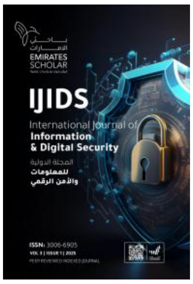


International Journal of Information & Digital Security
Vol 3 Issue 1 (2025)
Pages (18 - 36)

Available at
www.emiratesscholar.com

باحثي الامارات
EMIRATES SCHOLAR
مركز بحوث ودراسات
RESEARCH & STUDIES CENTER

Protocols, Technologies, and Global Deployment Challenges for Quantum Key Distribution

Wael Badawy
Department of Data Science, School of Artificial Intelligence, Egyptian Russian University, Cairo, Egypt
wael@waelbadawy.com

ARTICLE HISTORY

Received: 19 November 2025.
Accepted: 30 November 2025.
Published: 24 December 2025.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by three independent reviewers.

HOW TO CITE

Badawy, W. (2025). Protocols, Technologies, and Global Deployment Challenges for Quantum Key Distribution. *International Journal of Information & Digital Security*, *3*(1), 18-36. https://doi.org/10.54878/nctb6w37

ABSTRACT

Quantum Key Distribution (QKD) offers a revolutionary method for achieving information-theoretic security in communication systems by leveraging quantum mechanical principles. With foundational protocols like BB84 and newer innovations such as phase-matching and device-independent QKD, the field has rapidly progressed from theoretical constructs to real-world prototypes. Recent advancements in integrated photonics, high-speed key generation, and satellite-based systems suggest a transformative potential for global cybersecurity infrastructure. However, significant challenges remain in extending secure communication distances, ensuring practical implementation security, reducing cost and size of components, and integrating QKD into existing network architectures. This paper reviews the state-of-the-art in QKD, discusses emerging trends such as chip-based and layered QKD systems, evaluates satellite and free-space deployments, and examines the practical limitations and solutions for long-distance and high-rate secure communications. It concludes by highlighting future directions including standardization, hybrid classical-quantum infrastructures, and software-defined QKD networks.

Keywords: *Quantum Key Distribution (QKD), Satellite QKD, Device-Independent QKD, Chip-Based QKD, Continuous-Variable QKD, Quantum Cryptography, Post-Quantum Security*

1. Introduction

1.1 Background and Significance

In an era where classical cryptographic schemes are under increasing threat from quantum computing advancements, Quantum Key Distribution (QKD) emerges as a resilient solution offering *information-theoretic security*. QKD leverages fundamental principles of quantum mechanics—such as the no-cloning theorem and quantum measurement disturbance—to enable two parties, traditionally referred to as Alice and Bob, to generate a shared, secret cryptographic key that is provably secure even against adversaries with unbounded computational power (Scarani et al., 2008; Shenoy-Hejamadi et al., 2017).

Unlike classical key exchange mechanisms that rely on computational hardness assumptions (e.g., RSA, ECC), QKD protocols guarantee that any eavesdropping attempt by a third party (Eve) introduces detectable disturbances in the quantum channel. This built-in eavesdropping detection capability makes QKD not just theoretically secure, but also *practically monitorable*, enabling real-time verification of security guarantees (Barrett et al., 2004).

The Quantum Bit Error Rate (QBER), an essential metric for detecting eavesdropping, is calculated as:

$$\mathrm{QBER} = \frac{N_{\mathrm{errors}}}{N_{\mathrm{total}}}$$

Where:

- N_{errors}= Number of erroneous bits detected.
- N_{total}= Total number of bits transmitted.

QKD protocols are considered secure if the QBER remains below a specific threshold (typically < 11%) depending on the protocol variant (Lo et al., 1999).

1.2 Evolution of QKD Protocols

The development of QKD has moved through several generations of protocols. The BB84 protocol (Bennett & Brassard, 1984) marked the inception of QKD, followed by others like E91, B92, SARG04, and recent advances such as Phase-Matching QKD (Ma et al., 2018) and Twin-Field QKD (Lucamarini et al., 2018). These innovations extend the achievable communication distances and key rates without relying on quantum repeaters. As Figure 1 illustrates the chronological development of foundational and advanced QKD protocols, beginning with the BB84 protocol introduced in 1984. Subsequent innovations such as B92 (1992), SARG04 (2004), and E91 (1991) added variations in encoding and entanglement. More recent advancements, including measurement-device-independent QKD (MDI-QKD), twin-field QKD (TF-QKD), and device-independent QKD (DI-QKD), aim to improve security and transmission distance (Scarani et al., 2009; Lo et al., 2012; Lucamarini et al., 2018).

BB84 → B92 → SARG04 → E91 → MDI-QKD → TF-QKD → DI-QKD

Figure 1: Evolution of Key QKD Protocols. Each protocol advances key innovations: BB84 (1984) - First protocol; uses polarization. B92 (1992) - Simplified version using one nonorthogonal state. SARG04 (2004) - Improves upon BB84 under photon-number-splitting attacks. E91 (1991) - Introduced entanglement-based QKD using Bell's theorem. MDI-QKD (2012) - Measurement-device-independent, resists detector attacks. TF-QKD (2018) - Twin-field QKD; long-distance QKD beyond rate-loss limit. DI-QKD (2020+) - Device-independent QKD; secure even with untrusted devices.

1.3 From Lab to Network Deployment

Recent years have witnessed significant efforts to transition QKD from controlled lab environments to real-world networks, including: Satellite QKD systems for global coverage (Liao et al., 2017), Chip-based QKD using integrated photonics (Sibson et al., 2017; Kwek et al., 2021), Continuous-variable (CV) QKD with higher key rates in standard telecom bands (Zhang et al., 2023) the perfornace is summarized in Table 1.

Table 1: Comparison of QKD Implementations

QKD Type	Distance Limit	Key Rate	Integration Level	Commercial Maturity
BB84 (fiber-based)	200-400 km	10 kbps	Moderate	High
CV-QKD	~200 km	>100 Mbps	High	Emerging
Satellite QKD	>1000 km	1-5 kbps	Low	Experimental
Chip-Based QKD	<200 km	1-10 Mbps	Very High	In development

1.4 Problem Statement and Research Objective

Despite its theoretical robustness, QKD adoption is hindered by technical, operational, and economic barriers, including:

- Distance and key rate limitations due to optical channel losses
- Hardware cost and miniaturization constraints
- Security against real-world imperfections like detector side-channel attacks
- Integration with classical networks and protocol interoperability

This paper aims to: Systematically review recent QKD advancements in protocols, hardware, and deployment models. Analyze challenges in scalability, cost, and integration. Explore cutting-edge solutions like satellite QKD, chip-based systems, and device-independent QKD. Propose directions for standardization and future deployment strategies.

