INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

QUANTUM KEY DISTRIBUTION IN OPTICAL FIBER AND FREE-SPACE NETWORKS: PROTOCOLS, SECURITY ANALYSIS, IMPLEMENTATION CHALLENGES, AND EMERGING DIRECTIONS

[1*]Diwakar Shrivastava, [1]Poonam Singh, [1]Gaurav Kumar Pandey, [1]Bhuprabha Bharti, [1]Ayushi Sharma

[1]Department of Computer Science & Engineering, Hindustan College of Science & Technology, Mathura, India

Abstract: **Quantum Key Distribution (QKD) constitutes one of the most profound practical applications of quantum mechanics, enabling two parties to exchange cryptographic keys whose security is guaranteed by the fundamental laws of physics rather than the assumed computational hardness of mathematical problems. As quantum computing capabilities continue to advance, classical public-key infrastructure faces an existential threat, rendering QKD a critical component of post-quantum secure communication architectures. This paper presents a comprehensive survey of QKD spanning foundational protocols, rigorous security proofs, hardware implementation challenges, deployment experiences across metropolitan fiber networks, and recent satellite-based experiments. We analyze the BB84, E91, B92, SARG04, continuous-variable, measurement-device-independent (MDI-QKD), and twin-field (TF-QKD) protocols in depth, examining their security assumptions, achievable key rates, and practical limitations. Particular attention is given to side-channel vulnerabilities in realistic implementations, decoy-state methods for mitigating photon-number-splitting attacks, and finite-key security analysis. We review key performance benchmarks from commercial systems and discuss integration with classical network infrastructure. The paper concludes by identifying open challenges in quantum repeater development, satellite QKD scalability, and standardization efforts essential for large-scale deployment.**

Index Terms: **quantum key distribution, BB84 protocol, continuous-variable QKD, measurement-device-independent QKD, twin-field QKD, decoy-state method, quantum cryptography, quantum networks, photon number splitting, satellite QKD**

1. INTRODUCTION

The security of modern digital communications rests almost entirely on the assumed computational intractability of problems such as integer factorization and discrete logarithm computation. Public-key schemes including RSA, DSA, and elliptic-curve cryptography protect the overwhelming majority of internet traffic and financial transactions globally. However, the emergence of large-scale quantum computers capable of executing Shor's algorithm threatens this foundation: an adversary equipped with a sufficiently powerful quantum processor could break RSA-2048 encryption in hours rather than the billions of years required by classical hardware [1, 2].

Quantum Key Distribution offers a fundamentally different security paradigm. Rather than basing security on unproven computational assumptions, QKD derives its guarantees directly from physical laws - specifically, the no-cloning theorem and the measurement disturbance principle inherent in quantum mechanics [3, 4]. An eavesdropper, commonly denoted Eve, cannot intercept quantum states transmitted between Alice and Bob without introducing detectable disturbances. When the quantum bit error rate (QBER) remains below a protocol-specific threshold, Alice and Bob can be statistically certain that no eavesdropper has acquired significant information about their raw key material [5, 6].

The field of QKD began with the seminal BB84 protocol proposed by Bennett and Brassard in 1984, which exploited the non-orthogonality of quantum states and the uncertainty principle to prevent eavesdropping [1]. Since then, the landscape has grown enormously. Ekert proposed an entanglement-based protocol in 1991 exploiting Bell inequalities [2], while continuous-variable (CV) approaches emerged in the early 2000s, enabling detection with conventional homodyne and heterodyne receivers rather than single-photon detectors [19, 20]. More recently, MDI-QKD [9] and TF-QKD [14] have extended achievable distances significantly while eliminating critical detector-side vulnerabilities.

Despite these theoretical advances, real-world deployment faces numerous challenges. Photon loss in optical fiber limits transmission distance; detector inefficiencies reduce key rates; timing jitter introduces errors; and multi-photon pulses from practical laser sources open attack vectors such as the photon-number-splitting (PNS) attack [10, 17]. Additionally, commercial QKD systems have been shown to harbor implementation-specific vulnerabilities exploited by Trojan horse attacks [40, 41], necessitating hardware-level countermeasures.

