A Quantum Encryption Algorithm based on the Rail Fence Mechanism to Provide Data Integrity

Arshad Ali
Department of Computer and Information System, Islamic University of Madinah, Al-Madinah al-Munawwarah, Saudi Arabia
a.ali@iu.edu.sa

M. A. H. Farquad
Department of Computer Information Science, Higher Colleges of Technology, Ras Al Khaimah, United Arab Emirates
amohammed3@hct.ac.ae

C. Atheeq
GITAM University, Hyderabad, India
atheeq.prof@gmail.com (corresponding author)

C. Altaf
Lords Institute of Engineering and Technology, Hyderabad, India
altaf.ece@gmail.com

Received: 14 September 2024 | Revised: 6 October 2024 and 26 October 2024 | Accepted: 29 October 2024

 DOI: https://doi.org/10.48084/etasr.8993

ABSTRACT

The rapid development of quantum computer technology poses an increasing threat to conventional encryption algorithms, and accordingly, more advanced security practices need to be developed. The current paper presents an innovative quantum cryptographic mechanism that combines classical encryption techniques with quantum principles such as superposition, entanglement, and uncertainty to enhance data security in digital communication. The proposed scheme, defined as Enhanced Quantum Key Distribution (EQKD), demonstrates superior performance in key metrics, including Quantum Bit Error Rate (QBER), fidelity, key distribution rate, and resilience to eavesdropping. In particular, EQKD achieves lower QBER and higher fidelity over longer distances while also enhancing key generation efficiency and increasing the probability of detecting eavesdropping attempt. These findings highlight the effectiveness of EQKD in improving the security and reliability of quantum cryptographic systems.

Keywords-quantum cryptography; integrity; encryption; communication

I. INTRODUCTION

With the constant evolution of information technology, secure data transmission has become a top priority. However, traditional cryptographic methods that rely on mathematical complexity, are continuously threatened by the exponential growth of quantum computational power [1]. Quantum cryptography is recently a developed method of encryption that utilizes the principles of quantum mechanics such as superposition and entanglement to create secure, eavesdrop-proof communication channels that can withstand emerging technology's computational challenges [2]. Quantum Key Distribution (QKD) is a powerful quantum protocol that uses these mechanisms to securely generate and exchange cryptographic keys between communicating parties [3]. Except this, quantum cryptography employs classical encryption algorithms like rail fence and helical to protect messages. To seamlessly integrate this with the OKD infrastructure to maintain security and performance, efficient encryption and decryption mechanisms are needed.

Quantum cryptographic systems offer enhanced security, however, they face considerable challenges that hinder their widespread adoption [4]. Key obstacles to the broader implementation of quantum cryptography include the following:

A. Photon Loss

Quantum communication typically occurs over fiber optic cables, and photon loss occurs as the distance increases, reducing the effectiveness of quantum key distribution over large networks.

B. Detector Vulnerabilities

The quantum detectors used in quantum cryptography systems are sensitive and prone to side-channel attacks, where vulnerabilities in the hardware are exploited to gain access to communication.

C. Environmental Sensitivity

Quantum systems are highly sensitive to environmental factors such as temperature, electromagnetic interference, and vibrations, which can disrupt quantum states and reduce system reliability.

D. Cost and Complexity

Building, maintaining, and scaling quantum cryptographic systems is currently expensive and complex due to the need for single-photon sources, quantum memories, and other advanced technologies.

This study seeks to address these challenges by introducing a novel quantum cryptographic mechanism that integrates classical encryption with quantum principles. In contrast to previous works, our approach prioritizes practical implementation and strengthened security measures, aiming to overcome real-world obstacles and advance the development of quantum-secure communication systems.

II. RELATED WORK

In the literature survey, the work done in [5] focuses on the design of quantum communication protocols within the realm of quantum cryptography. The primary objective of their study is to compare the performance of various quantum-inspired algorithms, specifically Quantum Inspired Genetic Algorithm (QIGA), Quantum Inspired Cuckoo Search Algorithm (QICSA), and Quantum Inspired Tabu Search Algorithm (QITSA), against traditional classical algorithms such as GA, CSA, and TSA. While their work provides valuable insights, it is important to note certain limitations and areas that could benefit from further exploration.

