INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

QUANTUM CRYPTOGRAPHY: EMERGING PARADIGMS FOR SECURE COMMUNICATION

Mary Ahino J
Assistant Professor,
Department of Computer Science,
Annai Scholastica Arts and Science College for Women,
Pamban, Tamil Nadu, India.

Abstract:

Quantum cryptography has evolved from a theoretical curiosity into a practically deployable technology for securing communication in an era increasingly threatened by the computational power of quantum computers. Classical public-key cryptosystems, such as RSA and elliptic-curve cryptography, derive their security from computational hardness assumptions that are vulnerable to Shor's algorithm once large-scale fault-tolerant quantum computers become available. Quantum cryptography, and in particular Quantum Key Distribution (QKD), offers information-theoretic security grounded in the laws of quantum mechanics rather than computational complexity. This paper presents a comprehensive review of the foundational principles of quantum cryptography, surveys established QKD protocols including BB84, B92, and E91, and examines emerging paradigms such as Measurement-Device-Independent QKD, Twin-Field QKD, Continuous-Variable QKD, Device-Independent QKD, satellite-based QKD, and quantum repeater networks that are shaping the future "quantum internet." The paper further discusses the complementary role of post-quantum cryptography, practical implementation challenges, real-world deployments, and open research problems. The objective is to provide researchers and practitioners with a structured understanding of how these emerging paradigms collectively advance the goal of provably secure, long-term communication infrastructure.

Keywords: Quantum cryptography, Quantum Key Distribution (QKD), BB84 protocol, post-quantum cryptography, quantum repeaters, quantum internet, device-independent QKD, satellite QKD.

I. Introduction

The security of modern digital communication rests overwhelmingly on classical public-key cryptographic schemes whose strength derives from the presumed intractability of problems such as integer factorization and the discrete logarithm. While these assumptions have withstood decades of classical cryptanalysis, the advent of quantum computing introduces a fundamentally different threat model. Shor's algorithm demonstrates that a sufficiently large, fault-

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

tolerant quantum computer can factor large integers and compute discrete logarithms in polynomial time, effectively breaking RSA, Diffie–Hellman, and elliptic-curve cryptosystems. Although large-scale quantum computers capable of executing Shor's algorithm at cryptographically relevant scales do not yet exist, the "harvest now, decrypt later" threat, in which adversaries record encrypted traffic today for decryption once quantum computers mature, has made the transition toward quantum-resistant security an urgent priority.

Quantum cryptography addresses this challenge from a different angle than post-quantum cryptography. Rather than replacing hard mathematical problems with ones believed to be quantum-resistant, quantum cryptography exploits the physical laws governing quantum systems, such as the no-cloning theorem and the observer effect, to achieve security guarantees that are independent of an adversary's computational power. The most mature application of this approach is Quantum Key Distribution (QKD), which allows two parties to establish a shared secret key whose secrecy can be certified by the laws of physics rather than by unproven computational assumptions.

This paper reviews the theoretical underpinnings of quantum cryptography, traces the evolution of QKD protocols, and provides a structured survey of emerging paradigms that extend QKD beyond its original point-to-point, trusted-node limitations toward device independence, long-distance transmission, and global-scale quantum networks. The remainder of the paper is organized as follows. Section II introduces the fundamental quantum-mechanical principles underlying quantum cryptography. Section III reviews established QKD protocols. Section IV surveys emerging paradigms. Section V discusses applications, Section VI addresses open challenges, Section VII outlines future research directions, and Section VIII concludes the paper.

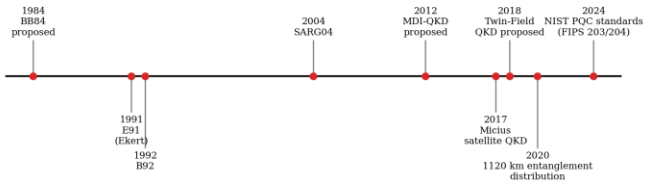

Fig 1: Timeline of major milestones in the development of quantum cryptography, from the original BB84 proposal to recent NIST post-quantum cryptography standards.

