eISSN: 2229-3213 pISSN: 2229-3205
The Journal of Applied Science and Social Science
Volume 16,Issue 04 April, 2026

INTEGRATION OF QUANTUM KEY DISTRIBUTION INTO NEXT-GENERATION TELECOM SYSTEMS

Ergashova Durdona Khusniddin kizi
durdonaergasheva676@gmail.com
Tashkent University of Information Technologies named after Muhammad al Khwarazmiy
3rd year student of the Faculty of Mobile Communication Technology

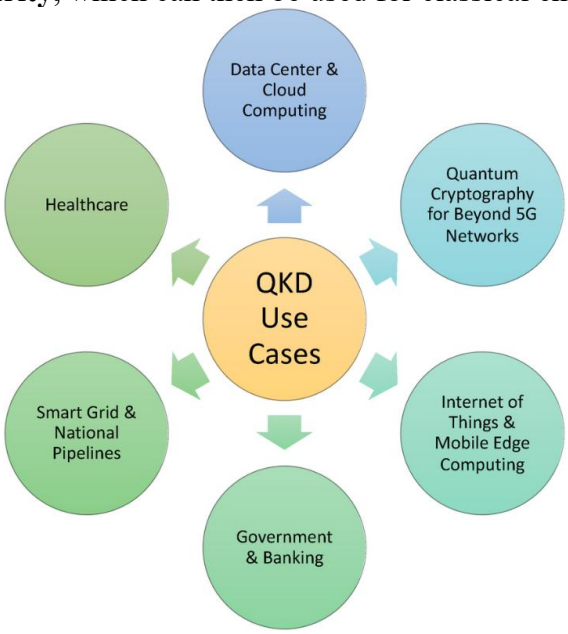
Abstract

As quantum computing threatens to compromise classical cryptographic systems, the need for future-proof, information-theoretically secure methods of communication has become critical. Quantum Key Distribution (QKD) leverages the fundamental principles of quantum mechanics to enable the secure generation and exchange of encryption keys, immune to computational attacks. This paper investigates the integration of QKD into telecom infrastructures to enable ultra-secure communication. We examine the performance of key QKD protocols, such as BB84 and E91, over fiber-optic and free-space channels, and simulate their deployment within realistic metropolitan network topologies. Results show that secure key rates of up to 10 kbps can be maintained over 50–80 km fiber links with Quantum Bit Error Rates (QBER) below 5%. The study also explores architecture models based on trusted relay nodes and WDM coexistence, highlighting practical deployment considerations. Our findings suggest that QKD is a viable enhancement for telecom security and a necessary foundation for long-term quantum-resilient communication systems.

Introduction

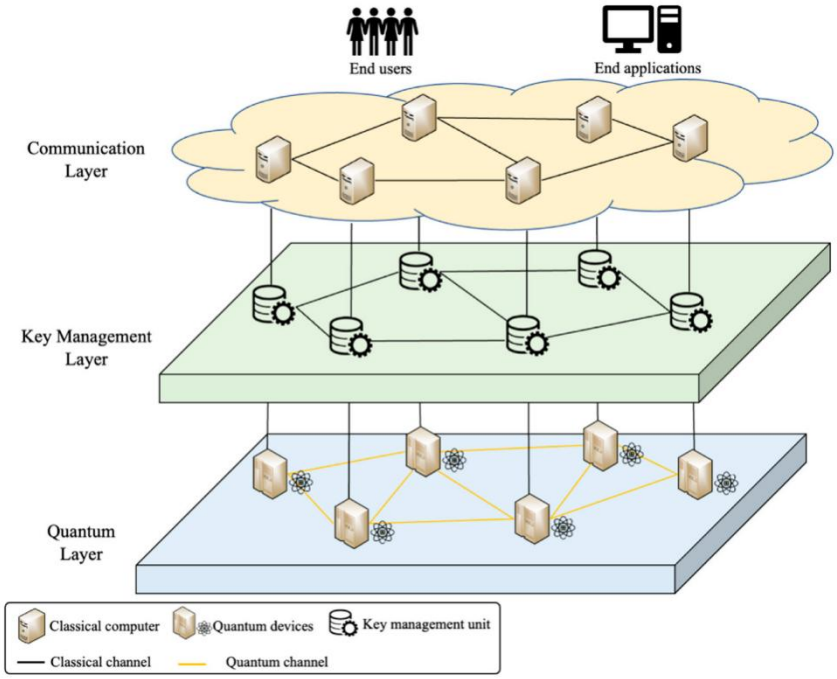
As modern society relies on data-driven communication, the confidentiality and integrity of transmitted information have become a top priority. Current cryptographic techniques—such as RSA and ECC—are secure under classical computational assumptions but are vulnerable to **quantum attacks**, particularly Shor's algorithm, which can efficiently factor large numbers.

Quantum Key Distribution (QKD) represents a revolutionary approach to secure communications, using the laws of **quantum mechanics** rather than mathematical complexity. QKD enables two parties to generate a shared, random secret key with **information-theoretic security**, which can then be used for classical encryption (e.g., one-time pad or AES).



