OPEN ACCESS JOURNALS
Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21559795

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Review Article

Volume-06|Issue-04|2026

Role of Quantum Key Distribution System against Various Threats in Digital Era: A Review

Shashikala M[1] and Channa Krishna Raju[2]

Research Scholar, Sri Siddhartha Academics of Higher Education, Tumkur, India.
Professor and Head, Department of AI and ML, Sri Siddhartha Institute of Technology, Tumkur, India.

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Shashikala, M. & Raju, C. K. (2026). Role of Quantum Key Distribution System against Various Threats in Digital Era: A Review. *Indiana Journal of Multidisciplinary Research, 6*(4), 84-89.

Abstract: Abstract. This study investigates how Quantum Key Distribution serves as a novel cryptographic methodology utilizing quantum physics principles to counter contemporary cybersecurity challenges. QKD's intrinsic characteristics provide exceptional resistance to conventional intrusion methods while delivering encryption strength that cannot be mathematically compromised. Our analysis examines QKD protocol behavior under diverse threat conditions within mod ern digital ecosystems. We concentrate on implementation-level weaknesses, especially those targeting physical elements like photon detection systems, to identify security gaps and develop mitigation approaches. Furthermore, we investigate the complexity of integrating QKD with legacy communication systems, analyzing vulnerabilities at the intersection of quantum and classical technologies while recommending protective mechanisms for these transitional zones.

Keywords: Quantum Key Distribution, Security threats · Photon detectors · Hardware attacks · Secure communication.

INTRODUCTION

The advent of Quantum Key Distribution has transformed digital security by employing quantum physics laws to generate cryptographic keys offering verifiable security properties. Conventional key establishment protocols cannot match QKD's inherent security features, particularly its capacity to recognize illicit interception, offering safeguards constrained solely by physical principles instead of computational limitations [1, 2]. Nevertheless, operational QKD systems confront tangible security obstacles, encompassing device-level weaknesses, signal capture methodologies, and com-plex offensive techniques exploiting quantum characteristics [3, 6]. This detailed assessment examines practical QKD security, investigating both revolutionary capabilities and deployment barriers.

Quantum Cryptographic Foundations

Systems employing Quantum Key Distribution harness quantum effects like superposition phenomena and particle entanglement for safeguarding data transmission. QKD's defining attribute is its eavesdropper detection capability: illicit quantum bit observation inevitably modifies their quantum states, revealing the intrusion [1, 4]. Traditional cryptographic methods base security on mathematically challenging computational problems, while QKD obtains protection through fundamental physical laws, facilitating secret key creation resistant to opponents possessing infinite computational capacity [2, 3]. Notably, QKD operates as a key creation and distribution tool rather than executing encryption operations; generated secure keys integrate with traditional encryption algorithms, including the cryptographically perfect one-time pad under proper implementation [1, 6].

Essential Security Contributions of QKD

QKD supplies unconditional security assurances founded on quantum physics laws, delivering strong protection against future quantum computing dangers. Core advantages encompass:

- Security grounding in physical laws instead of computational hardness assumptions [1, 2]
- Built-in detection of illicit surveillance or signal capture [3]
- Safeguarding encryption infrastructure against approaching quantum computer capabilities [4]

Via exceptionally secure key establishment procedures, QKD constitutes a major progression in defending digital communications against advanced and adaptive cyber dangers [5].

Study Goals and Coverage

This assessment delivers extensive QKD technology coverage, spanning theoretical underpinnings, protocol alternatives, security features, operational implementations, and developmental prospects. We merge theoretical frameworks with empirical discoveries, stressing QKD's protective functions against quantum-age cyber threats. Our evaluation encompasses

***Corresponding Author:** Shashikala M

existing constraints and developing remedies to advance practical utilization.

Defined research goals comprise:

- Establishing the essential nature of secure key distribution within contemporary cryptography, especially regarding quantum computing risks [2, 4]
- Clarifying QKD operational mechanisms, encompassing superposition, entanglement, and quantum state non-replication [1, 3]
- Executing comparative assessment of varied QKD protocols [5]
- Surveying present implementations and active research programs [1, 2, 3]
- Recording deployment obstacles and exploring viable remedies [6]
- Recommending progress trajectories to strengthen practical system viability and durability [4, 5].