II. Fundamentals of Quantum Cryptography

Quantum cryptography derives its security guarantees from three interrelated quantum-mechanical principles.

A. Heisenberg Uncertainty and Non-Orthogonal States

When information is encoded in non-orthogonal quantum states, such as photon polarization states measured in different bases, any attempt by an eavesdropper to measure the state necessarily disturbs it unless the correct measurement basis is known in advance. Because the sender and receiver can

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

statistically detect this disturbance, eavesdropping attempts become observable, transforming a passive interception problem into a detectable physical event.

B. The No-Cloning Theorem

The no-cloning theorem states that an arbitrary unknown quantum state cannot be copied with perfect fidelity. This precludes an eavesdropper from intercepting a quantum bit (qubit), duplicating it, forwarding one copy to the legitimate receiver, and retaining the other for later analysis, a strategy that is trivial against classical signals but physically impossible against quantum ones.

C. Quantum Entanglement

Entangled particle pairs exhibit correlations that cannot be explained by any local hidden-variable theory, as formalized by Bell's inequalities. Entanglement-based protocols exploit violations of Bell inequalities to certify the security of a shared key even when the internal workings of the measurement devices are not trusted, forming the basis of device-independent approaches discussed in Section IV.

Together, these principles allow two communicating parties, conventionally named Alice and Bob, to detect the presence of an eavesdropper, commonly named Eve, and to distill a secret key whose security can be quantified using information-theoretic bounds rather than computational hardness assumptions.

III. Established QKD Protocols

A. BB84 Protocol

Proposed by Bennett and Brassard in 1984, BB84 remains the foundational QKD protocol. Alice encodes random bits onto single photons using one of two conjugate bases, rectilinear or diagonal, and transmits them to Bob, who measures each photon in a randomly chosen basis. After transmission, Alice and Bob publicly compare their basis choices, discarding results where the bases differ, and retain the remaining bits as a raw key. Error estimation on a random subset of the key reveals the presence of eavesdropping, after which error correction and privacy amplification yield a shorter, information-theoretically secure final key.

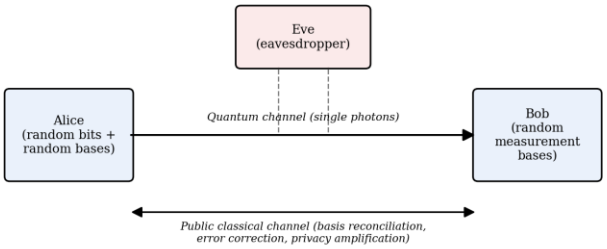

Fig. 2. Schematic of the BB84 quantum key distribution protocol, showing the quantum channel between Alice and Bob, a potential eavesdropper (Eve), and the auxiliary public classical channel used for post-processing.

B. B92 and SARG04

The B92 protocol simplifies BB84 by using only two non-orthogonal states rather than four, reducing implementation complexity at the cost of lower key generation efficiency. SARG04 was later introduced to

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

improve robustness against photon-number-splitting attacks that exploit multi-photon pulses emitted by imperfect single-photon sources, an important consideration for practical weak coherent pulse implementations.

C. E91 (Ekert) Protocol

Ekert's 1991 protocol takes a different approach, distributing entangled photon pairs to Alice and Bob and using violations of Bell's inequality to certify security. Because security follows directly from the observed violation of local realism rather than from assumptions about the source, E91 laid the conceptual groundwork for later device-independent protocols.

Table 1: Comparison of Established QKD Protocols

Protocol	Encoding	Security Basis	Typical Max. Distance	Year
BB84	Photon polarization (4 states, 2 bases)	No-cloning + disturbance detection	~200 km (fiber)	1984
B92	Photon polarization (2 states)	No-cloning + disturbance detection	~100 km (fiber)	1992
E91 (Ekert)	Entangled photon pairs	Bell inequality violation	~100 km (fiber)	1991
SARG04	Photon polarization (4 states)	Robust to photon-number-splitting	~150 km (fiber)	2004

IV. Emerging Paradigms

While BB84-family protocols proved the feasibility of quantum key distribution, practical deployment exposed vulnerabilities in real-world implementations and limitations in transmission distance. The following emerging paradigms address these shortcomings and extend quantum cryptography toward a scalable, trustworthy quantum communication infrastructure.

