RCHUB: JOURNAL OF COMPUTATIONAL INTELLIGENCE SCIENCE AND ENGINEERING (JCISE)
VOL: 2, ISSUE 1, JANUARY-MARCH 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

QUANTUM KEY DISTRIBUTION FOR SECURE INTERNET OF THINGS: A COMPREHENSIVE SURVEY

GEETHA RANI. S[1], Dr. F. LEENA VINMALAR[2]
1 Research Scholar, A.V.P College of Arts and Science(Co-Education), Tirupur
Email: dr.sgeetharani@gmail.com, https://orcid.org/0009-0007-7256-1914
2 Assistant Professor, A.V.P College of Arts and Science(Co-Education), Tirupur
Email: anuleena7@gmail.com

Abstract:

The fast development of Internet of Things (IoT) devices has introduced unknown security issues in the networked systems. Classical cryptography methods are restricted to sophisticated attacks and the emerging threat of quantum computing. This survey paper presents the overview of quantum key distribution (QKD) use in IoT settings, systematic review of the research trend, technological solutions, challenges, and future developments. We examine more than 150 published in-between 2018-2025 research papers, categorize the current QKD-IoT solutions, and uncover gaps in the research. We find that hybrid QKD-classical cryptography designs provide promise of realistic IoT implementation and edge-based quantum gateways emerge as an architecture of scalable implementation.

Keywords: *Internet of Things(IoT), Quantum Cryptography, Quantum Key Distribution (QKD), Quantum Key Distribution Protocols.*

1. Introduction:

The Internet of Things (IoT) has revolutionized the way contemporary computing is being done because it develops unified systems of intelligent devices that communicate, share information, and make autonomous decisions. The IoT applications are now part of the critical infrastructure of smart homes, industry, medical monitoring, and autonomous vehicles. With this connectivity however, comes enormous security vulnerabilities which conventional cryptographic means have a difficult time mitigating. The root of the problem is that IoT is heterogeneous: different devices that have different computational power, energy limitations, and communication protocols, provide a complicated security environment. The mathematical security of traditional encryption schemes is currently challenged by the possibilities of quantum computing in addition to a growing arsenal of attack vectors. Further, the limited resources of most of the IoT devices restrict the use of strong

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

cryptographic algorithms. Quantum Key Distribution is an alternative that becomes a good solution to the challenges since it utilizes quantum mechanical laws to achieve information-theoretic security. QKD is unconditional security unlike the computational security of the classical cryptography that is grounded on the basic physical laws. The survey focuses on the intersection between QKD and IoT security and the analysis of the current studies, implementation issues, and future opportunities.

1.1 Scope and Objectives

This survey is intended to identify:

- Provide a comprehensive analysis of QKD applications in IoT security
- Categorize existing research approaches and methodologies
- Identify implementation challenges and proposed solutions
- Analyze performance metrics and evaluation frameworks
- Discuss future research directions and emerging trends

1.2 Survey Methodology

Our systematic literature review included articles published between 2018 and 2025 and aimed at peer-reviewed articles published by IEEE, ACM, and Springer among other reputable journals. In search engine and article databases, we incorporated the following keywords: quantum key distribution, IoT security, quantum cryptography, secure IoT communication and so forth. Our analysis of 156 relevant papers was based on approach, area of application, and technological focus classification.

2. Background and Fundamentals

2.1 IoT Security Landscape.

The problem of IoT security is due to some essential peculiarities:

Heterogeneity: IoT environments are heterogeneous with the presence of different devices with different computer capacities, which may encompass a range of powerful edge gateways to resource-constrained sensors. This multiplicity makes it a challenge to introduce homogenous security measures.

Scale: A modern IoT deployment can contain thousands to millions of connected devices, and it is not a simple task to manage security centrally and pose a wide range of potential attack surfaces.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Resource Constraints: A large number of IoT devices have hard limits on energy, memory, and processing resources, which limits the complexity of the security mechanisms implemented.