This paper aims to provide researchers, engineers, and security professionals with a consolidated reference encompassing the theoretical underpinnings, security analysis methodologies, practical implementation considerations, and current deployment status of QKD technology. The remainder of this paper is organized as follows. Section 2 reviews foundational protocols. Section 3 addresses security proofs and key metrics. Section 4 analyzes attack models and countermeasures. Section 5 discusses implementation

hardware. Section 6 surveys real-world deployments. Section 7 examines satellite-based QKD. Section 8 identifies open challenges and future directions. Section 9 concludes.

2. QKD PROTOCOL LANDSCAPE

2.1 Prepare-and-Measure Protocols

The BB84 protocol encodes classical bits onto the polarization of individual photons using two conjugate bases: rectilinear (horizontal/vertical) and diagonal (45 degrees/135 degrees) [1]. Alice randomly selects a basis for each bit and prepares photons accordingly; Bob randomly selects measurement bases. After quantum transmission, they publicly compare bases and retain only the bits where their choices matched - a procedure known as basis sifting - yielding a sifted key of approximately half the raw key length. The non-commutativity of the two measurement bases ensures that any eavesdropping attempt by Eve inevitably introduces a QBER of at least 25% in the intercepted fraction, making her presence detectable [4, 5].

The B92 protocol simplifies BB84 by using only two non-orthogonal states, reducing hardware complexity at the cost of lower efficiency and somewhat narrower security margins [3]. The SARG04 protocol modifies the classical sifting procedure of BB84, making it robust against photon-number-splitting attacks when weak coherent pulse sources are used, even without decoy states [10, 17].

2.2 Entanglement-Based Protocols

Ekert's E91 protocol distributes entangled photon pairs to Alice and Bob; each measures in a randomly chosen basis [2]. Security is certified through the violation of Bell inequalities (CHSH inequality), confirming that the shared states cannot be explained by a local hidden variable model and hence that Eve holds no information about the outcomes. E91 is particularly significant from a foundational perspective, connecting quantum key distribution to the deepest principles of quantum nonlocality.

Device-independent QKD (DI-QKD) extends this idea by basing security entirely on observed Bell inequality violations, with no trust placed in the measurement devices themselves [30]. While theoretically very powerful, DI-QKD requires near-unity detection efficiencies and remains experimentally demanding. Loophole-free Bell tests accomplished around 2015 represent critical prerequisites for practical DI-QKD [31].

2.3 Continuous-Variable QKD

Rather than encoding information in discrete quantum states of individual photons, CV-QKD modulates the quadrature amplitudes (amplitude and phase) of coherent or squeezed optical states and detects them with homodyne or heterodyne receivers [19, 20]. This approach is compatible with standard telecommunications infrastructure including erbium-doped fiber amplifiers and wavelength-division multiplexing, making it attractive for integration into existing fiber networks.

The GG02 protocol, introduced by Grosshans and Grangier, uses Gaussian-modulated coherent states and reverse reconciliation to achieve positive secret key rates even under high-loss conditions [38, 39]. Security proofs for Gaussian CV-QKD have been rigorously established, with Leverrier providing an unconditional composable security proof via a Gaussian de Finetti reduction [21]. Practical demonstrations over metropolitan fiber distances have confirmed the viability of CV-QKD as a complement to discrete-variable systems [42].

2.4 Measurement-Device-Independent and Twin-Field QKD

MDI-QKD eliminates all detector-side vulnerabilities by having Alice and Bob each send quantum states to an untrusted relay node that performs a Bell-state measurement [9]. Since the relay's measurement result only reveals which Bell state was projected - providing no information about the individual states - the security of the protocol is completely independent of the relay's honesty or the detectors' characteristics. MDI-QKD has been experimentally demonstrated over distances exceeding 200 km [43, 44].

Twin-field QKD achieves a fundamentally superior key-rate versus distance scaling by having Alice and Bob encode keys onto the global phase of optical fields sent to a central station, which performs single-photon interference [14]. Unlike MDI-QKD whose key rate scales as O(n^2) in channel transmittance n, TF-QKD scales as O(n) - the same as a quantum repeater - making it possible to achieve positive key rates at distances previously unattainable without repeaters. Experimental demonstrations have exceeded 830 km in optical fiber [36].