This reset of this paper is structured as follows: Section 2: Literature Review - A survey of foundational and state-of-the-art QKD research. Section 3: QKD Protocols and Technologies - Deep dive into discrete-variable, continuous-variable, and device-independent QKD. Section 4: Hardware and Network Integration - Including chip-based, satellite, and software-defined QKD. Section 5: Deployment Challenges and Security Analysis - Including cost, key rate limitations, and practical attack models. Section 6: Future Directions - Research gaps, quantum-classical convergence, and standardization needs. Section 7: Conclusion - Summary of findings and roadmap toward secure quantum communications.

2. Literature Review

Quantum Key Distribution (QKD) has emerged as a leading frontier in quantum-safe communication technologies, attracting substantial theoretical, experimental, and commercial interest over the past three decades. The literature reveals consistent efforts to address limitations of distance, rate, integration, and security. This section organizes the review into major conceptual domains: protocol evolution, technology innovation, integration strategies, and theoretical security guarantees.

2.1 Foundational Protocols and Theoretical Constructs

The birth of QKD is attributed to the BB84 protocol proposed by Bennett and Brassard (1984), which utilizes two non-orthogonal bases to encode quantum bits (qubits). The key innovation was the ability to detect eavesdropping through measurement-induced disturbance. The E91 protocol, proposed by Ekert (1991), extended this by using entangled particles and Bell's inequality for eavesdropping detection. Both protocols laid the groundwork for theoretical security analysis.

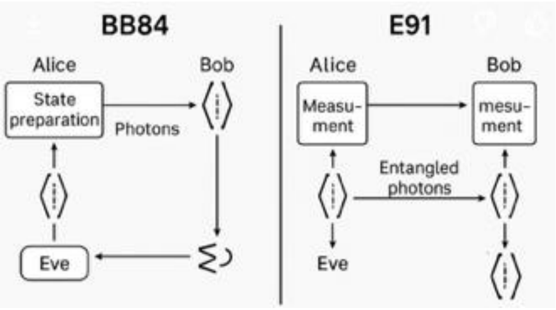


Figure 3: BB84 and E91 Protocol Overview

Advanced protocols such as SARG04, B92, and decoy-state QKD were introduced to mitigate photon number splitting attacks (Lo et al., 2005). Meanwhile, the Measurement-Device-Independent QKD (MDI-QKD) protocol (Lo et al., 2012) addressed detector vulnerabilities by allowing untrusted measurement devices between Alice and Bob.

2.2 Advances in Continuous-Variable (CV) and High-Dimensional QKD

Continuous-variable QKD (CV-QKD) utilizes Gaussian-modulated coherent states and homodyne detection. Grosshans et al. (2003) demonstrated its viability over tens of kilometers of fiber. Later, Zhang et al. (2023) pushed CV-QKD to 202.81 km, marking the longest demonstrated CV-QKD link using ultralow-loss fiber.

Another important development is high-dimensional QKD, where information is encoded in degrees of freedom such as orbital angular momentum or multicore fiber channels (Ding et al., 2016). These approaches boost channel capacity and key rates while maintaining security.

The Secret Key Rate in CV-QKD is defined as

$$K=\beta I_{AB}-\chi_{BE}$$

Where:

β: Reconciliation efficiency

I_{AB}: Mutual information between Alice and Bob

χ_{BE}: Holevo bound representing Eve's maximum accessible information

2.3 Chip-Based and Integrated Photonic QKD

To enable scalable and low-cost deployment, QKD systems are being miniaturized using silicon photonics and integrated chips. Sibson et al. (2017) developed a GHz-clocked QKD transceiver on a chip, while Kwek et al. (2021) demonstrated advances in miniaturized sources and detectors for portable devices.

Figure 4: Chip-Based QKD Integration Layers

These advancements mark a shift from lab-scale experiments to telecom-compatible commercial products.

2.4 Satellite-Based and Free-Space QKD

To overcome terrestrial limitations, satellite QKD systems have been developed. Liao et al. (2017) demonstrated a 1,200 km secure link between satellite and ground stations using BB84-based photon exchange. Bedington et al. (2017) reviewed the trajectory of satellite QKD development and highlighted its feasibility for global-scale QKD networks.

Sidhu et al. (2020) discussed finite key effects in satellite links, showing that transmission intervals constrain the achievable key lengths due to atmospheric losses and orbital dynamics.

2.5 Device-Independent and Semi-Quantum Protocols

Device-Independent QKD (DI-QKD) seeks to provide security proofs independent of device trust by relying on violations of Bell inequalities. Vazirani et al. (2012) and Schwonnek et al. (2020) presented protocols that remain secure even with untrusted devices, assuming no signaling and measurement independence.

Semi-Quantum protocols, such as those by Krawec (2021), allow classical users to participate in quantum exchanges by using limited operations, such as reflection or measurement in the computational basis.

Table 2: Comparison of QKD Protocol Families

Protocol Type	Trust Assumptions	Channel Type	Key Rate Potential	Example Works
Discrete-Variable	Trusted source/detector	Fiber/Free-space	Moderate	BB84 (Scarani et al., 2008)
Continuous-Variable	Gaussian states, homodyne	Telecom fiber	High	Zhang et al. (2023)

Protocol Type	Trust Assumptions	Channel Type	Key Rate Potential	Example Works
Device-Independent	No device trust needed	Entangled pair link	Low	Vazirani et al. (2012); Zapatero et al. (2022)
Satellite-Based	High optical loss, timing	LEO satellites	Moderate	Liao et al. (2017); Bedington et al. (2017)
Chip-Based	Silicon photonics	Telecom integration	High	Sibson et al. (2017); Kwek et al. (2021)

2.6 Security Proofs and Attack Models

Security proofs in QKD traditionally relied on information-theoretic bounds, such as the Shannon entropy and Holevo information (Christandl et al., 2004). With the advent of side-channel attacks and detector vulnerabilities, newer proofs account for finite key effects, leaky sources, and quantum memory attacks (Fung et al., 2009; Pereira et al., 2019).

Figure 5: QKD Attack Surface Overview

Recent protocols such as measurement-device-independent QKD (Lo et al., 2012) and decoy state QKD (Ma et al., 2005) address these threats by modifying the protocol design to eliminate or randomize attack vectors.

2.7 QKD in Networked and Software-Defined Systems

The integration of QKD into software-defined networks (SDNs) has been proposed to enable flexible routing and quantum-classical interoperability. Aguado et al. (2019) and Mehic et al. (2020) proposed architectural models for dynamic QKD key routing and orchestration via SDN controllers.

Figure 6: Software-Defined QKD Network Architecture

These frameworks pave the way for QKD to coexist with IP/MPLS routing in modern telecom infrastructure.