QUANTUM KEY DISTRIBUTION TECHNOLOGIES

QKD architectures enable protected cryptographic key transmission through quantum state communication, predominantly encoded within single photons, connecting communication endpoints traditionally labeled Alice (transmission source) and Bob (reception destination) [1]. Via quantum state observation, both endpoints establish a mutual secret key. QKD architectures necessitate two separate channels: a quantum channel conveying quantum states and a classical public channel managing coordination and verification operations ensuring key reliability. Quantum channel choice—fiber optic or atmospheric transmission—depends upon range specifications and transmission parameters. Contrasting classical methodologies depending on computational complexity, QKD exploits core quantum physics laws to attain unconditional security via quantum principles, one-time pad ciphering, and cryptographic hash functions [1, 2].

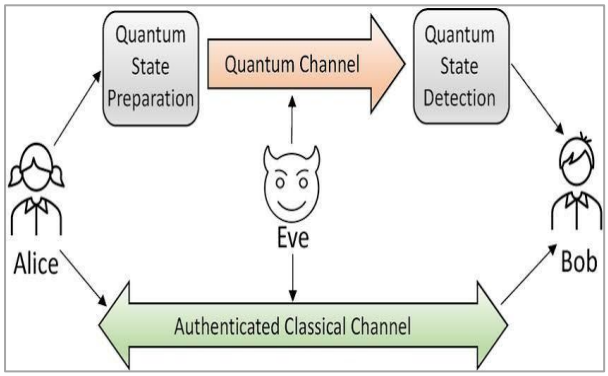

Fig.1. Illustrates a generic QKD system, highlighting the quantum and public channels.

Foundational QKD Principles

Quantum Computing Algorithms and Security Ramifications

Multiple quantum computing algorithms constitute major dangers to traditional cryptographic frameworks:

- Shor's Algorithm: Facilitates polynomial-time integer factorization, compromising public-key systems like RSA and ECC [4]
- Grover's Algorithm: Delivers quadratic acceleration for unsorted search operations, essentially reducing symmetric cipher security strength by half (exemplified by AES) [4]
- Quantum Fourier Transform (QFT): Enables phase approximation and supports constructions like Shor's, permitting calculations impossible for classical machines [4].

Quantum Mechanical Principles

Photonic Polarization

Single photon polarization constitutes a basic qubit characteristic. Individual photons demonstrate distinct polarization conditions separate from coherent light's aggregate properties. Photons exhibit polarization across particular planes (horizontal, vertical, or intermediary orientations). BB84 protocol employs polarization variations (like ±45°) for binary information encoding, where distinct orientations signify logical '0' and '1' values. Photons exhibiting polarization in one plane face blockage by filters oriented toward perpendicular planes, guaranteeing illicit observations modify photon conditions and facilitate eavesdropping identification [1].

Heisenberg's Uncertainty Constraint

Heisenberg's uncertainty constraint establishes that paired physical attributes (exemplified by position and momentum) resist simultaneous measurement at arbitrary precision levels. Operationally, examining any quantum characteristic of a photon or qubit inescapably disrupts its condition, inserting random alterations. This phenomenon proves especially significant at individual-photon magnitudes, where any observation or disturbance transforms the quantum arrangement, barring eavesdroppers from information extraction without detection [1].

No-Cloning Quantum Theorem

The quantum no-cloning theorem demonstrates that unknown arbitrary quantum conditions resist perfect replication. Though imprecise cloning stays feasible, quantum mechanics' linearity and unitarity requirements prevent precise qubit duplication. This characteristic ensures any opponent (Eve) endeavoring to replicate qubits for key acquisition introduces identifiable errors, preserving communication reliability between Alice and Bob [1, 5]

Superposition Phenomenon

Quantum superposition permits quantum arrangements (photons, electrons) to occupy numerous conditions

***Corresponding Author:** Shashikala M

concurrently until observation transpires. Contrasting classical bits signifying either 0 or 1, qubits encode condition mixtures. This characteristic permit concurrent information manipulation in quantum arrangements and establishes the basis for protected QKD protocols [1].

Quantum Entanglement Phenomenon

Quantum entanglement manifests when particle pairs (like photons) exhibit linked attributes regardless of physical distance. Observing one particle immediately establishes its entangled companion's condition. Within QKD deployments, Alice and Bob employ entangled qubit pairs producing linked keys. Throughout key extraction, Alice encodes arbitrary bit sequences in entangled qubits, dispatching one qubit per pair to Bob while keeping the other. Following observation, both endpoints evaluate statistical links, commonly utilizing Bell inequality assessments. Significant variations from anticipated links indicate eavesdropper existence [1, 5].

QKD Protocol Classifications

QKD protocols separate into two principal classifications: prepare-and-measure protocols and entanglement-based protocols [1].