TABLE 1. COMPARATIVE OVERVIEW OF MAJOR QKD PROTOCOLS

Protocol	Photon Source	Unconditional Security	Max Range	Key Features
BB84	**Single photon**	**Yes**	**~50 km**	**Basis sifting, privacy amplification**
E91	**Entangled pairs**	**Yes**	**~100 km**	**Bell inequality violation test**
B92	**Two non-orth. states**	**Partial**	**~30 km**	**Simplified BB84 variant**
SARG04	**4 non-orth. states**	**Yes**	**~80 km**	**PNS attack resistant**
CV-QKD	**Coherent/squeezed**	**Yes**	**~100 km**	**Gaussian modulation**
MDI-QKD	**Entangled/single**	**Yes**	**~200 km**	**Measurement-device-independent**
TF-QKD	**Phase-encoded**	**Yes**	**~500 km**	**Twin-field encoding**

3. SECURITY ANALYSIS AND KEY RATE METRICS

3.1 Information-Theoretic Security Framework

Rigorous security proofs for QKD are formulated within a composable security framework, which guarantees that a QKD-generated key remains secure when used as input to other cryptographic protocols [29, 30]. The composable security definition requires that the output key be statistically indistinguishable - up to a small failure probability epsilon - from a uniformly random string that is independent of Eve's quantum state. Shor and Preskill's proof [4], building on Lo and Chau's earlier result [11], established unconditional security for BB84 by connecting it to quantum error-correcting codes. Renner's generalized framework using smooth min-entropy extended these results to finite key lengths [29].

The secret key rate R per channel use is bounded by R >= Q1(1 - h(e1)) - Q_mu * h(E_mu), where Q1 is the single-photon gain, e1 is the single-photon error rate, E_mu is the overall QBER, and h(.) is the binary entropy function [13, 18]. In practice, finite-key corrections are significant: for a security parameter epsilon = 10^-10 and block length of 10^8 bits, finite-key effects reduce the asymptotic key rate by 30-50% [13, 45].

3.2 Decoy-State Method

Practical QKD systems use attenuated laser pulses rather than true single-photon sources. Weak coherent pulses follow a Poissonian photon-number distribution, meaning a non-negligible fraction of pulses contain two or more photons. An eavesdropper can suppress single-photon pulses and measure multi-photon pulses without introducing errors - the photon-number-splitting attack [10]. Hwang proposed the decoy-state method to circumvent this: Alice randomly varies the mean photon number mu among multiple intensity settings (signal, decoy, vacuum) [17]. Statistical comparison of detection rates across these settings allows Alice and Bob to tightly bound the single-photon gain Q1 and error rate e1, enabling the use of realistic laser sources with security approaching that of true single-photon implementations [18, 45].

3.3 Finite-Key Analysis

Asymptotic security proofs assume infinitely long raw keys, a condition never met in practice. Finite-key analysis addresses the statistical fluctuations that arise when parameter estimation is performed on finite data samples [13]. Tomamichel and colleagues showed that the tightest finite-key bounds employ smooth min-entropy and lead to security proofs that are tight within a small multiplicative constant of the asymptotic rate [13]. For MDI-QKD, finite-key bounds have been derived accounting for statistical uncertainties in both the sifted key and the parameter estimation blocks [45].

4. ATTACK MODELS AND COUNTERMEASURES

Despite the information-theoretic security of idealized QKD, practical implementations introduce deviations from the theoretical model that can be exploited by sophisticated adversaries. A comprehensive taxonomy of attacks and the corresponding countermeasures is essential for evaluating real-world deployment security [16, 40, 41].

TABLE 2. ATTACK MODELS IN PRACTICAL QKD SYSTEMS AND ASSOCIATED COUNTERMEASURES

Attack Type	Mechanism	Threat Level	Countermeasure
Photon Number Splitting (PNS)	**Intercept multi-photon pulses**	**High for weak coherent sources**	**Decoy state method, low mean photon number**
Intercept-Resend	**Measure and resend photons**	**Introduces 25% QBER**	**Monitor QBER threshold; abort if > 11%**
Trojan Horse	**Inject bright pulses into Alice**	**Practical with optical equipment**	**Optical isolators, wavelength filters**
Side-Channel	**Exploit detector imperfections**	**Real hardware vulnerabilities**	**MDI-QKD, device-independent QKD**
Detector Blinding	**Saturate single-photon detectors**	**Demonstrated experimentally**	**Randomize detection windows, patch detectors**
Man-in-the-Middle	**Full channel interception**	**Requires no authenticated channel**	**Information-theoretic authentication (Wegman-Carter)**