A. Measurement-Device-Independent QKD (MDI-QKD)

Side-channel attacks that exploit imperfections in detectors, such as detector-blinding attacks, represent one of the most practical threats to deployed QKD systems. MDI-QKD eliminates this attack surface entirely by removing trust in the measurement device. Both Alice and Bob send quantum states to an untrusted intermediate relay that performs a Bell-state measurement and publicly announces the outcome, without ever needing to be trusted itself. Because the relay's measurement results reveal no information about the encoded bits without the participants' bases, security is guaranteed even if the relay is fully controlled by an adversary.

B. Twin-Field QKD (TF-QKD)

Conventional QKD key rates decay exponentially with channel loss, fundamentally limiting achievable distance without trusted intermediate nodes, a bound formalized by the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) rate-loss bound. Twin-Field QKD overcomes this by having Alice and Bob each send phase-randomized weak coherent pulses toward a central untrusted station, where single-photon

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

interference is measured. Because the key rate in TF-QKD scales with the square root of the channel transmittance rather than linearly with transmittance, it enables secure key distribution over metropolitan and even inter-city fiber distances exceeding 500 km without trusted repeaters, effectively surpassing the rate-loss bound applicable to conventional point-to-point QKD.

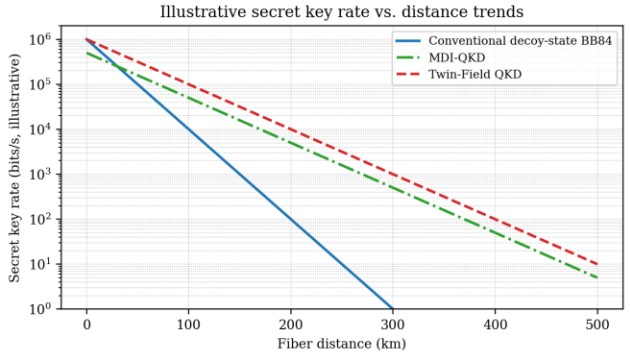

Fig. 3. Illustrative trend of achievable secret key rate versus fiber distance for conventional decoy-state BB84, MDI-QKD, and Twin-Field QKD. Curves are qualitative and intended to show relative scaling behavior rather than measured experimental data.

C. Continuous-Variable QKD (CV-QKD)

Instead of encoding information in discrete photon states, CV-QKD encodes key information in continuous quadrature variables of coherent or squeezed states of light, and uses homodyne or heterodyne detection compatible with standard telecommunications hardware. This compatibility with existing optical infrastructure makes CV-QKD attractive for cost-effective integration into metropolitan fiber networks, though it typically achieves shorter secure distances than discrete-variable protocols due to excess noise sensitivity.

D. Device-Independent QKD (DI-QKD)

DI-QKD represents the strongest security paradigm currently conceivable: it certifies security based solely on the observed statistics of a Bell-inequality violation, without any assumption about the internal workings of the source or measurement devices. Recent experimental demonstrations using loophole-free Bell tests over short distances have validated the feasibility of DI-QKD, although stringent detection-efficiency and loss requirements currently confine it to laboratory-scale distances, motivating ongoing research into loss-tolerant DI-QKD variants.

E. Satellite-Based and Free-Space QKD

Fiber-based QKD suffers exponential signal attenuation, restricting practical single-link distances to a few hundred kilometers. Satellite-based QKD circumvents this limitation by transmitting quantum signals through free space, where atmospheric and vacuum attenuation is significantly lower than fiber loss over comparable distances. China's Micius satellite has demonstrated intercontinental quantum key distribution between ground stations separated by thousands of kilometers, as well as satellite-relayed entanglement distribution, establishing satellite QKD as a viable backbone for global-scale quantum-secured

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

communication when combined with terrestrial fiber networks.