Patterns of communication: IoT networks demonstrate various communication patterns, such as the device-to-device, device-to-cloud, and mesh networking, and each of them demands specific security strategies.

2.2.1 Principles of Quantum Key Distribution.

Quantum Key Distribution is an approach based on quantum mechanical properties and helps communicate parties in a secure way to exchange keys. QKD protocols are based on the basic principles of quantum sciences and thus, their security depends on the same principle.

Quantum No-Cloning Theorem: The quantum states cannot be replicated to perfection and this does not allow the eavesdroppers to intercept and relay quantum information in such a way that they remain undetected.

Heisenberg Uncertainty Principle: Any act of measuring a quantum system changes the state of the system and any attempt to eavesdrop can be noted by a higher error rate.

Quantum Entanglement: Correlated quantum states make it possible to use secure key distribution protocols, which can spot any interference of the communication channel.

2.3 Classical QKD Protocols:

There are a number of protocols of QKD which are developed and evaluated: BB84 Protocol: BB84 protocol is proposed by Bennett and Brassard in 1984 and involves using four quantum states to encode bits with security being based on the fact that it is impossible to tell the difference between two non-orthogonal quantum states. E91 Protocol: E91 was invented in 1991 by Ekert that relies on the entangled photon pairs and the violations of the Bell inequality to detect eavesdropping attacks. SARG04 Protocol: This is based on the improvement of BB84 to offer better resistance to photon-number-splitting attacks. Continuous Variable QKD: It has continuous quantum variables (such as position and momentum), and has the potential to provide benefits in fibre-optic implementation.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

3. Literature Review and Classification

3.1 Research Trend Analysis

We find that there is a marked rise in the research of QKD-IoT with the number of publications growing by 12 articles in 2018 to 47 articles in 2024. The field of research has shifted its emphasis on theory to the application issues and composite security models.

Temporal Distribution:

- ✓ 2018 - 2019: Theoretical foundations and feasibility studies (15%)
- ✓ 2020 - 2021: Protocol adaptations and simulation studies (28%)
- ✓ 2022 - 2023: Hybrid architectures and performance analysis (35%)
- ✓ 2024 - 2025: Implementation challenges and real-world deployments (22%)

3.2 Research Categories:

The existing research is divided into five major spheres by us:

3.2.1 Protocol Development and Theoretical Foundations:

The studies in this field are aimed at modifying classical QKD protocols to the IoT setting and creating novel protocols that can be used by resource-constrained devices.

Key Contributions:

- Modified BB84 protocols for low-power devices
- Lightweight quantum key agreement schemes
- Error correction mechanisms for noisy IoT channels
- Security proofs for IoT-adapted QKD protocols

Representative Works:

A simplified version of BB84 that cuts by 40% of the computational overhead is proposed by Chen et al. (2021).

Kumar and Sharma (2022), a hybrid protocol between classical and quantum protocols with a success rate of 99.7% success in key agreement was developed.

Liu et al. (2023) proposed the methods of correcting errors that are specific to the pattern of communication of IoT.

3.2.2 Architecture and System Design:

This group includes studies of system architectures to combine QKD into the IoT infrastructures.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Architectural Approaches:

1. Central Architecture:

Key distribution is controlled by Central QKD server over all the IoT devices.

2. Distributed Architecture:

Multiple QKD nodes provide redundancy and scalability.

3. Hierarchical Architecture:

Combines centralized and distributed elements with gateway-based implementation

4. Hybrid Architecture:

Combines quantum and classical cryptography.

Edge Gateway Solutions:

Several designs suggest edge-based designs in which quantum-enabled gateways process QKD functionality and resource-limited devices are based on classical cryptography and quantum-distributed keys. This is a compromise between security and practical implementation restrictions.

3.2.3 Analysis and Optimization of Performance.

Studies that are based on performance metrics, optimization strategies, and comparison between implementing QKD-IoT.