The detector-blinding attack, experimentally demonstrated by Lydersen and colleagues [40], represents one of the most significant practical vulnerabilities discovered in commercial QKD hardware. By flooding single-photon avalanche diode (SPAD) detectors with bright continuous illumination, the adversary forces them into a linear, non-quantum operating regime, enabling click-on-demand control through carefully timed optical pulses. This completely circumvents quantum security guarantees. MDI-QKD inherently eliminates this class of attacks by removing trust from measurement devices [9]. In systems where MDI-QKD is not deployed, hardware-level countermeasures include randomized detection-window timing, optical attenuation at detector inputs, and real-time monitoring of detector count rates for anomalous behavior [41].

The Trojan horse attack exploits the bidirectional nature of optical components: an adversary injects a bright probe pulse into Alice's or Bob's apparatus and analyzes the reflected light, potentially reading out basis or state information [40]. Defense requires high-isolation optical circulators, narrowband wavelength filters, and optical power monitors at device ingress ports. The SECOQC and Tokyo QKD network implementations incorporated such countermeasures as standard practice [48, 50].

5. IMPLEMENTATION HARDWARE

5.1 Single-Photon Sources and Detectors

Ideal QKD requires on-demand single-photon sources - devices that emit exactly one photon per trigger pulse. While semiconductor quantum dots, nitrogen-vacancy centers in diamond, and single molecules have been investigated as deterministic single-photon emitters, none yet achieves the combination of high emission rate, narrow linewidth, near-unity efficiency, and room-temperature operation required for field deployment [7, 15]. In practice, attenuated laser pulses with mean photon number mu ~ 0.1-0.5 per pulse, combined with the decoy-state method [17, 18], remain the dominant source technology in commercial systems.

On the detection side, silicon single-photon avalanche diodes (Si-SPADs) offer high efficiency (~65%) at wavelengths below 900 nm, while InGaAs SPADs operate in the telecom O- and C-bands (1310 and 1550 nm) with efficiencies of 25-30% and dark count rates of ~1,000 cps. Superconducting nanowire single-photon detectors (SNSPDs) achieve efficiencies exceeding 90%, timing jitters below 30 ps, and dark count rates below 1 cps, making them the preferred choice for long-distance experiments [33, 34], though their requirement for cryogenic cooling (~2.5 K) limits field deployment flexibility.

5.2 Optical Fiber and Free-Space Channels

Standard single-mode fiber at 1550 nm exhibits loss of approximately 0.2 dB/km, limiting point-to-point QKD without repeaters to roughly 300-400 km with state-of-the-art SNSPDs and TF-QKD [14, 36]. Ultra-low-loss fiber (~0.15 dB/km) and hollow-core photonic bandgap fibers (~0.1 dB/km) offer marginal improvements [7]. In free-space channels, atmospheric turbulence, beam wander, and pointing errors introduce additional loss and noise; adaptive optics and fast steering mirrors mitigate these effects in satellite QKD links [22, 23].

5.3 Timing Synchronization and Wavelength Multiplexing

Precise timing synchronization between Alice and Bob is critical: timing jitter directly increases QBER. GPS-disciplined oscillators and optical clock distribution via classical wavelength channels enable sub-100 ps synchronization in deployed networks [47]. Wavelength-division multiplexing allows QKD signals to coexist with classical data channels on the same fiber; however, spontaneous Raman scattering from high-power classical channels introduces background noise photons into QKD detector windows, requiring careful selection of QKD wavelengths and power budgets [37, 47].

6. REAL-WORLD DEPLOYMENTS AND COMMERCIAL SYSTEMS

QKD has transitioned from laboratory demonstrations to metropolitan network deployments across multiple continents. The SECOQC network in Vienna (2008) was among the first multi-node networks, connecting six nodes over 200 km of standard telecom fiber using a trusted-node relay architecture [48]. The Tokyo QKD network (2010) achieved sustained key distribution across a 45-km fiber loop, integrating QKD key material into a real-time encrypted video conferencing application [50]. China's quantum communication backbone, spanning over 4,600 km between Beijing and Shanghai, combines fiber-based QKD segments interconnected via trusted nodes and linked to the Micius satellite for ground-to-satellite key exchange [26].

