Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Implementation of Quantum Key Distribution with Classical Algorithms

Dr. P. Dhana Lakshmi
Assistant professor
Department of Electronics and Communication Engineering,
Acharya Nagarjuna University, Guntur, A.P, India

P. Modini, I. Kiran Kumar,
I. Bharath Srikanth
UG Students
Department of Electronics and Communication Engineering,
Acharya Nagarjuna University, Guntur, A.P, India

Abstract - Implementing Quantum Key Distribution (QKD) using the BB84 protocol. The system allows two users to securely share a secret key by simulating quantum protocol using classical computer algorithms to manage and process the data. Random bits are generated, encoded into quantum states, and transmitted virtually between sender and receiver. After transmission, both users compare selected bits to detect error. Classical algorithms are then applied for error correction, key verification, and privacy amplification to produce a final shared secret key. By combining the power of quantum simulation with classical computing algorithms, the project achieves a secure, efficient, and practical approach to key distribution. This integration demonstrates how cloud-based quantum tools and classical algorithms can work together to build reliable and secure communication systems.

Key words: Quantum Key Distribution, BB84 Protocol, Quantum Cryptography, Classical Algorithms, Secure Key Exchange, Error Correction, Privacy Amplification.

I.INTRODUCTION

In General, Classical Cryptography is the fundamental approach to secure communication by converting readable data into ciphertext. This technique is used by most of the classical computers till today. In this process keys play a crucial role. An encryption key is used to convert plaintext into a ciphertext, while a decryption key is used to convert it back into its original form. Based on the key used classical cryptography is classified into two types. They are Symmetric encryption [i] and Asymmetric Encryption [ii].

In Symmetric Encryption a Single Key is used by the sender and receiver for encryption and decryption of data. Whether, In Asymmetric Encryption a Public key is used for Encryption by anyone with the key and a Private secure key, which only the receiver was able to decrypt it. Classical cryptography broadly depends on Mathematical Algorithms like Advanced Encryption standards [AES], Data Encryption Standards [DES]. These are highly efficient cryptographic techniques but, they effected by the Powerful Quantum computers.

Quantum Cryptography is a Secure Communication Approach that Uses the Principles of Quantum mechanics to protect information against eavesdropping. Unlike classical cryptographic methods that depends on computational complexity, Quantum cryptography ensures security through the fundamental behavior of quantum particles, where any attempt to measure the transmitted data unavoidably disturbs their state and reveals the presence of an intruder. The most well-known application is Quantum Key Distribution (QKD), which enables two parties to generate and share a secret encryption key with provable security. This method leverages quantum properties such as superposition and entanglement, making it theoretically resistant to attacks even from powerful quantum computers.

In practice, QKD is implemented through protocols such as BB84 protocol and E91 protocol. where quantum bits (qubits) are transmitted using different bases or entangled states. These protocols rely on quantum operations realized through gates like Hadamard gate for creating superposition, Pauli-X gate (I) and Pauli-Z gate (II) for state transformations by bit flipping and phase flipping, and CNOT gate for entanglement generation. Despite its strong theoretical security, QKD faces practical drawbacks including limited transmission distance, vulnerability to device imperfections, high implementation cost, and susceptibility to side-channel attacks.

In this study, the implementation of Quantum Key Distribution is carried out using the BB84 protocol.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Following the quantum key generation phase, classical algorithms are employed for error correction and privacy amplification to improve the reliability and security of the generated key. While physical losses in the quantum channel cannot be eliminated, their impact on key integrity and secrecy is mitigated through these post-processing techniques, enabling effective integration of quantum communication with classical cryptographic methods.

