APSK — Amplitude and Phase Shift Keying
- AWS — Amazon Web Services
- BB84 — Bennett-Brassard 1984 Protocol
- B92 — Bennett 1992 Protocol
- CCSA — China Communications Standards Association
- CPRI — Common Public Radio Interface
- CV — Continuous Variable
- CV-QKD — Continuous Variable Quantum Key Distribution
- DI-QKD — Device-Independent Quantum Key Distribution
- DV — Discrete Variable
- DV-QKD — Discrete Variable Quantum Key Distribution
- DWDM — Dense Wavelength Division Multiplexing
- E91 — Ekert 1991 Protocol
- eCPRI — enhanced Common Public Radio Interface
- EPR — Einstein-Podolsky-Rosen
- ETSI — European Telecommunications Standards Institute
- FEC — Forward Error Correction
- GG02 — Grosshans-Grangier 2002 Protocol
- IDQ — ID Quantique
- IEC — International Electrotechnical Commission
- IEEE — Institute of Electrical and Electronics Engineers
- IETF — Internet Engineering Task Force
- IP — Internet Protocol
- IPsec — Internet Protocol Security
- ISO — International Organization for Standardization
- ISG — Industry Specification Group
- ITU — International Telecommunication Union
- ITU-T — ITU Telecommunication Standardization Sector

- JTC — Joint Technical Committee
- KMS — Key Management System
- LDPC — Low-Density Parity-Check
- MDI — Measurement-Device-Independent
- MDI-QKD — Measurement-Device-Independent Quantum Key Distribution
- NIST — National Institute of Standards and Technology
- OAM — Orbital Angular Momentum
- OLT — Optical Line Terminal
- ONU — Optical Network Unit
- OSI — Open Systems Interconnection
- PLOB — Pirandola-Laurenza-Ottaviani-Banchi (limit)
- PMP-QKD — Phase-Matching Protocol Quantum Key Distribution
- PON — Passive Optical Network
- PQC — Post-Quantum Cryptography
- QAM — Quadrature Amplitude Modulation
- QBER — Quantum Bit Error Rate
- QC — Quantum Communication
- QCMC — Quantum Communication Mobile Communication
- QIN — Quantum Information Network
- QIS — Quantum Information Science
- QKD — Quantum Key Distribution
- QKDN — Quantum Key Distribution Network
- QKM — Quantum Key Manager
- QPSK — Quadrature Phase Shift Keying
- QRNG — Quantum Random Number Generator
- QSDC — Quantum Secure Direct Communication
- QSN — Quantum Security Network
- RAN — Radio Access Network
- REST — Representational State Transfer
- RoF — Radio over Fiber
- SARG04 — Scarani-Acín-Ribordy-Gisin 2004 Protocol
- SC — Study Committee
- SDN — Software-Defined Networking
- SG — Study Group
- SNSPD — Superconducting Nanowire Single-Photon Detector
- SNS-TF-QKD — Sending-or-Not-Sending Twin-Field QKD
- SPAD — Single-Photon Avalanche Diode
- TCP — Transmission Control Protocol
- TDM — Time Division Multiplexing
- TF-QKD — Twin-Field Quantum Key Distribution
- TLS — Transport Layer Security
- USTC — University of Science and Technology of China
- VPN — Virtual Private Network
- WDM — Wavelength Division Multiplexing
- WG — Working Group
- xQAM — x-order Quadrature Amplitude Modulation

References

[Ladd10] T. D. Ladd, F. Jelezko, R. Laflamme, et al., "Quantum computers," *Nature*, 2010, vol. 464, no. 7285, pp. 45-53.

[Gisin07] N. Gisin, R. Thew, "Quantum communication," *Nature Photonics*, 2007, vol. 1, no. 3, pp. 165-171.

[Langer09] T. Länger, G. Lenhart, "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD," *New Journal of Physics*, 2009, vol. 11, no. 5, pp. 055051-1-055051-16.

[Chen21] Y. A. Chen, Q. Zhang, T. Y. Chen, et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, 2021, vol. 589, no. 7841, pp. 214-219.

[Bennett84] C. H. Bennett, G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[Dirac81] P. A. M. Dirac, *The Principles of Quantum Mechanics*, Oxford: Oxford University Press, 1981.

[Heisenberg85] W. Heisenberg, "On the intuitive content of quantum-theoretical kinematics and mechanics," Berlin: Springer, 1985, pp. 478-504.