TABLE 3. PERFORMANCE METRICS OF SELECTED COMMERCIAL AND RESEARCH QKD SYSTEMS

System/Vendor	Protocol Used	Key Rate	Distance	Notes
ID Quantique (Clavis3)	**BB84 + decoy**	**1 Mbps**	**Up to 100 km**	**ETSI-compliant, AES-256 integration**
Toshiba QKD	**BB84 variant**	**10 Mbps**	**Up to 120 km**	**High-speed, WDM compatible**
QuantumCTek	**BB84 + MDI**	**10 Mbps**	**Up to 200 km**	**National backbone deployment**
MagiQ Technologies	**BB84**	**100 kbps**	**Up to 50 km**	**Enterprise-grade appliance**
Huawei QKD	**CV-QKD**	**1 Mbps**	**Up to 80 km**	**Telecom network integration**
SK Telecom/IDQ	**BB84 + relay**	**Variable**	**Unlimited (relay)**	**Seoul metro network**

The commercial QKD market has grown substantially, with vendors including ID Quantique (Switzerland), Toshiba (UK/Japan), QuantumCTek (China), MagiQ Technologies (USA), and SK Telecom (South Korea) offering rack-mounted QKD appliances for enterprise and government customers [7, 15]. Key rates of 1-10 Mbps over metropolitan distances are now routinely achievable, sufficient for symmetric key refresh of AES-256 encrypted links. Integration with classical network equipment, including optical transport nodes and software-defined networking controllers, is advancing through standardization efforts in ETSI, ITU-T, and ISO/IEC [15, 16].

7. SATELLITE-BASED QUANTUM KEY DISTRIBUTION

Extending QKD beyond metropolitan scales requires either quantum repeaters or free-space optical links via satellite. The Micius satellite, launched by China in 2016, demonstrated the feasibility of satellite-to-ground QKD [23], satellite-to-ground entanglement distribution [22], and ground-to-satellite teleportation. Over a 1,200-km entanglement distribution link, a CHSH parameter S = 2.37 +/- 0.09 was measured, exceeding the classical bound of 2 with high statistical significance [22]. Quantum key distribution was achieved at night with a secure key rate of ~1 kbps from a 500-km orbit, enabling encrypted video calls between Beijing and Vienna [26].

The key technical challenges in satellite QKD include: (i) high free-space path loss (~40 dB at 500 km altitude), mitigated by large-aperture ground telescopes (>=1 m); (ii) atmospheric turbulence, addressed through adaptive optics; (iii) narrow acquisition and tracking windows during low-earth-orbit passes of ~300 s per pass; and (iv) daytime operation, which requires extremely tight spatial filtering and narrow-band spectral filtering to suppress solar background [23, 27]. Medium-earth-orbit and geostationary platforms would dramatically improve duty cycle but demand even higher-sensitivity detection [27].

Quantum repeaters, which use entanglement swapping and purification to extend QKD range without trusted nodes, remain a major research frontier [24, 25]. Current quantum memory technologies - including rare-earth ion-doped crystals, atomic ensembles, and nitrogen-vacancy centers in diamond - achieve storage times of milliseconds to seconds with limited multimode capacity, insufficient for continental-scale repeater chains [25]. Nonetheless, incremental progress in memory-assisted MDI-QKD represents a promising intermediate step toward full repeater networks.

8. BB84 PROTOCOL FLOWCHART

Figure 1 presents a step-by-step description of the BB84 QKD protocol from photon preparation to final key establishment.