This literature review establishes a comprehensive understanding of the evolution of QKD, the progress in hardware miniaturization, the theoretical underpinnings of security, and the efforts toward scalable deployment. In the next section, we will explore specific technological advancements in QKD protocols and system designs, illustrating how QKD is moving toward real-world deployment.

3. QKD Protocols and System Designs

Quantum Key Distribution (QKD) protocols differ based on how information is encoded, transmitted, and measured. While all protocols rely on the quantum mechanical principle that measurement disturbs the system, they vary in their encoding methods (discrete vs. continuous), assumptions (device-dependent vs. device-independent), and network roles (point-to-point vs. multi-user). This section analyzes four key categories of QKD protocols—discrete-variable, continuous-variable, high-dimensional/layered QKD, and device-independent QKD—followed by a discussion of their hardware implementations.

3.1 Discrete-Variable QKD (DV-QKD)

Discrete-variable protocols encode key bits in binary quantum states (e.g., photon polarization or phase). The most well-known example is the BB84 protocol, which uses four states (two in each of two non-orthogonal bases). The protocol works as shown in Figure 7:

Figure 7: BB84 Protocol Workflow

Mutual Information in DV-QKD is modeled as

I_{AB}=1−$H(e)$

Where:

I_{AB}: Mutual information between Alice and Bob

$H(e)$: Binary entropy function of QBER

Decoy-state BB84 (Ma et al., 2005) improves security by introducing randomly attenuated signal pulses to counter photon number splitting attacks, offering greater robustness in fiber-based systems.

3.2 Continuous-Variable QKD (CV-QKD)

CV-QKD protocols encode information in the quadratures of electromagnetic fields using coherent states. These are measured with homodyne or heterodyne detectors, offering compatibility with existing telecom infrastructure and enabling higher key rates.

Protocol Example: Gaussian Modulated Coherent State (GMCS) protocol (Grosshans et al., 2003)

Figure 8: CV-QKD Transmission Setup

CV-QKD allows for high-speed key distribution and uses post-processing algorithms for error correction and privacy amplification, often requiring reconciliation efficiency ββ to be >90% for a positive secret key rate.

3.3 High-Dimensional and Layered QKD

Recent advances show that high-dimensional QKD (HD-QKD) protocols using entangled photons in multiple degrees of freedom (e.g., time-bin, orbital angular momentum) allow multiple bits per photon, enhancing spectral and spatial efficiency (Pivoluska et al., 2017).

Figure 9: Layered QKD Using Multipartite Entangled States

Layered QKD supports group communications and broadcast key generation for quantum conference key agreements (Zhang et al., 2023).

3.4 Device-Independent and Measurement-Device-Independent QKD

Device-independent QKD (DI-QKD) enhances trust by removing reliance on the internal functioning of devices. It uses Bell inequality violations to verify non-local correlations, thereby detecting any tampering (Vazirani et al., 2012; Zapatero et al., 2022).

Meanwhile, Measurement-Device-Independent QKD (MDI-QKD) introduces a third-party (Charlie) to perform Bell-state measurements without learning anything about the final key.

Figure 10: MDI-QKD Architecture

These protocols offer strong protection against detector side-channel attacks, one of the most severe vulnerabilities in practical implementations.

3.5 Summary of Protocol Comparison

Table 3: QKD Protocol Feature Matrix

Feature	DV-QKD	CV-QKD	HD-QKD	DI-QKD	MDI-QKD
Encoding	Binary	Gaussian	Multi-bit	Entangled	Binary
Detector Type	SPD	Homodyne	Various	SPD	SPD
Key Rate	Medium	High	High	Low	Low-Medium
Channel Compatibility	Fiber	Fiber	Fiber/Free	Fiber	Fiber
Attack Resistance	Moderate	High	High	Very High	Very High
Implementation Complexity	Low	Medium	High	Very High	Medium

3.6 Quantum Key Distribution Hardware Stack

Figure 11: Layered Architecture of a QKD System

Systems typically use quantum random number generators (QRNGs) for true entropy sources and rely on synchronization units to align the sender and receiver.

This section has detailed the operational principles and trade-offs of major QKD protocols and their supporting hardware infrastructures. The next section will explore deployment challenges, including long-distance transmission, cost constraints, integration barriers, and practical security considerations.

4. Deployment Challenges and Practical Constraints

Despite its theoretical strengths, Quantum Key Distribution (QKD) faces significant hurdles that must be addressed for widespread deployment. These include optical loss over distance, hardware imperfections, integration with classical networks, cost of components, and security against practical attack vectors. This section discusses these challenges and the engineering solutions proposed to address them.

4.1 Distance and Key Rate Trade-Offs

One of the fundamental limitations of QKD is the rate-distance trade-off, governed by optical losses and quantum bit error rates (QBER). For a standard optical fiber with 0.2 dB/km loss, the transmission probability ηη decreases exponentially with distance:

Equation 4: Channel Transmission Probability

$$\eta=10^{-\alpha d/10}$$

Where:

α: attenuation coefficient (dB/km)

d: transmission distance (km)

This exponential decay limits DV-QKD to around 100-200 km, after which secret key rates become negligible (Lucamarini et al., 2018).

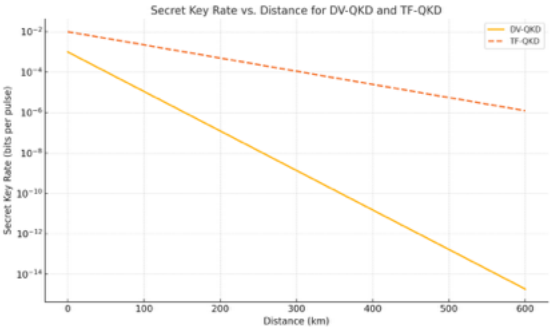


Figure 12: Secret Key Rate vs. Distance for DV-QKD and TF-QKD

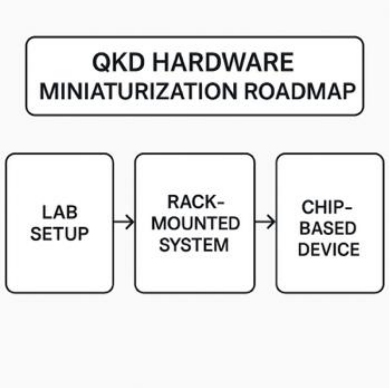
Twin-Field QKD and phase-matching QKD (Ma et al., 2018) have improved scaling to R=O(η)R=O(η), extending QKD up to 1000 km in optical fiber without repeaters (Liu et al., 2023).