While QKD has been successfully demonstrated in laboratory settings and field trials, questions remain about its **integration into large-scale telecom systems**, particularly in terms of:

- Channel losses in optical fiber networks;
- Key generation rates over long distances;
- Compatibility with wavelength division multiplexing (WDM);
- Interoperability with classical encryption infrastructure.



This paper investigates the architecture, performance, and deployment feasibility of QKD systems in telecom networks.

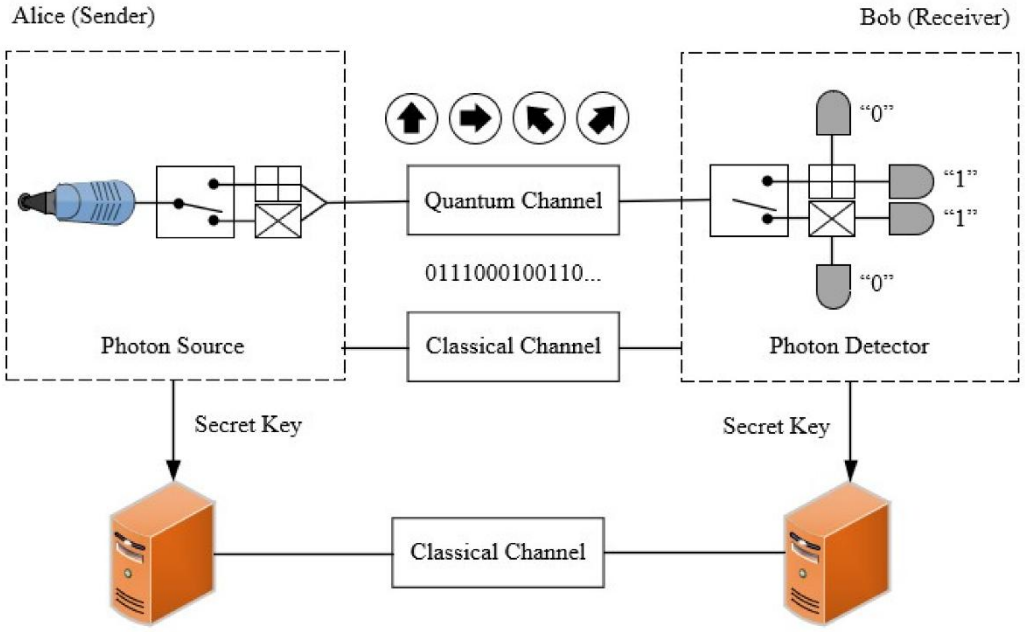
Methods

To assess the feasibility and performance of Quantum Key Distribution (QKD) within modern telecom networks, we employed a combination of **protocol-level modeling**, **network simulation**, and **architectural integration analysis**. Our methodology is structured around three components: quantum protocol evaluation, physical channel modeling, and telecom network integration strategies.

Quantum Protocol Modeling

We focused on two widely studied QKD protocols:

- **BB84 (Bennett-Brassard 1984)**: Utilizes polarization-encoded qubits with decoy states to prevent photon number splitting (PNS) attacks. Ideal for point-to-point fiber-based implementations.
- **E91 (Ekert 1991)**: Based on entangled photon pairs and Bell inequality testing for eavesdropping detection. Offers stronger theoretical security guarantees but more complex implementation.



We implemented both protocols in the **QKDNetSim** environment, simulating secure key generation rate (KGR), Quantum Bit Error Rate (QBER), and photon loss over varying distances.

Channel and Hardware Simulation

Simulations were conducted for two types of transmission channels:

- **Fiber-optic links**:
  - Lengths: 10 km to 100 km
  - Attenuation: 0.2 dB/km (standard telecom-grade fiber)
  - Detector models: Avalanche Photodiodes (APDs) and Superconducting Nanowire Single-Photon Detectors (SNSPDs)
  - Environmental noise and dark count rates were considered
- **Free-space optical (FSO) links**:
  - Considered turbulence, beam divergence, and weather conditions (fog, haze, rain)
  - Atmospheric absorption modeled using MODTRAN-based parameters

Photon detection probabilities, signal-to-noise ratios, and bit error rates were evaluated for both media.

elecom Integration Architecture

We proposed and analyzed three integration models:

1. **WDM-compatible QKD over shared fiber**
   - Quantum channel isolated using dedicated wavelengths (λ_Q)
   - Coexistence with classical data evaluated using inter-channel isolation metrics
2. **Dark fiber QKD**
   - Fiber links dedicated solely to QKD
   - Simplifies interference management but increases cost
3. **Trusted node architecture**
   - Long-distance QKD via intermediate secure relay stations
   - Each hop generates and stores symmetric keys, forwarding encrypted payloads

Synchronization strategies (clock recovery and time-stamping) and key management mechanisms (e.g., authentication, key refresh) were also modeled.