Prepare-and-Measure Protocol Category

Prepare Within prepare-and-measure QKD, the transmission source (Alice) inserts information into quantum conditions like polarized photons and dispatches them to the reception endpoint (Bob), who executes observations utilizing randomly selected measurement bases. Protocol designation originates from these separate preparation and observation stages [1, 5].

Protection depends on core quantum principles:

- Heisenberg's Uncertainty Constraint: Observation inherently transforms quantum conditions, rendering eavesdropping identifiable via inserted disturbances
- Quantum No-Cloning Theorem: Unknown quantum conditions resist perfect replication, preventing error-free qubit duplication by opponents

Any illicit disturbance inserts quantifiable variations, permitting Alice and Bob to identify prospective eavesdroppers and confirm key transmission reliability [1]. Device-Independent QKD (DIQKD) augments prepare-and-measure protocols through removing reliance on internal device reliability. DIQKD confirms protection via observable quantum links, like Bell inequality breaches, supplying strong protection even with defective, untrusted, or infiltrated devices [1, 5].

Entanglement-Based Protocol Category

Entanglement-based QKD utilizes entangled photon pairs establishing mutual secret keys. Unlike prepare-and-measure approaches, both Alice and Bob obtain one photon from entangled pairs, producing keys from linked observation results. These protocols exploit quantum entanglement's distinctive characteristics [1, 5]. Essential features encompass:

- Quantum Correlation: Entangled photon pair observations generate powerfully linked results independent of Alice-Bob distance. Any eavesdropper (Eve) disturbance or observation modifies links detectably
- Bell Inequality Confirmation: Protection confirmation via Bell inequality breach assessments. Observation result variations from anticipated links suggest prospective intrusion or eavesdropping
- Device Defect Resistance: Entanglement-based protocols, especially DIQKD variations, necessitate no device internal function confidence. Protection relies exclusively on witnessed quantum links, safeguarding against infiltrated devices [1, 7]

Notable entanglement-based protocols encompass:

- E91 Protocol: Artur Ekert's design utilizing entangled photon pairs and Bell inequality assessments for protected key creation. Interception endeavors diminish observed links, indicating eavesdropping [1]
- BBM92 Protocol: Entanglement-based BB84 modification where Alice and Bob each observe one photon from entangled pairs. Linked observation results construct the key; variations suggest prospective eavesdropping [1]
- Differential Phase Shift (DPS) Protocol: Employs entanglement and phase links for protected key conveyance. DPS withstands Photon Number Splitting (PNS) attacks and accommodates practical deployment owing to straightforward architecture [1, 5]

Entanglement-based QKD guarantees elevated protection through identifying quantum condition disturbance endeavors and confirming key production via core quantum physics principles.

THREAT VECTORS AND EMPIRICAL OBSERVATIONS

Though QKD maintains theoretical protection, operational deployments stay susceptible to multiple attacks. This segment investigates notable attack categories, their operation methods, and empirical outcomes across varied QKD protocols.

Eves dropping

Eavesdropping encompasses opponents disrupting quantum channels through inserting illicit devices capturing key data throughout conveyance [1, 14]. Empirical investigations on BB84, B92, and BBM92 protocols reveal that B92 demonstrates minimal error percentages (0.199–0.256), BB84 exhibits elevated

***Corresponding Author:** Shashikala M

percentages (0.231–0.313), and BBM92 supplies intermediary capability, validating dependability [1]. Protection evaluation validates BB84 sustains confidentiality assuming error percentages between Alice and Bob stay beneath 7.56%. Integrated error rectification and privacy enhancement guarantee ultimate key confidentiality even facing optimal eavesdropping attacks [15].

Photon Number Splitting Attack

PNS attacks leverage multi-photon transmissions, permitting eavesdroppers to capture single photons without disrupting others arriving at the receiver. The SARG04 protocol, a modified BB84 variation, reduces PNS attacks when integrated with decoy conditions altering photon strengths, facilitating interference identification. Nevertheless, architectures utilizing weak coherent pulses stay vulnerable, as individual photon capture may not elevate error percentages [10, 13].

Trojan Horse Attack

Trojan Horse attacks (light insertion attacks) focus on QKD hardware instead of quantum signals [6]. Reduction approaches encompass constraining light admission to particular wavelengths, restricting optical component operational timeframes, and reducing reflected light. Investigation proves that physical layer weaknesses can undermine QKD's theoretical protection, highlighting strong hardware safeguard necessity. Passive surveillance devices and optical separators prevent illicit light architecture admission, strengthening comprehensive protection [6, 10, 11].