Key Metrics:

- **Quantum Bit Error Rate (QBER):** Measures channel noise and potential eavesdropping
- **Key Generation Rate:** Throughput of secure key production
- **Energy Consumption:** Power requirements for QKD operations
- **Latency:** Time delay in key distribution and establishment
- **Scalability:** System performance as network size increases

Optimization Strategies:

- Adaptive protocols that adjust parameters based on channel conditions
- Machine learning approaches for optimal resource allocation
- Load balancing techniques for distributed QKD networks

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

3.2.4 Application –Specific Implementations:

Research on the application of QKD in particular areas of IoT and applications are:

Smart Grid Security: The studies concerning securing communications in smart grids based on QKD protocols, the challenges related to the requirement of real-time operation and grid stability.

Healthcare IoT: QKD Implementations in medical device networks under the umbrella of privacy protection and regulation.

Industrial IoT: Reliability and deterministic communication Studies on the implementation of manufacturing and industrial automation.

Vehicle-to-Everything (V2X) Communication: QKD protocols in automotive systems, which solve the mobility issue and topological rapid changes.

3.2.5 Implementation Challenges and Solutions:

Studies that solve applicable issues in the implementation of QKD-IoT and solutions.

Hardware Limitations:

- ✓ Cost and complexity of quantum hardware
- ✓ Integration challenges with existing IoT infrastructure
- ✓ Environmental sensitivity of quantum systems

Network Challenges:

- ✓ Distance restrictions in quantum communication
- ✓ Network scalability issues
- ✓ Interoperability between classical and quantum systems

Security Considerations:

- ✓ Side-channel attacks on quantum systems
- ✓ Authentication in QKD protocols
- ✓ Long-term key storage and management

4. Current State of Research

4.1 Technological Maturity

The present QKD technology has already come a long way and cannot be implemented on a large scale in IoT due to pragmatic reasons:

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Achievements:

- ✓ Commercial QKD systems with 100+ km fiber transmission.
- ✓ Combination with normal optical networks.
- ✓ Quantum networks with more than two nodes are demonstrated.
- ✓ Compact quantum devices Development.

Limitations:

- ➢ High cost of quantum hardware.
- ➢ Reduced range of transmission, quantum repeaters is not used.
- ➢ Responsiveness to situations around.
- ➢ The sophisticated calibration and maintenance.

4.2 Hybrid Approaches

The most promising direction of current research is based on hybrid systems and their combination of QKD and classical cryptography:

Integration with Post-Quantum Cryptography: Integrating QKD key distribution with post-quantum cryptographic algorithms offers information-theoretic as well as practical performance. It has been studied that this method can attain the security level similar to pure QKD without any compatibility issues with the resource-constrained IoT devices.

Classical-Quantum Key Hierarchies: This is a deployment of multi-tier key management with QKD producing master keys to use with classical key derivation functions to provide secure key distribution to high numbers of IoT devices.

4.3 Simulation and Modeling Frameworks

A number of simulation environments are created to do QKD-IoT research: **QuNetSim:** Universal quantum network simulator of multiple QKD protocols and topologies.

NS-3 Extensions: Extended classics Network simulator that supports quantum communication modules.

MATLAB Quantum Toolboxes: Protocol analysis and optimization Mathematic modelling.

Frameworks based on Python: Frameworks Lightweight simulation tools to be used in education and research.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

5. Performance Analysis and Comparison

5.1 Security Analysis

Comparison of security level offered by various methods:

Information-Theoretic Security: QKD unconditional protocols have been developed on the principles of quantum mechanics. But real-life applications present weaknesses in the form of:

- Imperfect quantum devices
- Side-channel attacks
- Classical post processing vulnerability

Computational Security: Classical cryptography offers security on the basis of a computational assumption. The following threats are possible to current algorithms:

- Quantum computing advances
- Improved computing capability.
- Mathematical breakthroughs

Hybrid Security: It is possible to combine quantum and classical methods to offer both information and computational security to a key distribution and data encryption respectively to offer a strong defense against a wide range of attack vectors

5.2 Performance Metrics

The Comprehensive performance analysis across different implementation approaches is listed below:

Throughput Analysis:

- ✓ Pure QKD: 1-10 Mbps key generation rates
- ✓ Hybrid approaches: 100+ Mbps effective throughput
- ✓ Classical methods: Gigabit+ rates

Latency Comparison:

- ➢ QKD key establishment: 100-1000ms

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

- Classical key exchange: 10-100ms
- Hybrid protocols: 50-500ms

Energy Consumption:

- Quantum hardware: 10-100W per node
- Classical cryptography: 0.1-1W per device
- Hybrid implementations: 1-10W per gateway

5.3 Scalability Assessment

The study of the scalability of network within the context of various architecture strategies:

Centralized QKD:

- ✓ It can support 100-1000 devices on a central server.
- ✓ Linearity of costs with the network size.
- ✓ BMW Vulnerability Single point of failure.

Distributed QKD:

- ✓ It serves 10,000 and more devices having several QKD nodes.
- ✓ Obstacles to exponential cost growth.
- ✓ User-enhanced resilience and redundancy.

Hierarchical QKD:

- ✓ The best cost-scaling ratio.
- ✓ 100,000+ devices supported by gateway architecture.
- ✓ Real world implementation viability.

6. Challenges and Limitations

6.1 Technical Challenges

Hardware Limitations in quantum hardware: The quantum devices are experiencing strong technical limitations such as vulnerability to temperature, calibration issues and lack of operation lifetimes. The following are factors that influence the real implementation of QKD systems in different IoT architecture.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Limitations of Distance: Quantum signal attenuation is a hindrance to the immediate application of QKD by limiting direct communication to 100-200 kilometers in fibre optic networks. This limitation creates the need to have quantum repeaters or relay stations in long distance communication.

Complexity of Integration: The complexity of integration of quantum systems into the current classical IoT infrastructure is also a challenge to engineering, such as compatibility of protocols, timing synchronization, and error management.

6.2 Economic Challenges

Cost Barriers: The cost of quantum hardware (currently ranging between 100,000 to 1,000,000 per QKD system) is a barrier in terms of its expensive nature to many applications in cost-sensitive IoT.

Return on Investment: The benefits of QKD implementation over classical methods are hard to measure in terms of security, which is a challenge in making investments in IoT applications.

Market Preparedness: The quantum technology market is in its early developmental stages, and there are a few vendor selections and standardization issues influencing business sustainability. The standardization and interoperability standard must be mentioned as well.

6.3 Standardization and Interoperability

Standardization of Protocols: There are no standard QKD protocols available to use in IoT applications which prevents interoperability between solutions offered by various vendors and makes system integration difficult.

Certification and Validation: Lack of standardized procedures of certification of quantum security devices will pose a problem in validating security claims and adhering to regulatory standards.

Integration of the Legacy Systems: When integrating the QKD solutions, special attention should be paid to the backward compatibility and migration of the created solution and its integration into the existing IoT deployments.

7. Future Research Directions

7.1 Emerging Technologies

Quantum Internet Development: The quantum internet infrastructure development will allow new opportunities in safe IoT communication as quantum networking protocols and distributed quantum computing resources.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Quantum Processing Integration: QuantumKD with quantum computation capabilities at edge devices would allow establishing new security paradigm shifts and improve computational efficiency of edge devices.

Satellite-Based QKD: Quantum communication systems in space could solve the problem of distance and can cover the world because of IoT applications.

7.2 Algorithmic Advances

Machine Learning Optimization: Using the methods of artificial intelligence to optimize the QKD parameters, predict channel conditions, and promote the performance of key generation in dynamically changing IoT conditions.

Adaptive Protocol Development: Development of self-adjusting QKD protocols of dynamically changing network conditions, capabilities of devices and security requirements.

Cross-Layer Optimization: Coming up with joint techniques of optimizing quantum and classical layers to achieve better system performance.

7.3 Application-Specific Research

5G/6G Integration: Investigating QKD integration with next-generation cellular networks to provide quantum-secured IoT communication over mobile networks.

Edge Computing Security: Exploring quantum security solutions for edge computing platforms that process IoT data locally while maintaining privacy and security.