F. Quantum Repeaters and the Quantum Internet

Quantum repeaters aim to overcome fiber-loss limitations without violating the no-cloning theorem by using entanglement swapping and quantum memories to extend entanglement across successive segments of a network, effectively realizing a quantum analogue of classical signal amplification. Successful development of practical, high-fidelity quantum repeaters is widely regarded as the key enabling technology for a future "quantum internet," a global network capable of distributing entanglement and secret keys among arbitrarily distant nodes, supporting applications beyond QKD such as distributed quantum computing and blind quantum computation.

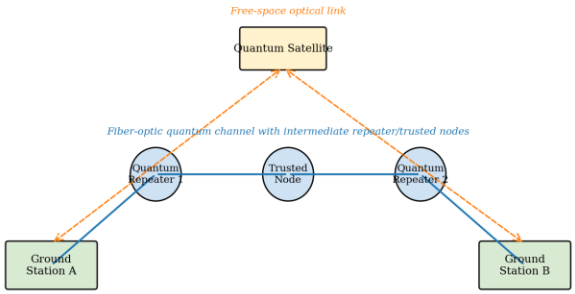

Fig. 4. Illustrative hybrid quantum network architecture combining a satellite free-space link with a terrestrial fiber-optic backbone employing quantum repeater and trusted-node segments.

G. Post-Quantum Cryptography as a Complementary Paradigm

Post-quantum cryptography (PQC) develops classical algorithms, based on lattices, codes, hash functions, and multivariate equations, that are believed to resist attacks from quantum computers while running on existing classical hardware. Although PQC does not offer the information-theoretic guarantees of QKD, its ease of deployment over existing infrastructure makes it a practical near-term complement. The National Institute of Standards and Technology (NIST) has standardized lattice-based schemes such as CRYSTALS-Kyber and CRYSTALS-Dilithium for this purpose. Hybrid architectures that combine QKD-derived keys with PQC-based authentication are increasingly viewed as a pragmatic transitional strategy, combining physical-layer security with the flexibility and authentication capabilities of classical cryptography.

Table 2: Comparison of Emerging QKD Paradigms

Paradigm	Key Innovation	Primary Benefit	Maturity Level
MDI-QKD	Untrusted Bell-state relay measurement	Immune to detector side-channel attacks	Field trials
Twin-Field QKD	Single-photon interference at central node	Beats point-to-point rate-loss bound	Lab / early field
CV-QKD	Homodyne/heterodyne detection of coherent states	Compatible with telecom hardware	Commercial pilots
DI-QKD	Loophole-free Bell test certification	No trust needed in any device	Laboratory demo
Satellite QKD	Free-space link via orbiting satellite	Global-scale, low-loss	Operational (Micius)

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

Paradigm	Key Innovation	Primary Benefit	Maturity Level
		backbone	
Quantum Repeaters	Entanglement swapping + quantum memory	Extends range without measuring qubits	Early research

Table 3: QKD versus Post-Quantum Cryptography

Aspect	QKD	Post-Quantum Cryptography
Security basis	Laws of quantum physics	Computational hardness assumptions
Hardware needs	Specialized photonic/optical hardware	Runs on existing classical hardware
Long-term security	Information-theoretic	Conjectured, subject to future cryptanalysis
Deployment cost	High (fiber/satellite links, detectors)	Low (software/firmware update)
Range	Limited by loss / repeater maturity	Effectively unlimited (network-agnostic)

V. Applications

- Government and defense communication: securing classified communication channels against long-term harvest-and-decrypt threats.
- Financial infrastructure: protecting interbank transactions and settlement systems, several of which have piloted metropolitan QKD networks.
- Critical infrastructure and power grids: securing SCADA and control-system communication against nation-state adversaries.
- Healthcare data protection: safeguarding long-lived sensitive patient records that require decades-long confidentiality.
- Quantum-secured cloud and data-center interconnects: protecting east-west traffic between geographically distributed data centers.

Metropolitan QKD networks have already been deployed in cities including Beijing, Vienna, Geneva, and Tokyo, typically combining trusted-node fiber links with, in some cases, satellite relays for backbone connectivity, demonstrating the practical maturity of near-term quantum-secured networking.