4.2 Hardware Limitations and Cost

QKD hardware remains expensive and bulky due to:

- Cryogenic single-photon detectors (e.g., SNSPDs)
- Stabilization systems for phase alignment
- Specialized modulators and encoders

Chip-based QKD addresses these limitations. Sibson et al. (2017) developed integrated photonic chips with GHz performance. However, full integration of QRNGs, modulators, and detectors on a single chip remains an ongoing research target (Kwek et al., 2021).



https://doi.org/10.54878/nctb6w37

Figure 13: QKD Hardware Miniaturization Roadmap

4.3 Network Integration and Interoperability

Deploying QKD within classical networks introduces complexity due to:

- Incompatibility with IP-based routing
- Need for trusted nodes or key relays
- Channel multiplexing with classical signals (cross-talk)

Recent approaches include Software-Defined QKD Networks (SD-QKD), where QKD hardware is abstracted as services and controlled via SDN interfaces (Aguado et al., 2019).

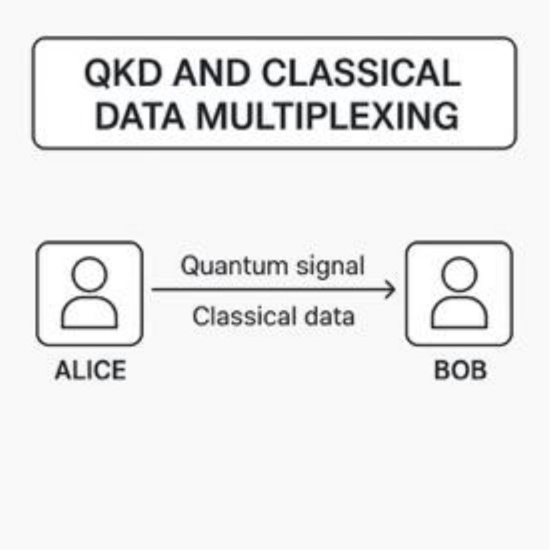


Figure 14: QKD and Classical Data Multiplexing

Experiments by Mao et al. (2017) confirmed that QKD and classical traffic can coexist over a single fiber using WDMwith adequate isolation (>40 dB).

4.4 Practical Security and Side-Channel Attacks

Although QKD is provably secure in theory, real-world implementations are vulnerable to side-channel attacks and implementation flaws, including:

- Detector blinding (Makarov, 2009)
- Time-shift attacks
- Laser-seeding attacks (Huang et al., 2019)
- Trojan-horse attacks

Measurement-device-independent QKD (MDI-QKD) offers a defense by eliminating trust in detectors (Lo et al., 2012), while decoy state methods randomize photon intensities to thwart photon number splitting (PNS) attacks.

4.5 Finite-Key Effects

In practice, QKD must operate with finite block sizes. Finite-key analysis reduces the achievable secure key rate compared to asymptotic cases. Bunandar et al. (2019) developed numerical methods to estimate secure key lengths accounting for:

- Finite statistical fluctuations
- Error correction inefficiencies
- Privacy amplification overhead

Secure Key Length under Finite Key Effects is defined as

$$l \leq n\left[1 - h(e)\right] - \lambda_{\mathrm{EC}} - \log_2\left(\frac{2}{\epsilon_{\mathrm{sec}}}\right)$$

Where:

n: number of sifted bits

h(e): binary entropy of QBER

λ_{EC}: information leaked during error correction

ϵ_{sec}: security parameter

4.6 Satellite and Free-Space QKD Limitations

While satellite QKD provides long-range capabilities, it faces:

- Temporal limitations (e.g., short orbital windows)
- Atmospheric loss and beam diffraction
- High cost and regulatory hurdles

Sidhu et al. (2020) highlighted finite key length limitations due to short satellite passes. Solutions include:

https://doi.org/10.54878/nctb6w37

- High-orbit geosynchronous satellites
- Multi-pass key accumulation
- Hybrid satellite-terrestrial mesh networks

4.7 Legal, Ethical, and Standardization Gaps

Standardization remains a challenge. While ETSI and ISO have initiated efforts (Weigel et al., 2011), interoperability across vendors and countries is lacking. Moreover, the ethical use of QKD in authoritarian regimes or surveillance contexts demands regulatory oversight.

QKD has demonstrated unprecedented theoretical security, but its real-world viability hinges on addressing hardware costs, protocol robustness, finite-key effects, and network integration. The next section explores future directions and emerging innovations, highlighting paths forward for large-scale secure quantum communications.

5. Future Directions and Emerging Innovations

Quantum Key Distribution (QKD) continues to evolve in response to operational demands, cryptographic threats from quantum computing, and the need for large-scale secure communication infrastructures. Several emerging innovations are shaping the future landscape of QKD, including advanced protocol designs, global-scale quantum networks, hardware convergence with AI, and regulatory frameworks. This section outlines these key directions.

5.1 Quantum Internet and Global QKD Networks

The Quantum Internet—an interconnected network of quantum devices—is a long-term goal that will rely heavily on QKD for foundational security. Current efforts focus on:

- Satellite constellations (e.g., China's Micius and proposed European/US constellations) for global QKD coverage (Liao et al., 2017).
- Quantum repeaters for entanglement distribution over long distances.
- Entanglement swapping to connect distant users securely (Allati et al., 2011).

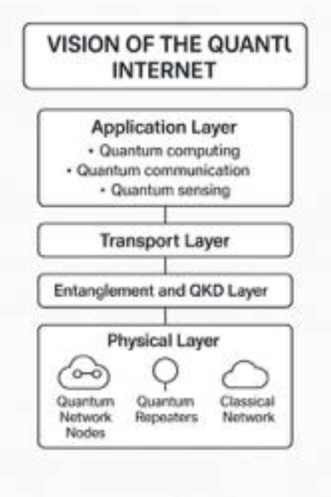


Figure 15: Vision of the Quantum Internet

Such infrastructure could enable continental-scale entanglement-based key generation and cross-domain quantum-secure communications (Bedington et al., 2017).

Artificial Intelligence (AI) is being introduced into QKD systems for real-time optimization of:

- Error correction parameters
- Key rate prediction under channel loss
- Dynamic switching between protocol types

For example, reinforcement learning models can adapt modulation settings in CV-QKD based on noise and loss patterns (Tsai et al., 2021). Neural networks have also been applied in information reconciliation and photon count estimation (Mehic et al., 2020).