II. LITERATURE REVIEW

The development of Quantum Key Distribution (QKD) represents a major advancement in secure communication, where security is based on the principles of quantum mechanics. The origin of QKD can be traced to the pioneering work of Charles H. Bennett and Gilles Brassard, who introduced the BB84 protocol in 1984 [1]. Their work demonstrated that quantum states can be used for secure key exchange with the ability to detect eavesdropping. The theoretical foundation of QKD was further strengthened by Vishal Sahni [2], who introduced key concepts of quantum computing, and by Michael A. Nielsen and Isaac L. Chuang [3], whose work provided a comprehensive framework for quantum computation and information theory. These studies established the basis for the design and analysis of QKD systems. Subsequent research focused on protocol analysis and comparison. Begimbayeva Y. and Zhaxalykov T. [4] analyzed multiple QKD protocols including BB84, B92, and E91 protocol. Chankyun Lee, Ilkwon Sohn, and Wonhyuk Lee [5] focused on eavesdropping detection mechanisms in BB84 systems. Similarly, Bahl K. [6] studied the efficiency of BB84 and B92 protocols under noise and attack scenarios using simulation techniques. Furthermore, Ain N. U., Waquar M., Bilal A., and Haider A. K. [11] proposed a hybrid approach combining BB84 and E91 protocols to improve resilience and enhance eavesdropper detection. As the field progressed, research shifted toward implementation and practical realization. Kosik M. and Moreno J. [7] implemented the BB84 protocol using Amazon Braket, demonstrating the feasibility of cloud-based quantum simulations. Tat-Thang, Thanh-Toan Dao, and Nhu-Quynh [8] developed a QKD application integrating quantum and classical communication channels. Similarly, Mozo H. *et al.* [9] proposed a hybrid framework combining simulated BB84 with AES-256 encryption for secure file transmission. In addition, quantum simulation platforms such as Qiskit, developed by IBM, have enabled researchers to design and simulate quantum circuits, supporting practical experimentation without requiring full quantum hardware. In parallel, optimization and security enhancement have been key research areas. Attena T., Bosman J. W., and Neuman N. [10] focused on optimizing decoy-state BB84 protocol parameters to improve efficiency. Devashish, Tan E., Nahar S., and Kamin L. [11] provided security proofs for decoy-state BB84 protocols, strengthening their reliability. Furthermore, Gdowski B. [14] introduced machine learning based techniques using Tree Parity Machines to enhance error correction and improve the final key rate. Recent research has also addressed real-world deployment and scalability. Saiyed A. I. [12] proposed hybrid architectures combining QKD with classical encryption for end-to-end security. Nair V. [13] explored the integration of QKD into existing communication networks, focusing on practical implementation challenges. Additionally, Tennessee Tech University [15] applied greedy algorithms for optimizing quantum server placement to ensure efficient and reliable key distribution. Despite these advancements, QKD systems still face challenges such as channel loss, noise, limited transmission distance, and high implementation costs. However, classical post-processing techniques, including error correction and privacy amplification, help mitigate the impact of these issues on key reliability and security. In summary, the evolution of QKD from the introduction of the BB84 protocol to modern hybrid and optimized implementations—demonstrates continuous progress toward practical and secure communication systems. The contributions of various researchers in protocol design, implementation, optimization, and integration highlight the growing maturity and future potential of QKD technologies.

III. METHODOLOGY

The proposed system implements Quantum Key Distribution based on the BB84 protocol, integrating quantum state simulation with classical post-processing techniques. Quantum operations are simulated using Qiskit Aer, while key reconciliation and security enhancement procedures are executed using classical algorithms. The methodology consists of sequential phases: quantum state preparation, transmission, measurement, basis reconciliation, error correction, and privacy amplification.

Quantum State Preparation: The sender (Alice) generates a random sequence of bits (0s and 1s). Each bit is encoded into a photon using a randomly chosen basis. This encoding uses the principle of Superposition

Bit sequence: $b_i \in \{0,1\}$

Basis sequence: $\Theta_i \in \{z, x\}$

Each bit is encoded into a quantum state depending on the chosen basis:

Rectilinear basis (Z): $0 \rightarrow |0\rangle, 1 \rightarrow |1\rangle$

Diagonal basis (X): $0 \rightarrow |+\rangle = |0\rangle + |12$, $1 \rightarrow |-\rangle = |0\rangle - |12$

Quantum Transmission

The encoded qubits are transmitted through a quantum channel. In simulation, state vectors represent qubits.

If an eavesdropper measures a qubit in the wrong basis, the state collapses probabilistically, introducing errors.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The probability of correct measurement is:

Measurement at Receiver

The receiver measures each incoming photon. For each photon, he randomly chooses a basis (+ or ×).