Intercept and Resend

Within Intercept-and-Resend attacks, opponents capture communications between endpoints, potentially altering data preceding retransmission. Regulated investigations reveal Eve can seize Alice's photons, retransmit them to Bob, and acquire roughly $1/\sqrt{2}$ of Alice's data. Elementary deployments produce minimal data acquisition (~0.2 bits per conveyed bit), whereas sophisticated methodologies like Breidbart basis or complete I/R attacks facilitate elevated data extraction [8].

Man-in-the-Middle Attack

Man-in-the-Middle attacks transpire when attackers situate themselves between transmission source and reception endpoint, masquerading as both endpoints. Within QKD architectures, such attacks permit Eve to capture quantum and classical messages and transmit altered responses. This situation can thoroughly undermine communication legitimacy, endangering key transmission procedure reliability.

Time-Shift Attack

Time-Shift attacks leverage single-photon detector performance fluctuations. Through modifying photon arrival schedules, attackers can influence detector reactions and acquire partial key data without significantly elevating error percentages. Investigations on BB84 plug-and-play architectures, encompassing commercial ID-500 QKD devices, prove that optical postponement lines and switches enable this attack, permitting Eve to retrieve data while staying predominantly unidentified [12].

Table 1. Experimental Analysis of QKD Attacks

Attack Type	Affected Protocol(s)	Observed Impact	Countermeasures
Eavesdropping	BB84, B92, BBM92	B92: 0.199–0.256 BB84: 0.231–0.313 BBM92: intermediary error rectification and privacy enhancement [15]	Eavesdropping-resistant BB84
Photon Number Splitting	SARG04	Susceptible to multi-photon capture	Decoy conditions; photon strength fluctuation [10,13]; optical separators
Trojan Horse	BB84, device-level	Device infiltration via inserted light	Active surveillance filters [10,11]; protocol confirmation
Intercept-and-Resend	BB84, B92	Elementary: 0.2 bits; Sophisticated: elevated acquisition	Error identification [8]; authentication protocols
Man-in-the-Middle	All QKD protocols	Total key infiltration if accomplished	Device-independent QKD [1,15]; detector randomization
Time-Shift	BB84	Partial key data without QBER elevation	Timing adjustment [12,14]

CHALLENGES

Though QKD supplies theoretically unbreakable key transmission, multiple practical constraints exist:

- Range Constraints: Fiber-based QKD functions efficiently within ~100–150 km owing to photon dissipation and decoherence, whereas satellite or atmospheric QKD broadens range but demands intricate quantum repeaters or trusted intermediary nodes [1, 3, 5]
- Economic Obstacles: High-precision elements, encompassing single-photon sources and detectors, render QKD costly, constraining implementation to research facilities and large-scale commercial

***Corresponding Author:** Shashikala M

deployments [1, 4]

- Authentication Reliance: Authentication continues depending on classical cryptographic techniques, potentially inserting weaknesses like man-in-the-middle attacks and requiring hybrid protection remedies [2, 5]
- Environmental Vulnerability: Environmental elements like atmospheric disturbance, fiber defects, and detector performance limitations can compromise signals and generate exploitable secondary channels [6, 10]
- Integration Complications: Integration with current communication infrastructures confronts obstacles owing to protocol compatibility and key administration concerns, constraining expandability [1, 16]

CONCLUSION

Quantum Key Distribution constitutes a revolutionary methodology for protecting communications via core quantum physics principles. Notwithstanding its capacity for extraordinary protection standards, practical deployment obstacles continue. Opponents possessing considerable resources and quantum computing capabilities could continue endeavoring sophisticated quantum attacks, demanding persistent investigation to strengthen protocol durability while sustaining data conveyance performance. Creating mutual keys across public channels stays fundamentally susceptible to quantum-based attacks and deployment defects. QKD supplies a viable remedy through facilitating protected key transmission and permitting eavesdropping identification grounded in quantum physical laws. Persistent advancement and integration of QKD into functional infrastructures prove vital to completely achieve Quantum Key Distribution advantages while reducing prospective weaknesses.