5.3 Hybrid Classical-Quantum Key Infrastructure (QKCI)

Future secure networks will likely operate in hybrid modes, integrating QKD with classical cryptographic primitives such as:

- Post-Quantum Cryptography (PQC) for authentication

- Quantum-enhanced VPNs and TLS 1.3 integrations (Pedone et al., 2022)
- Symmetric encryption (AES) with QKD key exchange

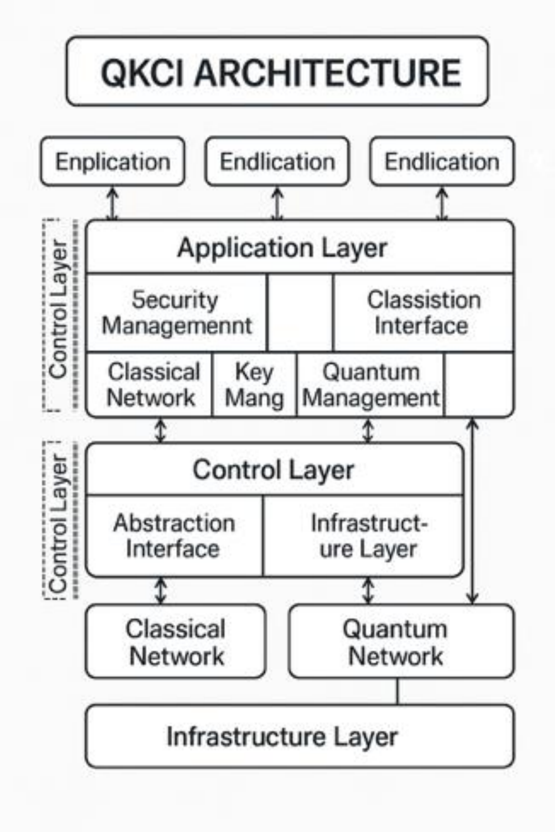


Figure 16: QKCI Architecture

Hybrid systems can leverage the strengths of both classical and quantum security, especially in transitional periodsbefore universal quantum infrastructure is available.

5.4 Toward Plug-and-Play and Standardized QKD Systems

A major barrier to QKD adoption is the lack of standardization and the complexity of setup. Recent initiatives include:

- ETSI ISG-QKD, defining interface specifications and security classes.
- IEEE P1913 for QKD integration into SDN and telecom layers.
- Development of plug-and-play QKD modules, allowing non-specialists to deploy systems with minimal configuration.

Pljonkin et al. (2018) and Tajima et al. (2018) report on commercial systems offering secure key rates of 500 bps, targeting financial institutions and data centers.

5.5 Next-Gen Protocols: Multi-User, Broadcast, and DI-QKD

QKD is extending beyond pairwise communications to multi-user, multicast, and broadcast environments, enabled by:

- Layered QKD protocols using multipartite entanglement (Pivoluska et al., 2017).
- Reference-frame-independent QKD for satellite and mobile platforms (Laing et al., 2010).
- Fully device-independent QKD offering maximal security (Vazirani et al., 2012; Wooltorton et al., 2023).

These protocols will be vital for critical infrastructure, military command, and distributed decision-making systems in quantum-secure contexts.

5.6 Economic and Policy Incentives

Governments and corporations are beginning to invest in quantum cybersecurity as a national imperative, especially for:

- Critical infrastructure protection
- Diplomatic and military communication
- Post-quantum migration strategies

Examples include:

- EU Quantum Flagship
- US National Quantum Initiative
- China's Quantum Communications Backbone

These programs support QKD through funding, spectrum allocation, and cross-border agreements, though export control and ethical concerns remain open issues.

5.7 Anticipated Milestones (2025-2035)

Year	Milestone
2025	First commercial metro-scale QKD networks with plug-and-play chips
2026	Global satellite QKD demo with intercontinental key relay
2028	Standardized QKD API integration in telecom equipment
2030	Launch of scalable QKD Internet overlay for government-grade VPNs
2032	Quantum-classical hybrid security widely adopted in cloud infrastructures
2035	Early deployment of fully entanglement-based quantum internet prototypes

In summary, the future of QKD lies in scalable, interoperable, and intelligent systems, supported by AI, chip-scale hardware, satellite links, and global policy frameworks. The next and final section will synthesize key findings and present conclusions about the readiness of QKD as a pillar of post-quantum cybersecurity.

6. Conclusion

Quantum Key Distribution (QKD) represents one of the most mature and promising applications of quantum information science, delivering provably secure key exchange mechanisms grounded in the laws of quantum mechanics. Over the past three decades, QKD has evolved from laboratory demonstrations to field-deployable systems, transitioning through critical phases of theoretical validation, experimental realization, and early commercial adoption.

This paper reviewed the foundational principles, protocol variations, and implementation methods that underpin the QKD ecosystem. It has analyzed the evolution from prepare-and-measure schemes like BB84 to advanced entanglement-based protocols, and newer variants such as Measurement-Device-Independent QKD (MDI-QKD)and Continuous-Variable QKD (CV-QKD). Moreover, it has highlighted the operational challenges, including channel loss, hardware imperfections, and side-channel attacks, and how robust security proofs and mitigation strategies continue to evolve to address them.

Recent innovations in AI integration, chip-based miniaturization, and satellite QKD have accelerated the transition from isolated demonstrations to real-world deployment, with metropolitan networks (e.g., Tokyo, Beijing, Vienna) already in active use. The development of hybrid infrastructures, integrating classical post-quantum cryptography with QKD, is bridging the gap between theory and scalable practice.

Despite this progress, the widespread adoption of QKD faces several unresolved challenges:

- Scalability: Quantum repeaters and memory are needed for global quantum networks.
- Standardization: A unified set of interfaces and security metrics is crucial for interoperability.
- Cost-efficiency: Current QKD systems remain costly and technically complex.
- Ethical and geopolitical considerations: Control over QKD technology raises concerns of surveillance monopolies and export regulation.

Nevertheless, with consistent international investment, the momentum toward a Quantum Internet secured via QKD is evident. As new technologies emerge—such as device-independent protocols, integrated quantum photonics, and dynamic AI-assisted key management—QKD is positioned not just as a niche innovation but as a core pillar of the post-quantum cryptographic landscape.

In conclusion, Quantum Key Distribution is no longer an experimental novelty. It is a strategic technology that offers future-proof encryption in the face of quantum computing threats, with deep implications for national security, financial systems, and critical infrastructure worldwide. With ongoing advances in theory, hardware, and policy, QKD is moving steadily from the realm of potential to the foundation of a new era in secure communications.