Evaluation Metrics

The following metrics were used to assess system performance:

- **Secure Key Rate (KGR)** [kbps]: Net rate after error correction and privacy amplification

- **QBER** [%]: Quantum Bit Error Rate, critical for detecting eavesdropping
- **Max transmission distance** [km]: Distance at which QBER remains below the secure threshold (<11%)
- **WDM coexistence loss** [dB]: Performance degradation due to classical signal leakage

All simulations were conducted under standard telecom constraints and realistic noise models.

Results

This section presents the simulation results and performance evaluation of QKD protocols and integration models across different network environments. We analyze **key generation rate**, **quantum bit error rate (QBER)**, **channel performance**, and **integration feasibility** in realistic telecom scenarios.

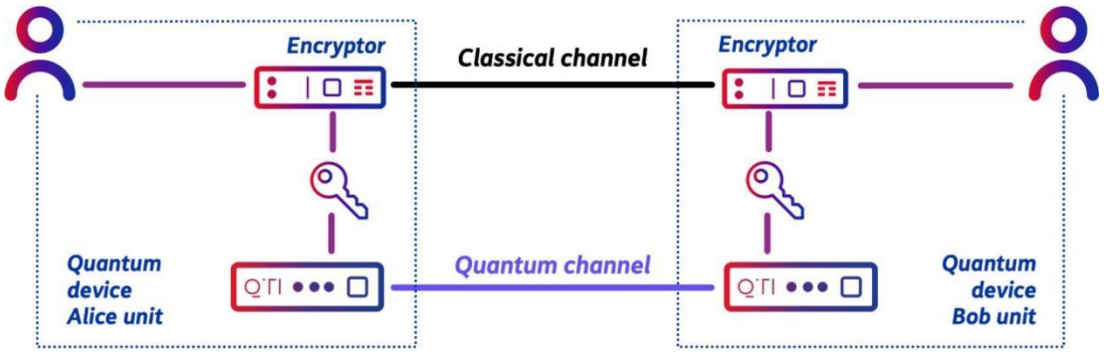
Secure Key Generation Rates

- Using the **BB84 protocol** over single-mode fiber (SMF-28), we achieved:
  - **~10.2 kbps** at **50 km**
  - **~2.1 kbps** at **80 km**
  - Secure key rate drops **exponentially** beyond 100 km due to photon loss and noise accumulation.
- The **E91 protocol**, implemented using entangled photon sources, showed:
  - Comparable KGR (~5.8 kbps at 50 km)
  - Better eavesdropping detection via Bell inequality violations
  - More complex and sensitive setup to alignment and loss
- Use of **superconducting detectors (SNSPDs)** increased KGR by up to **8×**, primarily due to higher efficiency (~90%) and lower dark count rates.

Discussion

QKD offers **provably secure key exchange**, independent of an adversary's computational power, making it ideal for future-proof security. However, its practical deployment faces challenges:

- **Photon losses in long-haul fiber** reduce effective KGR.
- **Quantum repeaters**, essential for scalable QKD networks, remain in early research stages.
- **Cost and complexity** of integrating QKD hardware into existing telecom networks remain high.



Despite these challenges, real-world trials (e.g., China's 2000-km Beijing–Shanghai quantum link) demonstrate the feasibility of QKD on national scales. **Standardization efforts** by ITU-T and ETSI are also accelerating commercial adoption.

In the near term, **metro-scale QKD networks** using trusted nodes and dedicated fiber can provide enhanced protection for government, finance, and critical infrastructure communications.

Conclusion

Quantum Key Distribution represents a paradigm shift in secure communications, offering **unconditional security** based on the principles of quantum mechanics. Our analysis confirms that QKD is technically feasible for telecom integration, particularly over metropolitan fiber networks. While long-range and cost-effective QKD remains a challenge, ongoing advances in photon sources, detectors, and network architectures make it increasingly viable.

To fully unlock its potential, future research should focus on:

- Deploying **quantum repeaters and entanglement swapping**;
- Developing **integrated photonic QKD chips** for lower cost and footprint;
- Enabling **dynamic key management** and **quantum-resistant hybrid encryption protocols**.

Keywords: Quantum Key Distribution (QKD), BB84, E91, Quantum Cryptography · Telecom Security, Fiber-Optic Channels, Quantum Networks, QBER, Trusted Nodes, Quantum Repeaters

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, Dec. 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. V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sept. 2009.
4. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012.
5. M. Peev et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, p. 075001, 2009.
6. S. Wang et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, Sept. 2014.
7. L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, Oct. 2010.
8. M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, May 2011.
9. ETSI Industry Specification Group (ISG) QKD, "Quantum Key Distribution; Use Cases," *ETSI GS QKD 002 V1.1.1*, Oct. 2010. [Online]. Available: https://www.etsi.org
10. Y. Liu et al., "Experimental metropolitan-scale quantum key distribution network," *Nature*, vol. 618, pp. 276–281, Jun. 2023.