[Wootters82] W. K. Wootters, W. H. Zurek, "A single quantum cannot be cloned," *Nature*, 1982, vol. 299, no. 5886, pp. 802-803.

[Zhang21] C. H. Zhang, *Design and experimental verification of novel quantum cryptography schemes*, Nanjing University of Posts and Telecommunications, 2021. [in Chinese]

[Ekert91] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, 1991, vol. 67, no. 6, pp. 661-663.

[Bennett92] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, 1992, vol. 68, no. 21, pp. 3121-3124.

[Lucamarini18] M. Lucamarini, Z. L. Yuan, J. F. Dynes, et al., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, 2018, vol. 557, no. 7705, pp. 400-403.

[Wang19] W. Wang, F. Xu, H. K. Lo, "Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks," *Physical Review X*, 2019, vol. 9, no. 4, pp. 041012-1-041012-30.

[Zhang24] Y. Zhang, Y. Bian, Z. Li, S. Yu, H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Applied Physics Reviews*, 2024, vol. 11, no. 1, pp. 011318-1-011318-54.

[Bahrami20] A. Bahrami, A. Lord, T. Spiller, "Quantum key distribution integration with optical dense wavelength division multiplexing: A review," *IET Quantum Communication*, 2020, vol. 1, no. 1, pp. 9-15.

[Tian23] Y. Tian, Y. Zhang, S. Liu, et al., "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," *Optics Letters*, 2023, vol. 48, no. 11, pp. 2953-2956.

[Li23] W. Li, L. Zhang, H. Tan, et al., "High-rate quantum key distribution exceeding 110 Mb/s," *Nature Photonics*, 2023, vol. 17, no. 5, pp. 416-421.

[Hajomer24] A. A. E. Hajomer, C. Bruynsteen, I. Derkach, et al., "Continuous-variable quantum key distribution at 10 Gbaud using an integrated photonic–electronic receiver," *Optica*, 2024, vol. 11, no. 9, pp. 1197-1204.

[Liu23] Y. Liu, W. J. Zhang, C. Jiang, et al., "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Physical Review Letters*, 2023, vol. 130, no. 21, pp. 210801-1-210801-6.

[Zhou23] L. Zhou, J. Lin, Y. M. Xie, et al., "Experimental quantum communication overcomes the rate–loss limit without global phase tracking," *Physical Review Letters*, 2023, vol. 130, no. 25, pp. 250801-1-250801-7.

[Avesani21] M. Avesani, L. Calderaro, M. Schiavon, et al., "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *NPJ Quantum Information*, 2021, vol. 7, no. 1, pp. 93-1-93-8.

[Sax23] R. Sax, A. Boaron, G. Boso, et al., "High-speed integrated QKD system," *Photonics Research*, 2023, vol. 11, no. 6, pp. 1007-1014.

[Dolphin23] J. A. Dolphin, T. K. Paraïso, H. Du, et al., "A hybrid integrated quantum key distribution transceiver chip," *NPJ Quantum Information*, 2023, vol. 9, no. 1, pp. 84-1-84-8.

[Dou23] T. Dou, S. Gao, C. L. Zhang, et al., "Coexistence of 1 Tbps classical optical communication and quantum key distribution over a 100.96 km few-mode fiber," *Optics Letters*, 2023, vol. 48, pp. 4905-4908.

[IDQ23] IDQ, "SK Telecom and Samsung unveil the Galaxy Quantum 4, providing more safety and performance with IDQ's QRNG chip," 2023. URL: https://www.idquantique.com/sk-telecomand-samsung-unveil-the-galaxy-quantum-4/.

[Heise24] Heise Online, "Swisscom and German start-up test quantum-security solution using entangled photons," 2024. URL: https://www.heise.de/news/Swisscom-und-deutsches-Start-up-testen-Quantum-Security-Loesung-10291699.html.

[Toshiba25] Toshiba Europe, "Toshiba and Orange Business launch France's first commercial quantum-secure network service," 2025. URL: https://www.toshiba.eu/quantum/news/toshiba-orange-launch-commercial-quantum-network/.

[Elliott02] C. Elliott, "Building the quantum network," *New Journal of Physics*, 2002, vol. 4, no. 1, pp. 46-1-46-12.

[Peev09] M. Peev, C. Pacher, R. Alléaume, et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, 2009, vol. 11, no. 7, pp. 075001-1-075001-37.