Sender and receiver communicate over a classical public channel. They share only their basis choices, not the actual bit values.

The receiver (Bob) independently selects a random basis:

$$\theta i1 \in \{z, x\}$$

I. **Pauli-x Gate**: The Pauli-X gate acts like a classical NOT gate but on a quantum level. It flips the state of a qubit. If the qubit is in the state **|0⟩**, it becomes **|1⟩**, and if it is **|1⟩**, it becomes **|0⟩**. Mathematically, it is represented as:

$$X = 0110$$

If too many bits differ, it indicates interference or eavesdropping. This relies on the Heisenberg Uncertainty Principle—measurement disturbs the system.

For a block of size n:

$$P(B) = \oplus_{i \in B} x_i \qquad (1)$$

Where $P(B) = X_1 \oplus x_2 \oplus X_3 \ldots \ldots$

II. **Hadamard Gate:** The Hadamard gate (H gate) is more powerful because it creates superposition, which is a key feature of quantum computing. It transforms a definite state into a combination of both possible states. Its matrix form is:

$$H = 12\ 111\text{-}1$$

Measurement outcomes depend on basis alignment.

The measurement results are collected and plotted as a frequency distribution graph, showing occurrences of bit values (0 and 1).

Basis Reconciliation (Sifting)

Alice and Bob compare their bases over a classical channel. Keep only the bits where both used the same basis, Discard the rest. It results a shorter sequence called the sifted key

Error Correction (Cascade-Based Approach)

Error correction is performed using parity checks. They publicly compare a small subset of the sifted key.

If parity differs between sender and receiver:

$$P_A \neq P_B \Rightarrow error\ exists$$

Binary search is applied to locate the error. This process is repeated in multiple rounds to minimize residual errors.