In the context of quantum cryptography, authors in [6] proposed a Dynamic Quantum Secret Sharing (DQSS) protocol that leverages the measurement properties of Greenberger–Horne–Zeilinger (GHZ) state along with the controlled-NOT (CNOT) gate to achieve greater quantum bit (qubit) efficiency compared to existing DQSS protocols. This protocol is also designed to simplify the process of adding new agents. Unlike some traditional approaches, the DQSS protocol does not require new participants to prepare quantum states or engage in complex quantum operations, making it more accessible and easier to implement in dynamic environments where the network of participants may frequently change. However, certain limitations are identified, particularly in scenarios where multiple agents need to be revoked. In these situations, the protocol's performance tends to decline, potentially affecting its overall efficiency and reliability. This highlights a trade-off between the ease of adding new participants and the challenges associated with revoking access, which could be a critical factor in practical implementations. These observations suggest that while the DQSS protocol offers significant benefits in terms of qubit efficiency and operational simplicity, further research is needed to address the performance issues related to agent revocation. The choreographed distributed electronic voting scheme proposed in [7] introduces a robust security framework using quantum technologies. The scheme employs quantum group blind signatures, the QKD protocol, and quantum one-time pads to ensure unconditional security, effectively safeguarding the privacy and anonymity of message owners. Additionally, the scheme allows a group supervisor to trace the source of a signature in the event of a dispute, enhancing accountability. Notably, the proposed methods are scalable, accommodating both signers and users, and they introduce a crucial authentication property to the electronic voting process, thereby strengthening the overall security and integrity of the voting system. In [8], the author proposed and examined a quantum Vernam cipher to improve quantum communication security. This approach utilizes entanglement to enable key recycling, presenting a novel way to secure quantum communication systems. The study also highlighted several challenges in implementing quantum cryptographic schemes. These challenges include the intrinsic complexity of quantum systems and operations, the significant resources required, and the technical difficulties of manipulating and transmitting quantum states. All these factors present considerable barriers to the implementation of quantum cryptographic protocols.

Authors in [9] highlighted that the Rail Fence cipher is particularly susceptible to cryptanalysis due to its predictable patterns, making it vulnerable to brute-force attacks and easily decipherable when some plaintext is known. Even when combined with other ciphers, the algorithm still relies on weak transposition techniques. Modern cryptanalysis methods can easily break any algorithms, especially with limited key lengths and patterns [10]. An enhanced version of the rail fence cipher, known as Block Rail Fence Cipher, is proposed in [11]. However, while this approach raises the algorithm's complexity, it still heavily depends on transposition which remains vulnerable to cryptanalysis when the encryption method is identified. The rail optimization method is limited by the message length, and while complexity increases, the security may not scale adequately for larger data sets.

While this study does not extensively address the need for standardized protocols and regulatory frameworks, their importance is recognized for the broader adoption of quantum cryptography systems. In future work, we can explore these aspects in detail to ensure better alignment with industry standards and interoperability requirements.

III. PROPOSED SYSTEM

The proposed method leverages the principles of quantum mechanics to establish a secure communication framework, addressing the vulnerabilities inherent in classical cryptographic techniques. This approach incorporates the following key quantum concepts:

A. Quantum Key Distribution using the Uncertainty Principle

The process begins with the implementation of QKD, which relies on the quantum uncertainty principle. This principle asserts that certain pairs of physical properties, such as position and momentum, cannot be measured simultaneously with arbitrary precision. In our proposed method, QKD is used to securely generate and distribute cryptographic keys between communicating parties. Any attempt to intercept or measure these quantum states introduces detectable disturbances, enabling the detection of eavesdropping and ensuring the integrity of the key distribution process. The foundation of QKD is based on the Heisenberg Uncertainty Principle, which can be expressed in (1):

$$\Delta_x \cdot \Delta_p \geq \frac{\hbar}{2} \quad (1)$$

where Δ_x represents the uncertainty in position, Δ_p is the uncertainty in momentum, and ħ is the reduced Planck's constant. This principle ensures that any measurement of a quantum state introduces a disturbance, making eavesdropping detectable.

The rate at which secure keys can be generated using QKD, denoted as R_{QKD}, is calculated as follows:

$$R_{QKD} = P_d \cdot \left(1 - 2Q_\mu\right) \cdot \log_2\left(\frac{1+Q_\mu}{1-Q_\mu}\right) \quad (2)$$

where P_d is the probability of detecting a photon at the receiver's end, and Q_μ is the QBER, representing the rate of errors due to noise and eavesdropping.