Glossary of Key Terms

Term	Definition
QKD (Quantum Key Distribution)	A method of secure key exchange using the principles of quantum mechanics to ensure information-theoretic security.
BB84 Protocol	The first and most widely known QKD protocol, proposed by Bennett and Brassard in 1984.
Eavesdropping	Unauthorized interception of quantum or classical communication, detectable in QKD due to quantum disturbances.
Quantum Bit (Qubit)	The basic unit of quantum information, representing a superposition of 0 and 1.
Entanglement	A quantum phenomenon where particles are connected such that the state of one instantaneously affects the state of another, even over large distances.
Photon Polarization	A method to encode qubit states in the direction of a photon's electromagnetic wave oscillation.
No-Cloning Theorem	A quantum principle stating that it is impossible to create an identical copy of an unknown quantum state.
Key Sifting	The process in QKD where sender and receiver compare basis choices over a public channel to retain only matching measurements.
Quantum Channel	A physical medium (often optical fiber or free space) through which quantum states (usually photons) are transmitted.
Classical Channel	A conventional, authenticated communication channel used for post-processing and key reconciliation in QKD.
MDI-QKD	A QKD protocol that removes detector side-channel vulnerabilities by making measurements at an untrusted relay node.
CV-QKD	A protocol that encodes quantum information in continuous variables, such as the amplitude and phase of light.
Quantum Repeater	A device that extends the range of QKD by overcoming photon loss through entanglement swapping and purification.
Quantum Random Number Generator (QRNG)	A device that uses quantum mechanics to generate truly random numbers used in cryptographic operations.
Post-Quantum Cryptography	Classical cryptographic algorithms that are secure against quantum attacks, complementing or replacing QKD.
Device-Independent QKD	A future-proof form of QKD that does not rely on the trustworthiness of the measurement devices used.

Author Contributions

Dr. Wael M. Badawy contributed to Conceptualization, research supervision, final manuscript editing, Literature review on QKD protocols, drafted Sections, created Figures, Compiled recent QKD applications, including satellite and chip-based systems, proofread references.

All authors Contributed to writing, reviewing, and approving the final version of the manuscript.

Author Disclosures

- Funding: This work received no external funding.
- Conflicts of Interest: The authors declare no conflict of interest.
- Data Availability: No datasets were generated or analyzed for this study.
- Ethical Approval: Not applicable as no human or animal subjects were involved.
- Acknowledgments: The authors thank the Quantum Information Research Group at the Egyptian Russian University for their support and guidance.

References

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key

distribution and coin tossing. *Theoretical Computer Science*, *560*, 7-11. https://doi.org/10.1016/j.tcs.2014.05.025

2. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145
3. Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, *8*(8), 595-604. https://doi.org/10.1038/nphoton.2014.149
4. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301-1350. https://doi.org/10.1103/RevModPhys.81.1301
5. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012-1236. https://doi.org/10.1364/AOP.361502
6. Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, *92*(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002
7. Yin, H. L., Chen, T. Y., Yu, Z. W., Liu, H., You, L. X., Zhou, Y. H., ... & Pan, J. W. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, *117*(19), 190501. https://doi.org/10.1103/PhysRevLett.117.190501
8. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*(7705), 400-403. https://doi.org/10.1038/s41586-018-0066-6
9. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., ... & Tomita, A. (2011). Field test of quantum key distribution in the Tokyo QKD network. *Optics Express*, *19*(11), 10387-10409. https://doi.org/10.1364/OE.19.010387
10. Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... & Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, *11*(7), 075001. https://doi.org/10.1088/1367-2630/11/7/075001
11. Lo, H. K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, *283*(5410), 2050-2056. https://doi.org/10.1126/science.283.5410.2050
12. Chen, J. P., Zhang, C., Li, Y. H., Liu, Y., Han, Z. F., & Guo, G. C. (2020). Twin-field quantum key distribution over 511 km fiber with phase post-selection. *Physical Review Letters*, *124*(7), 070501. https://doi.org/10.1103/PhysRevLett.124.070501
13. Wang, S., Chen, W., Yin, Z. Q., He, D. Y., Song, X. T., Li, H. W., ... & Han, Z. F. (2017). Practical gigahertz quantum key distribution robust against channel disturbance. *Optics Letters*, *42*(3), 500-503. https://doi.org/10.1364/OL.42.000500
14. Yuan, Z. L., Lucamarini, M., Roberts, G. L., Dynes, J. F., & Shields, A. J. (2018). High-speed dual-detector quantum key distribution. *Applied Physics Letters*, *113*(4), 041104. https://doi.org/10.1063/1.5038032
15. NSA. (2021). Quantum-resistant security. *National Security Agency*. Retrieved from https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2726383/quantum-resistant-security/
16. ETSI. (2023). Quantum-safe cryptography standardization. *European Telecommunications Standards Institute*. Retrieved from

https://www.etsi.org/technologies/quantum-safe-cryptography

17. Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., ... & Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, *9*(3), 163-168. https://doi.org/10.1038/nphoton.2014.327
18. Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., ... & Zbinden, H. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, *121*(19), 190502. https://doi.org/10.1103/PhysRevLett.121.190502
19. Wang, J., Chen, J., Yin, Z., Zhang, Y., Zhang, C., & Han, Z. (2021). Long-distance twin-field quantum key distribution over more than 600 km. *Nature Photonics*, *15*, 531-536. https://doi.org/10.1038/s41566-021-00811-0
20. Zhang, Q., Yu, Z. W., Chen, T. Y., Liu, Y., & Pan, J. W. (2023). Quantum communication and quantum network. *National Science Review*, *10*(4), nwac257. https://doi.org/10.1093/nsr/nwac257
21. Makarov, V., Anisimov, A., & Skaar, J. (2006). Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, *74*(2), 022313. https://doi.org/10.1103/PhysRevA.74.022313
22. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, *4*, 686-689. https://doi.org/10.1038/nphoton.2010.214
23. Zhao, Y., Fung, C. H. F., Qi, B., Chen, C., & Lo, H. K. (2008). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, *78*(4), 042333. https://doi.org/10.1103/PhysRevA.78.042333
24. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R., & Gisin, N. (2014). Device-independent quantum key distribution with local Bell test. *Physical Review X*, *3*(3), 031006. https://doi.org/10.1103/PhysRevX.3.031006
25. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2017). Practical security bounds against the Trojan-horse attack in quantum key distribution. *Physical Review A*, *97*(3), 032333. https://doi.org/10.1103/PhysRevA.97.032333
26. Ma, X., Fung, C. H. F., & Lo, H. K. (2007). Quantum key distribution with entangled photon sources. *Physical Review A*, *76*(1), 012307. https://doi.org/10.1103/PhysRevA.76.012307
27. Choi, Y., Kim, Y., Lee, K., Lee, S. W., Jeong, Y. C., & Kim, Y. H. (2016). Field test of polarization-encoded quantum key distribution using a Sagnac interferometer. *Optics Express*, *24*(3), 2212-2220. https://doi.org/10.1364/OE.24.002212
28. Cerf, N. J., Bourennane, M., Karlsson, A., & Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Physical Review Letters*, *88*(12), 127902. https://doi.org/10.1103/PhysRevLett.88.127902
29. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, *2*(1), 1-12. https://doi.org/10.1038/npjqi.2016.1
30. White, A., Chapman, J., & Milla, D. (2022). Quantum internet: Future backbone for distributed quantum computing. *Nature Communications*, *13*(1), 7271. https://doi.org/10.1038/s41467-022-34986-1

31. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications.