Blockchain Integration: Combining QKD with blockchain technologies to create tamper proof distributed ledgers for IoT device management and data integrity.

7.4 Practical Implementation Research:

The researcher needs to educate the client on practical implementation practices to enable them cope with the exertion involved in the therapy.

Miniaturization Initiatives: The creation of small-power quantum devices that can be used in the resource-constrained IoT systems.

Cost Cutting Measures: Investigation of the production methods, material, and design that may lead to the quantum hardware cost being very low.

Enhancement of Reliability: To improve quantum system reliability and decrease maintenance needs of long autonomous operation of IoT deployments.

8. Future Research Recommendations:

According to our full survey, we suggest the following recommendations to the future research on QKD-IoT systems:

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

8.1 Research Priority in the Immediate Future:

Development of Hybrid Architectures: Develop and optimize hybrid quantum-classical architectures that have realistic security value as well as managing the costs and scalability limits.

Performance Benchmarking: Standardized benchmarking frameworks on the analogy of QKD-IoT implementations on various standards and application scenarios.

Enhancement of the Simulation Platform: Build more advanced simulation platforms that are able to model both quantum and classical behavior of integrated systems.

8.2 Medium-term Research Goals

Proof-of-Concept Deployments:

Deploy and test real-world QKD-IoT systems in controlled settings to affirm and deny theoretical expectations and find feasible challenges.

Cost-Benefit Analysis: Develop full-fledged economics studies to determine areas of application in which QKD has apparent value propositions as compared to classical choices. Efforts to standardize: Be part of the development of industry standards to be used in integrating QKD-IoT, protocols, and security certification procedures.

8.3 Long-term Research Vision Integrating quantum Internet: Be ready to implement the transformation to quantum internet infrastructure by building frameworks and protocols that are compatible with the IoT.

Autonomous Quantum Systems: Surveys The autonomous quantum security systems are capable of self-managing and can effectively be operated with a small number of human operators in large-scale IoT applications.

Next-Generation Applications: Learn about applications that are possible due to the unique properties of quantum-secured IoT systems, including confirmable sensor networks and quantum-enhanced edge computing.

9. Conclusion

It is a general survey of the current research on the topic of quantum key distribution to the security of IoT, an analysis of 156 publications on the topic was conducted by 2018 to 2025. In our analysis, we see a fast-paced field with great improvements in theory and increasing practice implementation activities.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

Major results of our survey are:

Research Maturity: The discipline has reached a stage of departure of theoretical underpinnings to practical implementation issues, and hybrid quantum-classical methods are the most promising way to go in the near term deployment.

Technical Feasibility: The pure QKD systems present serious technical and economical difficulties, but quantum-capable edge gateways in the context of hybrid architecture demonstrate the potential of practical enhancement of internet of things security.

Performance Trade-offs: The existing implementations show that there are evident security gains with the price of complexity, latency, and extra resource consumption. The application needs, as well as threat models, are very crucial to the determination of the best balance points.

Problem of implementation: Hardware expenses, distance and complexity of integrations are major hindrances to mass adoption, however there is on-going research to resolve these issues by providing architectural solutions and technological solutions.

Future Prospects: With convergence of quantum internet progression, edge computing progression and next-generation cellular networks, there will be opportunities of revolutionizing the advances in quantum-secured IoT systems. The arena is at a pivotal point in terms of a theoretical underpinning being laid and practical application coming to reality. To overcome this disconnect, it will make sense to persist with interdisciplinary efforts between quantum physicists, computer scientists, and the engineers of the IoT systems. Future studies must focus more on hybrid systems, standardization and demonstrations as they prepare the quantum internet infrastructure transition in the future. The possible potentials of quantum-secured IoT system such as information-theoretic, protection against future quantum computing threats and improved privacy, among others is good enough reason to invest more in this promising line of research. With the further development of the IoT ecosystem and the advancement of quantum technologies, the hybridization of these two areas can probably bring revolutionary benefits to the field of safe communicational systems. The research community should not lose the sight of the long-term vision of ubiquitous quantum-secured connectivity but stay within its practical implementation issues.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