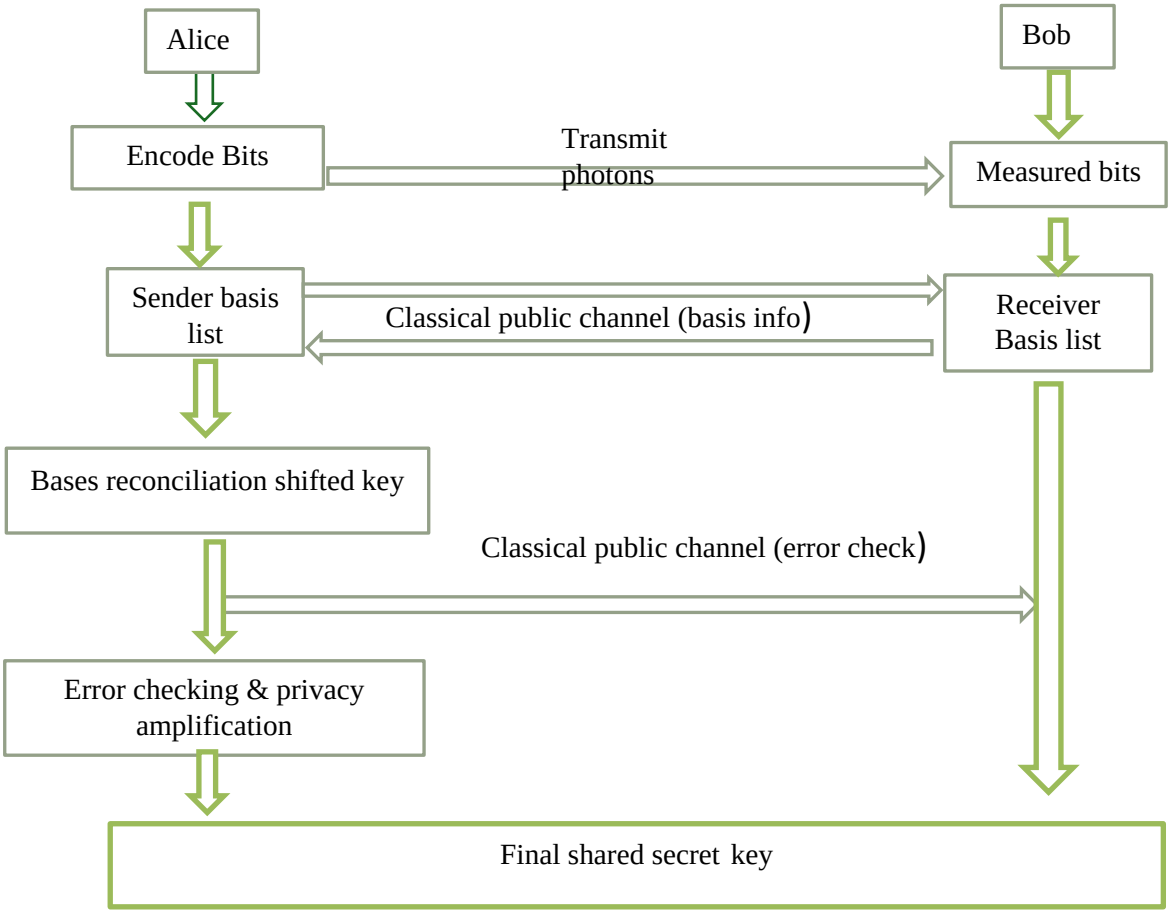

FIG 1: Methodology for QKD using BB84 with Classical Algorithms

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Privacy Amplification

To eliminate leaked information, the corrected key is compressed using a hash function such as SHA-256.
Both sender and receiver end up with an identical, secure key. This key can now be used for encryption (e.g., one-time pad or symmetric cryptography(i)).
Final key:

$$Kf=H(Kc) \quad (2)$$

Where Kcis corrected key, H is hash function
Key length reduction:
|Kf|<|Kc|
This ensures:
I(E,Kf)≈0

(where *I* is mutual information between Eve and final key).

IV. RESULTS

The performance of the proposed Quantum Key Distribution system based on the BB84 Protocol was evaluated using an 8-qubit simulation. The measurement results obtained from the quantum circuit are represented as a histogram. This histogram illustrates the frequency of observed bitstrings after quantum measurement. In this histogram an extra outcome is added as carry. Ideally, due to the probabilistic nature of quantum mechanics and random basis selection, the distribution of outcomes appears approximately uniform across possible states. This indicates that the system successfully preserves randomness, which is a critical requirement for secure key generation. Any deviation from uniformity can be attributed to factors such as basis mismatch or measurement uncertainty. However, no significant bias is observed, confirming that the simulation behaves consistently with theoretical expectations. Following measurement and basis reconciliation, sifted keys were generated and further processed through error correction and privacy amplification.