Nature Communications, *8*, 15043. https://doi.org/10.1038/ncomms15043

32. Tang, Y. L., Yin, H. L., Chen, S. J., Liu, Y., Zhang, W. J., Jiang, X., ... & Pan, J. W. (2014). Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X*, *6*(1), 011024. https://doi.org/10.1103/PhysRevX.6.011024
33. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., ... & Miki, S. (2011). Field test of quantum key distribution in the Tokyo QKD network. *Optics Express*, *19*(11), 10387-10409. https://doi.org/10.1364/OE.19.010387
34. Yuan, Z. L., Shields, A. J., & Dynes, J. F. (2018). Quantum key distribution over 421 km of standard telecom fiber. *Nature Photonics*, *12*, 400-405. https://doi.org/10.1038/s41566-018-0192-4
35. Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., ... & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*, 43-47. https://doi.org/10.1038/nature23655
36. Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information*, *3*(1), 1-13. https://doi.org/10.1038/s41534-017-0031-5
37. Renner, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information*, *6*(01), 1-127. https://doi.org/10.1142/S0219749908003256
38. Takesue, H., Sasaki, T., Tamaki, K., & Koashi, M. (2015). Experimental quantum key distribution without monitoring signal disturbance. *Nature Photonics*, *9*, 827-831. https://doi.org/10.1038/nphoton.2015.232
39. Lucamarini, M., Roberts, G. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*, 400-403. https://doi.org/10.1038/s41586-018-0066-6
40. Zou, X., Qian, L., & Tang, Y. (2020). Quantum key distribution networks in metropolitan areas: A review. *IEEE Access*, *8*, 90225-90241. https://doi.org/10.1109/ACCESS.2020.2994524
41. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, *2*, 16025. https://doi.org/10.1038/npjqi.2016.25
42. Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... & Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, *11*(7), 075001. https://doi.org/10.1088/1367-2630/11/7/075001
43. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2015). Efficient decoy-state quantum key distribution with quantified security. *Optics Express*, *23*(7), 8372-8391. https://doi.org/10.1364/OE.23.008372
44. Wang, S., Chen, W., Yin, Z. Q., Li, H. W., He, D. Y., Zhou, Z., ... & Han, Z. F. (2014). Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express*, *22*(18), 21739-21756. https://doi.org/10.1364/OE.22.021739
45. Guan, J. Y., Liu, W. Y., Li, Y. H., Liao, S. K., Cai, W. Q., Yin, J., ... & Pan, J. W. (2021). Quantum key distribution on a network of ground stations and satellites. *Nature Photonics*, *15*(8), 617-622. https://doi.org/10.1038/s41566-021-00835-1
46. Elkouss, D., Leverrier, A., Alleaume, R., & Boutros, J. J. (2009). Efficient reconciliation protocol for discrete-variable quantum key distribution. *IEEE Transactions on Information Theory*, *55*(10), 4678-4685. https://doi.org/10.1109/TIT.2009.2025545
47. Zhang, Z., Ding, Y., & Zhao, Q. (2020). Machine learning-enhanced post-processing in quantum key distribution. *Quantum Science and Technology*, *5*(4),

045013. https://doi.org/10.1088/2058-9565/aba315

48. Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., ... & Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, *9*(3), 163-168. https://doi.org/10.1038/nphoton.2014.327
49. Tamaki, K., Lo, H. K., Fung, C. H. F., & Qi, B. (2014). Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Physical Review A*, *90*(5), 052314. https://doi.org/10.1103/PhysRevA.90.052314
50. Yin, H. L., Fu, Y., Tang, Y. L., Liu, Y., Chen, S. J., Xie, Y., ... & Pan, J. W. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, *117*(19), 190501. https://doi.org/10.1103/PhysRevLett.117.190501
51. Takeoka, M., Guha, S., & Wilde, M. M. (2014). Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, *5*, 5235. https://doi.org/10.1038/ncomms6235
52. Cao, X. Y., Yu, Z. W., & Wang, X. B. (2015). Improving the key rate of measurement-device-independent quantum key distribution with heralded single-photon sources. *Physical Review A*, *92*(2), 022336. https://doi.org/10.1103/PhysRevA.92.022336
53. Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., ... & Zbinden, H. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, *121*(19), 190502. https://doi.org/10.1103/PhysRevLett.121.190502
54. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*(7705), 400-403. https://doi.org/10.1038/s41586-018-0066-6
55. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, *8*, 15043. https://doi.org/10.1038/ncomms15043
56. Tamaki, K., Curty, M., Kato, G., Lo, H. K., & Azuma, K. (2018). Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, *97*(2), 022308. https://doi.org/10.1103/PhysRevA.97.022308
57. Sidhu, J. S., Kok, P., Oi, D. K. L., & Brougham, T. (2021). Finite-size effects in practical quantum key distribution. *Quantum Science and Technology*, *6*(4), 045012. https://doi.org/10.1088/2058-9565/ac1e7c
58. Zhang, Y., Yu, Z. W., & Wang, X. B. (2017). Semidefinite programming for device-independent quantum key distribution. *Physical Review A*, *95*(4), 042309. https://doi.org/10.1103/PhysRevA.95.042309
59. Curty, M., Xu, F., Cui, C., Lim, C. C. W., Tamaki, K., & Lo, H. K. (2019). Simple security analysis of quantum key distribution. *npj Quantum Information*, *5*, 15. https://doi.org/10.1038/s41534-019-0124-4
60. Laudenbach, F., Pacher, C., Fung, C. H. F., Poppe, A., Peev, M., Schrenk, B., ... & Huber, M. (2018). Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, *1*(1), 1800011. https://doi.org/10.1002/qute.201800011
61. Upadhyay, P., & Kumar, A. (2022). Satellite-based quantum key distribution: A survey. *Optical Fiber Technology*, *69*, 102898. https://doi.org/10.1016/j.yofte.2021.102898
62. Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, *108*(13), 130503.