Table 4: Representative Global QKD Deployments

Deployment	Region	Type	Notable Feature
Beijing–Shanghai Backbone	China	Trusted-node fiber	~2,000 km terrestrial QKD backbone
Micius Satellite Network	China	Satellite + ground stations	Intercontinental key distribution
SECOQC Vienna Network	Austria	Metropolitan fiber	Early multi-node QKD testbed
Tokyo QKD Network	Japan	Metropolitan fiber	Multi-vendor interoperability trial
EuroQCI Initiative	European Union	Fiber + planned satellite	Pan-European quantum communication infrastructure

VI. Challenges and Open Issues

A. Distance and Key-Rate Limitations

Despite advances such as TF-QKD, secret key rates remain orders of magnitude lower than classical optical data rates, and untrusted long-distance networks still require

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

further maturation of quantum repeater technology.

B. Implementation Security

Gaps between theoretical security proofs and physical implementations continue to expose side-channel vulnerabilities, including detector blinding, Trojan-horse attacks, and imperfect source characterization. Closing these gaps requires rigorous device characterization and standardized security certification frameworks.

C. Cost and Infrastructure

Specialized hardware, including single-photon detectors, phase-stabilized interferometers, and cryogenic components, remains costly relative to classical networking equipment, limiting widespread commercial adoption outside high-value use cases.

D. Integration with Classical Networks

Authentication of the classical channel used during QKD post-processing still relies on pre-shared keys or classical/post-quantum digital signatures, meaning practical QKD deployments are rarely purely information-theoretically secure end-to-end and must be evaluated as part of a broader hybrid security architecture.

E. Standardization

The absence of universally adopted interoperability standards across vendors and network operators continues to hinder large-scale, multi-vendor quantum network deployment, though bodies such as ETSI and ITU-T have begun developing relevant technical specifications.

VII. Future Research Directions

- Development of high-efficiency, low-noise quantum memories to enable practical multiplexed quantum repeaters.
- Loss-tolerant device-independent protocols capable of operating over realistic metropolitan-scale channel losses.
- Integration of chip-scale photonic QKD transmitters and receivers to reduce cost and enable mass deployment.
- Standardized hybrid QKD/PQC security architectures with formal composable-security proofs for end-to-end systems.
- Expansion of satellite constellations and inter-satellite links to realize a continuously available global quantum backbone.
- Machine-learning-assisted anomaly detection for real-time identification of side-channel and implementation attacks.

VIII. Conclusion

Quantum cryptography has progressed from a foundational theoretical proposal to a family of increasingly practical technologies capable of securing communication against both present-day and future quantum-enabled adversaries. Established protocols such as BB84 and E91 established the feasibility of

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

physics-based key distribution, while emerging paradigms, including measurement-device-independent QKD, twin-field QKD, continuous-variable QKD, device-independent QKD, satellite-based QKD, and quantum repeater networks, are progressively addressing the distance, security, and scalability limitations of earlier implementations. Complemented by post-quantum cryptography for near-term, infrastructure-compatible protection, these emerging paradigms collectively chart a credible path toward a resilient, long-term secure global communication infrastructure. Continued progress in quantum hardware, implementation security, and standardization will determine the pace at which this vision is realized.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.
2. A.K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663, Aug. 1991.
3. A.H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, no. 21, pp. 3121–3124, May 1992.
4. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks," Phys. Rev. Lett., vol. 92, no. 5, 057901, 2004.
5. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, 130503, 2012.
6. 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, pp. 400–403, 2018.
7. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett., vol. 88, no. 5, 057902, 2002.
8. D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in Proc. 39th Annu. Symp. Foundations of Computer Science, 1998, pp. 503–509.
9. S.-K. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, pp. 43–47, 2017.
10. J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature, vol. 582, pp. 501–505, 2020.
11. H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," Phys. Rev. Lett., vol. 81, no. 26, pp. 5932–5935, 1998.
12. S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 2, No 03, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-735 PAGE NO: 008-017

road ahead," Science, vol. 362, no. 6412, eaam9288, 2018.

13. National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," NIST FIPS 203, 2024.
14. National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," NIST FIPS 204, 2024.
15. V. Scarani et al., "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.
16. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997.
17. R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Inf., vol. 3, no. 30, 2017.