REFERENCES

1 Brazaola-Vicario, A., Ruiz, A., Lage, O., Jacob, E., & Astorga, J. (2024). Quantum key distribution: A survey on current vulnerability trends and potential implementation risks. *Optics Continuum, 3*(8), 1438–1460. https://doi.org/10.1364/OPTCON.530352

2 Sushchev, I. S., Bulavkin, D. S., Bugai, K. E., Sidelnikova, A. S., & Dvoretskiy, D. A. (2024). Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis. *Physical Review Applied, 22*(3), Article 034032. https://doi.org/10.1103/PhysRevApplied.22.034032

3 Lu, Y. F., et al. (2025). Experimental measurement-device-independent quantum key distribution with flawed state-preparation over 303.37 km. *EPJ Quantum Technology, 12*, Article 103. https://doi.org/10.1140/epjqt/s40507-025-00408-4

4 Shao, S. F., Zhou, L., & Lin, J. (2025). High-rate measurement-device-independent quantum communication without optical reference light. *Physical Review X, 15*(2), Article 021066. https://doi.org/10.1103/PhysRevX.15.021066

5 Le Roy-Deloison, T., Lobo, E. P., Pauwels, J., & Pironio, S. (2025). Device-independent quantum key distribution based on routed Bell tests. *PRX Quantum, 6*(2), Article 020311. https://doi.org/10.1103/PRXQuantum.6.020311

6 Chen, J. P., et al. (2024). Twin-field quantum key distribution with local frequency locking. *Physical Review Letters, 132*(26), Article 260802. https://doi.org/10.1103/PhysRevLett.132.260802

7 Peng, Q., et al. (2025). Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack. *npj Quantum Information, 11*, Article 63. https://doi.org/10.1038/s41534-025-00963-9

8 Lobo, E. P., Pauwels, J., Le Roy-Deloison, T., & Pironio, S. (2024). Certifying long-range quantum correlations through routed Bell tests. *Quantum, 8*, Article 1332. https://doi.org/10.22331/q-2024-05-02-1332

9 Sun, Y., et al. (2025). Analyzing the performance of CV-MDI QKD under continuous-variable measurement-device-independent quantum key distribution. *Physical Review Applied, 23*(1), Article 014056. https://doi.org/10.1103/PhysRevApplied.23.014056

10 Liu, Y., et al. (2023). Experimental twin-field quantum key distribution over 1000 km fiber distance. *Physical Review Letters, 130*(22), Article 220801. https://doi.org/10.1103/PhysRevLett.130.220801

11 Müller, R. (2025). On high-dimensional twin-field quantum key distribution. *Quantum, 9*, Article 133. https://doi.org/10.22331/q-2025-07-15-133

12 Geng, M., et al. (2025). Advances of quantum key distribution and network integration. *npj Quantum Information, 11*, Article 124. https://doi.org/10.1038/s41534-025-00963-9

13 Wu, L., et al. (2025). Passive-state preparation continuous-variable quantum key distribution. *Optics Communications, 457*, 124–129. https://doi.org/10.1016/j.optcom.2025.124129

14 Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., & Lo, H.-K. (2018). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Physical Review A, 98*(6), Article 062314. https://doi.org/10.1103/PhysRevA.98.062314

15 Grasselli, F., et al. (2025). Quantum key distribution with basis-dependent detection: Practical detector modeling and security. *Physical Review Applied, 15*(2), Article 024050. https://doi.org/10.1103/PhysRevApplied.15.024050

16 Nasedkin, B., Kiselev, F., Filipov, I., Tolochko, D., Tchouragoulov, S., Kumar, K., & Makarov, V. (2023). Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects

***Corresponding Author:** Shashikala M

for Trojan-horse attacks. *Physical Review Applied, 20*(1), Article 014038

BIOGRAPHY

Dr Channakrishnaraju (C.K.Raju) has 30 years of teaching experience for UG and PG courses in computer Science and Engg, and is currently working as Professor and head in the Department of Artificial Intelligence and Machine Learning at Sri Siddhartha Institute of Technology, Tumkur. He obtained B.E from Bangalore University in the year 1995 and PG in software systems in the year 2000 From BITS, Pilani and Doctoral degree PhD in Computer Science and Engineering at Sri Siddhartha Academy of higher Education, Tumkur in the year 2017. His research interests are in the areas of wireless sensor networks, network security, Artificial intelligence, Cloud Computing, IOT, computer Architecture, soft computing and Evolutionary computing. He worked as Editorial member for several international journals, he worked as editorial chief for two reputed journals and he worked as reviewer and session chair for more than 30 IEEE international conferences. He published 65 papers in international journal and conferences. He Published Design Patent on" Ai based Solar Bicycle "In the Year 2023. He is acting as resource persons for several workshops and conferences. He Adjudicated PhD Thesis. He working as doctoral committee member for visveswaraih technological university Belgaum and Sri Siddhartha academy of higher education, Tumkur. He guided six PhD Scholars In Computer science and Engineering and Currently he is Guiding six PhD Scholars In Computer Science and Engineering at Sri Siddhartha academy of higher education. Tumkur. He can be contacted at email: ckraju@ssahe.edu.in.

***Corresponding Author:** Shashikala M