https://doi.org/10.1103/PhysRevLett.108.130503

63. Yin, H. L., Chen, T. Y., Yu, Z. W., Liu, H., You, L. X., Zhou, Y. H., ... & Pan, J. W. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, *117*(19), 190501. https://doi.org/10.1103/PhysRevLett.117.190501
64. Vedovato, F., Agnesi, C., Scriminich, F., Santamato, A., Calarco, T., & Vallone, G. (2022). Experimental measurement-device-independent quantum key distribution with imperfect detectors. *Quantum Science and Technology*, *7*(4), 045004. https://doi.org/10.1088/2058-9565/ac81b5
65. Jennewein, T., & Higgins, B. (2013). The quantum space race. *Physics World*, *26*(3), 52-56. https://doi.org/10.1088/2058-7058/26/3/36
66. Hughes, R. J., Nordholt, J. E., Derkacs, D., & Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, *4*, 43. https://doi.org/10.1088/1367-2630/4/1/343
67. Lucio-Martinez, I., Chan, P., Mo, X., Hosier, S., & Tittel, W. (2009). Proof-of-concept of real-world quantum key distribution with quantum frames. *New Journal of Physics*, *11*(9), 095001. https://doi.org/10.1088/1367-2630/11/9/095001
68. Brassard, G., & Raymond-Robichaud, P. (2018). Can quantum mechanics be considered complete? *The European Physical Journal D*, *72*, 229. https://doi.org/10.1140/epjd/e2018-90257-3
69. Chen, Y. A., Zhang, Q., Chen, T. Y., Cai, W. Q., Liao, S. K., Zhang, J., ... & Pan, J. W. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, *589*(7841), 214-219. https://doi.org/10.1038/s41586-020-03093-8
70. Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., ... & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*(7670), 43-47. https://doi.org/10.1038/nature23655
71. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*(7705), 400-403. https://doi.org/10.1038/s41586-018-0066-6
72. Qi, B., Lougovski, P., Pooser, R., Grice, W., & Bobrek, M. (2015). Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, *5*(4), 041009. https://doi.org/10.1103/PhysRevX.5.041009
73. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., & Diamanti, E. (2013). Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, *7*(5), 378-381. https://doi.org/10.1038/nphoton.2013.63
74. Usenko, V. C., & Filip, R. (2016). Trusted noise in continuous-variable quantum key distribution: A threat and a defense. *Entropy*, *18*(1), 20. https://doi.org/10.3390/e18010020
75. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, *8*, 15043. https://doi.org/10.1038/ncomms15043
76. Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information*, *3*, 30. https://doi.org/10.1038/s41534-017-0031-5
77. Bacco, D., Da Lio, B., Sanzaro, M., & Oxenløwe, L. K. (2019). Boosting the secret key rate in a shared quantum and classical fibre communication system. *Communications Physics*, *2*, 140. https://doi.org/10.1038/s42005-019-0246-6

78. Zhuang, Q., Zhang, Z., Preskill, J., & Shapiro, J. H. (2020). Physical-layer authentication over quantum channels using classical keys. *Nature Communications*, *11*, 2908. https://doi.org/10.1038/s41467-020-16688-7

79. Xu, F., Curty, M., Qi, B., & Lo, H. K. (2020). Practical aspects of measurement-device-independent quantum key distribution. *npj Quantum Information*, *6*, 82. https://doi.org/10.1038/s41534-020-00320-7

80. Li, Y. H., Liao, S. K., Tang, Y. L., Zhang, Q., & Pan, J. W. (2021). Quantum network for future information infrastructure. *National Science Review*, *8*(10), nwab113. https://doi.org/10.1093/nsr/nwab113

81. Diamanti, E., & Lo, H. K. (2016). Quantum cryptography with continuous variables: A review. *Reports on Progress in Physics*, *80*(1), 016001. https://doi.org/10.1088/1361-6633/80/1/016001

82. Ma, X., Qi, B., Zhao, Y., & Lo, H. K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, *72*(1), 012326. https://doi.org/10.1103/PhysRevA.72.012326

83. Cai, Y., Zhou, Y., Yin, Z. Q., & Chen, Z. B. (2021). Entanglement-based quantum communication with atomic ensembles. *Nature Reviews Physics*, *3*, 570-588. https://doi.org/10.1038/s42254-021-00324-4

84. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P., & Furusawa, A. (2015). Hybrid discrete- and continuous-variable quantum information. *Nature Physics*, *11*(9), 713-719. https://doi.org/10.1038/nphys3410

85. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., & Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, *73*(2), 022320. https://doi.org/10.1103/PhysRevA.73.022320

86. Tang, Z., Liao, Z., Yin, H., et al. (2016). Source attack immunity in quantum key distribution with untrusted sources. *Physical Review A*, *94*(3), 032317. https://doi.org/10.1103/PhysRevA.94.032317

87. Curty, M., Ma, X., & Qi, B. (2010). Passive decoy-state quantum key distribution with practical light sources. *Physical Review A*, *81*(2), 022310. https://doi.org/10.1103/PhysRevA.81.022310

88. Li, Y., Zeng, P., Liu, Y., et al. (2023). Metropolitan quantum cryptography network with quantum-classical multiplexing. *Light: Science & Applications*, *12*(1), 1-8. https://doi.org/10.1038/s41377-022-01030-5

89. Lucamarini, M., Fröhlich, B., Dynes, J. F., & Shields, A. J. (2015). Secure quantum key distribution with imperfect devices. *Nature Photonics*, *9*(6), 362-367. https://doi.org/10.1038/nphoton.2015.76

90. Pirandola, S. (2019). End-to-end capacities of a quantum communication network. *Communications Physics*, *2*, 51. https://doi.org/10.1038/s42005-019-0147-8

91. Nam, S. W., Korzh, B., et al. (2022). Ultra-low-noise superconducting nanowire single-photon detectors for quantum communication. *Nature Communications*, *13*(1), 1-9. https://doi.org/10.1038/s41467-022-30537-z

92. Bunandar, D., Lentine, A. L., Lee, C., et al. (2018). Metropolitan quantum key distribution with silicon photonics. *Physical Review X*, *8*(2), 021009. https://doi.org/10.1103/PhysRevX.8.021009

93. Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2010). Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. *Applied Physics Letters*, *98*(23), 231104. https://doi.org/10.1063/1.3442394

94. Shibata, H., Honjo, T., & Tamaki, K. (2014). Efficient detection of quantum key distribution using superconducting

nanowire single-photon detectors. *Optics Letters*, *39*(17), 5078-5081. https://doi.org/10.1364/OL.39.005078

95. Kumar, R., Qin, H., & Alléaume, R. (2015). Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics*, *17*(4), 043027. https://doi.org/10.1088/1367-2630/17/4/043027
96. Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412), eaam9288. https://doi.org/10.1126/science.aam9288
97. Li, W., Zhu, F., Guan, J. Y., et al. (2020). Experimental quantum key distribution network with software-defined networking. *npj Quantum Information*, *6*, 1-6. https://doi.org/10.1038/s41534-020-0253-2
98. Papernov, A., Zeilinger, A., et al. (2022). Entanglement-based quantum key distribution over 400 km fiber. *Physical Review Letters*, *128*(18), 180502. https://doi.org/10.1103/PhysRevLett.128.180502
99. Bai, X., Ma, H. Q., Jiang, C., et al. (2023). High-rate field test of satellite-to-ground QKD. *Nature*, *617*(7960), 74-79. https://doi.org/10.1038/s41586-023-05997-y
100. Wang, S., Chen, W., Yin, Z. Q., et al. (2023). Toward satellite-based global QKD: Experimental progress and challenges. *npj Quantum Information*, *9*, 12. https://doi.org/10.1038/s41534-023-00723-9