STEP 1: Alice generates a random bit string and a random basis string using rectilinear (+) or diagonal (x) bases.
STEP 2: Alice encodes each bit using the selected basis and transmits photons over the quantum channel.
STEP 3: Bob randomly selects measurement bases and measures each incoming photon independently.
STEP 4: Alice and Bob exchange basis choices over an authenticated classical channel (basis sifting).
STEP 5: Discard mismatched-basis bits. The sifted key retains approximately 50% of raw bits.
STEP 6: Error Estimation - Publicly compare a random subset of sifted key bits to estimate QBER.
Decision: If QBER < 11% threshold, continue. Otherwise, abort and restart.
STEP 7: Information Reconciliation - Apply Cascade or LDPC-based error correction over classical channel.
STEP 8: Privacy Amplification - Apply universal hash function to reduce Eve's information to negligible levels.
RESULT: SECRET KEY ESTABLISHED - Cryptographically secure, information-theoretically proven.

9. OPEN CHALLENGES AND FUTURE DIRECTIONS

Several critical challenges must be addressed before QKD can achieve widespread deployment at national and global scales. First, quantum repeater technology requires substantial advances in quantum memory efficiency, coherence time, and multimode storage capacity. Current demonstrations are limited to short segments; continental-scale repeater networks require coherence across memory modules spanning hundreds of kilometers and coordinated entanglement purification protocols [24, 25].

Second, integration with post-quantum cryptography (PQC) standards - including those recently standardized by NIST (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+) - is essential. Hybrid quantum-classical security architectures that combine PQC algorithms for authentication with QKD-generated keys for symmetric encryption provide defense in depth against both quantum and classical adversaries [15, 16].

Third, standardization remains fragmented. While ETSI has published QKD interface specifications and ITU-T Study Group 17 is developing security requirements, interoperability between equipment from different vendors is not yet guaranteed. The development of open QKD application programming interfaces (APIs) and reference implementations is a prerequisite for market growth [15].

Fourth, the cost and form factor of QKD hardware must decrease substantially. Today's rack-mounted systems cost on the order of tens of thousands of US dollars per endpoint. Silicon photonic integration of QKD components - including laser drivers, electro-optic modulators, and single-photon detectors - onto CMOS-compatible chips offers a pathway to dramatically reduced cost and size [7, 15]. Early demonstrations of chip-scale QKD transmitters and receivers have achieved key rates of hundreds of kbps over metropolitan distances, validating this approach.

Finally, device-independent QKD, while providing the strongest possible security guarantees, requires loophole-free Bell tests with near-unity detection efficiency - a condition that remains experimentally demanding even with the best available SNSPDs. Measurement-device-independent QKD represents a practical intermediate step, offering immunity to all detector-side attacks while remaining implementable with current hardware [9, 43, 44].

10. CONCLUSION

Quantum Key Distribution stands at the intersection of fundamental physics and applied cryptographic engineering. Over four decades since the original BB84 proposal, the field has matured from proof-of-concept laboratory experiments to metropolitan network deployments, intercontinental satellite demonstrations, and a nascent commercial industry. The theoretical security foundation - grounded in the laws of quantum mechanics rather than unproven computational assumptions - remains unimpeachable: no quantum or classical algorithm can break QKD without revealing its presence through detectable physical disturbances.

At the same time, bridging the gap between theoretical ideality and physical implementation demands rigorous attention to side-channel vulnerabilities, finite-key effects, hardware imperfections, and system-level integration challenges. Decoy-state methods and MDI-QKD have addressed the most critical practical attack surfaces. TF-QKD has pushed achievable distances to 830 km without repeaters. Satellite QKD has demonstrated global-scale entanglement distribution.

The path forward lies in three parallel directions: advancing quantum repeater technology to eliminate trusted-node relays; integrating QKD into hybrid PQC architectures for defense in depth; and achieving photonic chip-scale integration to dramatically reduce cost and accelerate deployment. As these technologies mature, QKD is poised to become a foundational component of the secure communication infrastructure that will underpin the quantum era.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, pp. 7-11, 2014 (reprint of 1984 ICASSP paper).

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, no. 6, pp. 661-663, 1991.

[3] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 457-475, 2003.

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol. 85, no. 2, pp. 441-444, 2000.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.

[6] V. Scarani et al., "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301-1350, 2009.

[7] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nature Photon., vol. 8, no. 8, pp. 595-604, 2014.

[8] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, p. 130502, 2012.

[9] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, p. 130503, 2012.

[10] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett., vol. 94, no. 23, p. 230503, 2005.

[11] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science, vol. 283, no. 5410, pp. 2050-2056, 1999.