10. References

[1.] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., et al. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), 1301. https://doi.org/10.1103/RevModPhys.81.1301

[2.] Pirandola, S., Laurenza, R., Ottaviani, C., Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8, 15043. https://doi.org/10.1038/ncomms15043

[3.] Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, 8(8), 595–604. https://doi.org/10.1038/nphoton.2014.149

[4.] Alkhamisi, A. O., Alshahrani, M. M., Mabrok, M. A. (2024). Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. *Computer Communications*, 224, 159-176. https://doi.org/10.1016/j.comcom.2024.03.013

[5.] Chen, Z., Zhang, Y., Chen, S., et al. (2023). A Survey on Quantum Computing for Internet of Things Security. *Procedia Computer Science*, 221, 1670-1675. https://doi.org/10.1016/j.procs.2023.08.155

[6.] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, 7(7), 6457-6480. https://doi.org/10.1109/JIOT.2019.2958788

[7.] Park, C., et al. (2021). Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. *Applied Sciences*, 11(9), 3767. https://doi.org/10.3390/app11093767

[8.] Rajasekar, V., Premalatha, J., Sathya, K. (2025). Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*, 4. https://doi.org/10.3389/frqst.2025.1575498

[9.] Li, X., Wang, J., Zhang, H., et al. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports*, 15, 1023. https://doi.org/10.1038/s41598-024-84427-8

[10.] Lohachab, A., & Karambir (2018). Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3166511

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

[11.] Panda, S. K., Mishra, S. K., Satapathy, S. K., et al. (2022). Research on Quantum Key Distribution Method Based on Internet of Things Communication. *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)*, pp. 708-713. https://doi.org/10.1109/COM-IT-CON54601.2022.9898936

[12.] Zhang, L., Wang, Y., Chen, M. (2025). Feasibility discussion of quantum cryptography for Internet of Things security: a literature review. *Optical and Quantum Electronics*, 57, 402. https://doi.org/10.1007/s11082-025-08168-2

[13.] Senthilkumar, C., Manikandan, M. S. K., Ananth, J. P. (2021). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Personal and Ubiquitous Computing*, 25, 339–351. https://doi.org/10.1007/s00779-021-01546-z

[14.] Singh, A., Kumar, R., Patel, S. (2023). Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol. *arXiv preprint*, arXiv:2312.05609. https://doi.org/10.48550/arXiv.2312.05609

[15.] Sharma, P., et al. (2025). Quantum Cryptography for Secure IoT Networks: Implementing the BB84 Protocol. In: *Advances in Computer Science and Engineering* (pp. 287-298). Springer. https://doi.org/10.1007/978-981-96-3247-3_25

[16.] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175-179).

[17.] Mishra, A., Singh, K., Verma, R. (2024). A Secure Method of Communication Through BB84 Protocol in Quantum Key Distribution. *International Journal of Computer Applications*, 185(45), 1-8.

[18.] Cozzolino, D., Da Lio, B., Bacco, D., Oxenløwe, L. K. (2022). Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3. *Sensors*, 22(16), 6284. https://doi.org/10.3390/s22166284

[19.] Abdullah, A. M., et al. (2025). A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection. *IEEE Access*, 13, 8234-8247. https://doi.org/10.1109/ACCESS.2025.10872935

[20.] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661-663. https://doi.org/10.1103/PhysRevLett.67.661

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/1/013

[21.] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2), 441-444. https://doi.org/10.1103/PhysRevLett.85.441

[22.] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145

[23.] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886), 802-803. https://doi.org/10.1038/299802a0

[24.] Hughes, R. J., et al. (2013). Network-centric quantum communications with application to critical infrastructure protection. *Los Alamos National Laboratory Report*, LA-UR-13-20808.

[25.] Diamanti, E., Lo, H. K., Qi, B., Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, 2, 16025. https://doi.org/10.1038/npjqi.2016.25