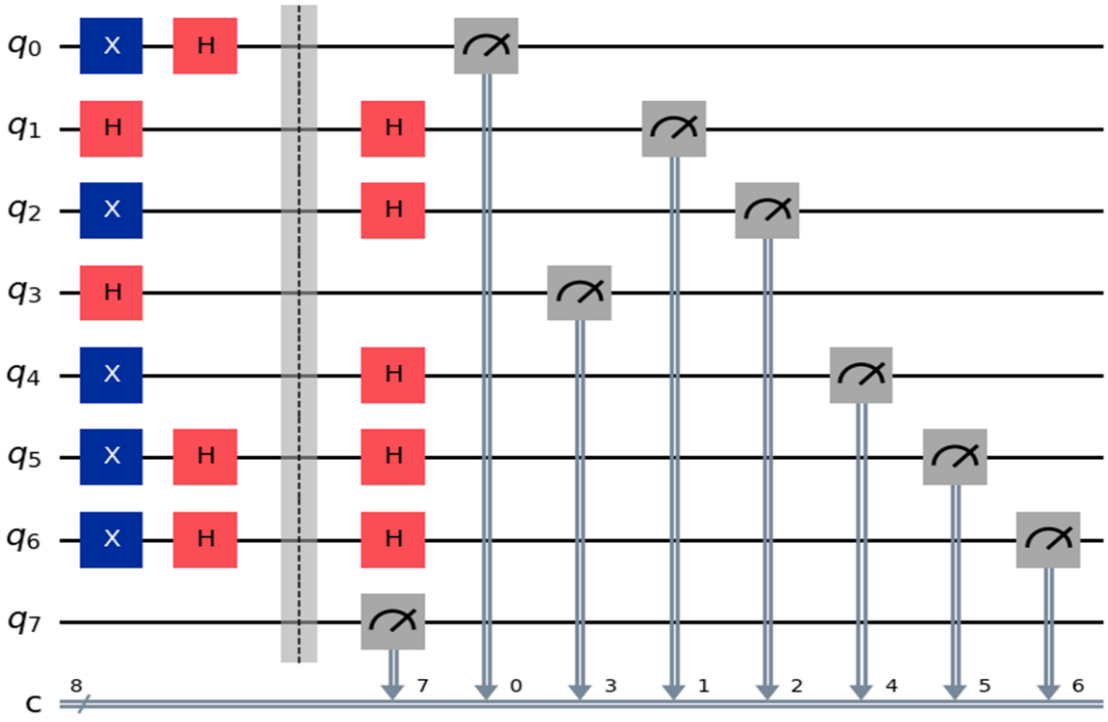

FIG 2: Quantum circuit represents quantum key distribution using 8 Qubits

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

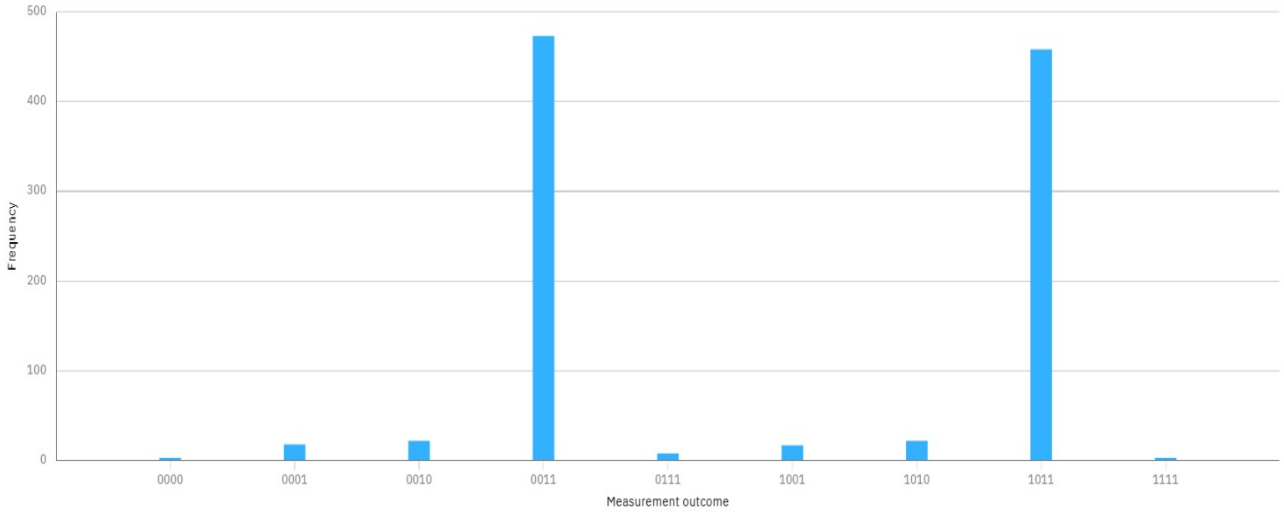

FIG 3: Measurement Outcome Frequency Distribution for 8-Qubit BB84 Protocol Simulation

The final secure keys obtained in different simulation runs are:
Final Secure Key: 2cc5063c8b289336c033bb52997d889aa530107c828fb493daf8a73627fa54cc
Final Secure Key: 42eaa10c1740cff3580a79e203d37380b2c491601dfde8c45f414f52db5c9a3c
Final Secure Key: 459c2daec5458568864215c57d12fa0ae28243b080971bb90d09fe020f8f265e