[12] D. Mayers, "Unconditional security in quantum cryptography," J. ACM, vol. 48, no. 3, pp. 351-406, 2001.

[13] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun., vol. 3, p. 634, 2012.

[14] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, no. 7705, pp. 400-403, 2018.

[15] S. Pirandola et al., "Advances in quantum cryptography," Adv. Opt. Photon., vol. 12, no. 4, pp. 1012-1236, 2020.

[16] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys., vol. 92, no. 2, p. 025002, 2020.

[17] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett., vol. 91, no. 5, p. 057901, 2003.

[18] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett., vol. 94, no. 23, p. 230504, 2005.

[19] C. Weedbrook et al., "Gaussian quantum information," Rev. Mod. Phys., vol. 84, no. 2, pp. 621-669, 2012.

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

[21] A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction," Phys. Rev. Lett., vol. 118, no. 20, p. 200501, 2017.

[22] J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers," Science, vol. 356, no. 6343, pp. 1140-1144, 2017.

[23] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, no. 7670, pp. 43-47, 2017.

[24] H.-J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, "Quantum repeaters," Phys. Rev. Lett., vol. 81, no. 26, pp. 5932-5935, 1998.

[25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys., vol. 83, no. 1, pp. 33-80, 2011.

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

[27] A. Huang et al., "Quantum key distribution over double-layer quantum satellite networks," IEEE Trans. Inf. Theory, vol. 67, no. 11, pp. 7225-7243, 2021.

[28] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A, vol. 461, no. 2053, pp. 207-235, 2005.

[29] R. Renner, "Security of quantum key distribution," Int. J. Quantum Inf., vol. 6, no. 1, pp. 1-127, 2008.

[30] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," arXiv:1409.3525, 2014.

[31] T. Lunghi et al., "Self-testing quantum random number generator," Phys. Rev. Lett., vol. 114, no. 15, p. 150501, 2015.

[32] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys., vol. 89, no. 1, p. 015004, 2017.

[33] B. Korzh et al., "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photon., vol. 9, no. 3, pp. 163-168, 2015.

[34] A. Boaron et al., "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett., vol. 121, no. 19, p. 190502, 2018.

[35] M. Minder et al., "Experimental quantum key distribution beyond the repeaterless secret key capacity," Nature Photon., vol. 13, no. 5, pp. 334-338, 2019.

[36] S. Wang et al., "Twin-field quantum key distribution over 830-km fibre," Nature Photon., vol. 16, no. 2, pp. 154-161, 2022.

[37] D. Bunandar et al., "Metropolitan quantum networks," Phys. Rev. X, vol. 8, no. 2, p. 021009, 2018.

[38] P. Jouguet et al., "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nature Photon., vol. 7, no. 5, pp. 378-381, 2013.

[39] V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A, vol. 81, no. 2, p. 022318, 2010.

[40] L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photon., vol. 4, no. 10, pp. 686-689, 2010.

[41] S. Sajeed et al., "Insecurity of detector-device-independent quantum key distribution," Phys. Rev. Lett., vol. 117, no. 25, p. 250505, 2016.

[42] Y. Zhang et al., "Continuous-variable QKD over 50 km commercial fiber," Quantum Sci. Technol., vol. 4, no. 3, p. 035006, 2019.

[43] A. Rubenok et al., "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," Phys. Rev. Lett., vol. 111, no. 13, p. 130501, 2013.

[44] Y. Liu et al., "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 111, no. 13, p. 130502, 2013.

[45] C. C. W. Lim et al., "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A, vol. 89, no. 2, p. 022307, 2014.

[46] Z. Yuan et al., "10-Mb/s quantum key distribution," J. Lightw. Technol., vol. 36, no. 16, pp. 3427-3433, 2018.

[47] J. F. Dynes et al., "Ultra-high bandwidth quantum secured fibre communications," npj Quantum Inf., vol. 2, p. 16009, 2016.

[48] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys., vol. 11, no. 7, p. 075001, 2009.

[49] T.-Y. Chen et al., "Field test of a practical secure communication network with decoy-state quantum cryptography," Opt. Express, vol. 17, no. 8, pp. 6540-6549, 2009.

[50] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express, vol. 19, no. 11, pp. 10387-10409, 2011.