[Stucki11]	D. Stucki, M. Legre, F. Buntschu, et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, 2011, vol. 13, no. 12, pp. 123001-1-123001-18.
[Mirza10]	A. Mirza, F. Petruccione, "Realizing long-term quantum cryptography," *JOSA B*, 2010, vol. 27, no. 6, pp. A185-A188.
[Yuan05]	Z. L. Yuan, A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Optics Express*, 2005, vol. 13, no. 2, pp. 660-665.
[Sasaki11]	M. Sasaki, M. Fujiwara, H. Ishizuka, et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, 2011, vol. 19, no. 11, pp. 10387-10409.
[Xu09]	F. X. Xu, W. Chen, S. Wang, et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, 2009, vol. 54, no. 17, pp. 2991-2997.
[ITUT21a]	ITU-T, "QKDNs—Software-defined networking control: Y.3805," Genève: ITU-T, 2021.
[ITUT22a]	ITU-T, "QKDN interworking framework: Y.3810," Genève: ITU-T, 2022.
[ITUT23a]	ITU-T, "QKDN interworking—Functional requirements: Y.3813," Genève: ITU-T, 2023.
[ITUT24a]	ITU-T, "QKDN interworking—Architecture: Y.3818," Genève: ITU-T, 2024.
[ITUT21b]	ITU-T, "QKDNs—Applications of machine learning: Y Suppl.70," Genève: ITU-T, 2021.
[ITUT23b]	ITU-T, "QKDNs—Functional requirements and architecture for ML enablement: Y.3814," Genève: ITU-T, 2023.
[ITUT24b]	ITU-T, "QKDN interworking—SDN control: Y.3820," Genève: ITU-T, 2024.
[ITUT24c]	ITU-T, "QKDN federation—Reference models: Y.3824," Genève: ITU-T, 2024.
[ITUT23c]	ITU-T, "QKDNs—Overview of resilience: Y.3815," Genève: ITU-T, 2023.
[ITUT24d]	ITU-T, "QKDNs—Requirements for resilience: Y.3821," Genève: ITU-T, 2024.
[ITUT25]	ITU-T, "QKDNs—Procedures for key-supply protection and recovery for resilience: Y.3830," Genève: ITU-T, 2025.
[ETSI10a]	ETSI, "Quantum Key Distribution (QKD) — Use Cases: GS QKD 002 V1.1.1," Sophia Antipolis: ETSI, 2010.
[ETSI10b]	ETSI, "Quantum Key Distribution (QKD) — Application Interface: GS QKD 004 V2.1.1," Sophia Antipolis: ETSI, 2010.
[ETSI16]	ETSI, "Quantum Key Distribution (QKD) — Component Characterization: Characterizing Optical Components for QKD Systems: GS QKD 011 V1.1.1," Sophia Antipolis: ETSI, 2016.
[ETSI18]	ETSI, "Quantum Key Distribution (QKD) — Components and Internal Interfaces: GS QKD 003 V2.1.1," Sophia Antipolis: ETSI, 2018.

[ETSI19]	ETSI, "Quantum Key Distribution (QKD) — Protocol and Data Format of REST-based Key Delivery API: GS QKD 014 V1.1.1," Sophia Antipolis: ETSI, 2019.
[ETSI22]	ETSI, "Quantum Key Distribution (QKD) — Orchestration Interface for Software-Defined Networks: GS QKD 018 V1.1.1," Sophia Antipolis: ETSI, 2022.
[CCSA21a]	CCSA, "Technical Requirements for Quantum Key Distribution (QKD) Systems — Part 1: Decoy-State BB84-Based QKD Systems: YD/T 3834.1-2021," Beijing: CCSA, 2021. [in Chinese]
[CCSA21b]	CCSA, "Test Methods for Quantum Key Distribution (QKD) Systems — Part 1: Decoy-State BB84-Based QKD Systems: YD/T 3835.1-2021," Beijing: CCSA, 2021. [in Chinese]
[CCSA21c]	CCSA, "Key Components and Modules for BB84-Based Quantum Key Distribution — Part 3: Quantum Random Number Generators (QRNG): YD/T 3907.3-2021," Beijing: CCSA, 2021. [in Chinese]

Last modified on November 17, 2025
This and other papers on Recent Advances in Networking are available online at
https://www.cse.wustl.edu/~jain/cse5700-25/index.html
Back to Raj Jain's Home Page