V. CONCLUSION

This work presents the successful implementation of a Quantum Key Distribution system based on the BB84 Protocol using quantum simulation integrated with classical post-processing techniques. The measurement outcome distribution obtained from the 8-qubit simulation reflects the probabilistic nature of quantum mechanics, ensuring true randomness in the generated data. The variation observed in the final secure keys across multiple runs demonstrates high entropy and the absence of predictable patterns, which are essential properties for strong cryptographic systems. The application of basis reconciliation ensures that only valid and correlated bits are retained, while error correction improves consistency between communicating parties. Furthermore, privacy amplification enhances security by eliminating any partial information that could have been exposed during transmission, resulting in a shorter but highly secure final key. The overall system effectively combines quantum principles with classical algorithms to achieve reliable, secure, and efficient key generation suitable for modern cryptographic applications. Future work can extend the system to real quantum hardware, scale it to larger qubit sizes, and improve efficiency through advanced error correction and privacy amplification techniques. Additionally, integrating the approach into practical quantum communication networks can support real-world secure applications.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang," Quantum Computation and Quantum Information", Cambridge University Press, 2010.
[2] V. Sahni," Quantum Computing", Tata McGraw-Hill, 2007
[3] A. Jain, A. Pathak, and V. K. Jain, "Optimizing the decoy-state BB84 QKD protocol parameters," Quantum Information Processing, vol. 20, Art. no. 154, Apr. 2021, Doi: 10.1007/s11128-021-03074-7.
[4] C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in BB84 quantum key distribution protocols," IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689–2701, Sep. 2022, Doi: 10.1109/TNSM.2022.3165202.
[5] J. Li, P. Zheng, Z. Li, K. Xue, Z. Xie, and N. Yu, "Integration of quantum key distribution networks and classical networks: An evolution perspective," IEEE Network, vol. 39, no. 3, pp. 180–187, May 2025, Doi: 10.1109/MNET.2025.3537691
[6] N. Ul Ain, M. Waqar, A. Bilal, A. Kim, H. Ali, and U. U. Tariq, "A novel approach based on quantum key distribution using BB84 and E91 protocol for resilient encryption and eavesdropper detection," IEEE Access, vol. 13, pp. 32819–32833, Feb. 2025, Doi: 10.1109/ACCESS.2025. 3539178..
[7] B. Gdowski, M. Mehic, and M. Niemiec, "Enhancing security of error correction in quantum key distribution using tree parity machine update rule randomization," Applied Sciences, vol. 15, no. 14, Art. no. 7958, Jul. 2025, Doi: 10.3390/app15147958.
[8] K. Dehingia and N. Dutta, "Hybrid quantum key distribution framework: Integrating BB84, B92, E91, and GHZ protocols for enhanced cryptographic security," Concurrency and Computation: Practice and Experience, Jul. 2025, Doi: 10.1002/cpe.70221.
[9] D. Tupkary, E. Y.-Z. Tan, S. Nahar, L. Kamin, and N. Lutkenhaus, "QKD security proofs for decoy-state BB84: Protocol variations, proof techniques, gaps and limitations," *arXiv*, Doi: 10.48550/arXiv.2502.10340, 2025
[10] H. E. Mozo, "Quantum-classical hybrid encryption framework based on simulated BB84 and AES-256: Design and experimental evaluation," arXiv preprint,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

arXiv:2511.02836[cs.CR],June,2025,Doi:10.48550/arXiv.2511.02836.

[11] A. Raj and V. Balachandran, "A hybrid encryption framework combining classical, post-quantum, and QKD methods," arXiv preprint, arXiv:2509.10551 [cs.CR], Sep. 2025, Doi: 10.48550/arXiv.2509.10551.

[12] M. Kosik and J. Moreno, "Implementing BB84 quantum key distribution on Amazon Braket: A practical guide," Amazon Web Services (AWS) Quantum Technologies Blog, Sep. 2025**.**

[13] Y. Begimbayeva and T. Zhaxalykov, "Research of quantum key distribution protocols: BB84, B92, E91," Scientific Journal of Astana IT University, vol. 10, Jun. 2022, Doi: 10.37943/QRKJ7456

[14] Tennessee Tech University, "Quantum research," Cybersecurity Education, Research and Outreach Center (CEROC),2025.https://www.tntech.edu/ceroc/quantum/quantumresearch.php

[15] T.-T. Nguyen, T.-T. Dao, and N.-Q. Luc, "Develop a quantum key distribution application based on the BB84 protocol combined with a classical channel," Int. J. Electrical Engineering and Informatics, vol. 14, no. 2, 2024, Doi: 10.11591/eei. v14i2.9051.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)