The probability of detecting an eavesdropper (Eve) during the key exchange can be modeled in (3):

$$P_{detect} = 1 - (1 - p_e)^n \quad (3)$$

where P_{detect} is the probability of detecting eavesdropping, p_e is the probability that a single bit of the key has been intercepted, and n is the number of qubits exchanged. After detecting and correcting errors, and applying privacy amplification, the final secure key rate can be expressed by:

$$R_s = R_{QKD} \cdot \left[1 - H_2\left(Q_\mu\right) - f_{EC} \cdot H_2\left(Q_\mu\right)\right] \quad (4)$$

where R_s represents the secure key rate after error correction and privacy amplification, f_{EC} is the efficiency of the error correction protocol, and $H_2\left(Q_\mu\right)$ denotes the binary entropy function defined as:

$$H_2\left(Q_\mu\right) = -\,Q_\mu \cdot \log_2(Q_\mu) - (1 - Q_\mu) \cdot \log_2(1 - Q_\mu) \quad (5)$$

These equations establish the foundation for implementing a secure QKD protocol, ensuring that any attempts to intercept or measure the quantum states are immediately detected, thus preserving the integrity of the key distribution process.

B. Secure Communication through Quantum Entanglement

Quantum entanglement is being used to establish secure communication channels. By distributing entangled particles between the communicating parties, the method ensures that any interception or measurement attempt by an adversary disrupts the entangled state, alerting the legitimate users. This property of entanglement provides an additional layer of security, making the communication channel resilient to interception.

The fundamental entangled state, often used in quantum communication, is called the Bell state. One of the maximally entangled Bell states can be expressed by:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (6)$$

where $|\Phi^+\rangle$ represents the entangled state, and $|00\rangle, |11\rangle$ are the possible states of two entangled qubits.

The correlation between measurements on entangled particles by two parties, commonly referred to as Alice (the sender) and Bob (the receiver), is given by:

$$\langle \mathrm{A.B} \rangle = -\cos(\theta_A - \theta_B) \quad (7)$$

where $\langle \mathrm{A.B} \rangle$ is the expected correlation between Alice's and Bob's measurement results, and θ_A, θ_B are the measurement angles chosen by Alice and Bob, respectively.

Fidelity measures how closely the actual entangled state matches the ideal entangled state after transmission or processing, as represented in (8):

$$F = \langle \Psi_{ideal} | \rho | \Psi_{ideal} \rangle \quad (8)$$

where F is the fidelity of the entangled state, $|\Psi_{ideal}\rangle$ is the ideal entangled state (e.g. a Bell state) and ρ is the density matrix of the actual entangled state after any potential interference.

If an adversary (Eve) attempts to measure or intercept the entangled particles, the entanglement will be disturbed, which can be detected by analyzing the violation of Bell's inequality:

$$S = |\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle| \quad (9)$$

where S is the Bell parameter, and $\langle A_i B_j \rangle$ are the correlations of measurements taken by Alice and Bob with different settings A_i and B_j. For entangled particles, quantum mechanics predicts $S \leq 2\sqrt{2}$. If S deviates significantly from this value, it indicates that the entanglement has been disturbed, suggesting potential eavesdropping.

C. Data Transmission using Quantum Superposition

Quantum systems, capable of existing in multiple states simultaneously, are used to transmit data securely. Security is further enhanced by encoding information in quantum states through the principle of superposition. This approach ensures that the cryptographic keys generated are inherently resistant to interception and decryption, even by advanced computational techniques.

The superposition of quantum states denoted as $|\Psi\rangle$, can be expressed by:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (10)$$

where $|0\rangle$ and $|1\rangle$ are the basis states (e.g. the computational basis) and α and β are complex probability amplitudes, with $|\alpha|^2 + |\beta|^2 = 1$. This superposition state allows the qubit to be

in both states simultaneously, which forms the basis for encoding information securely.

The probability of measuring the qubit in a particular state (either |0⟩|0\rangle|0⟩ or |1⟩|1\rangle|1⟩) after superposition, is given by:

$$P(|0\rangle) = |\alpha|^2, P(|1\rangle) = |\beta|^2 \quad (11)$$

where $P(|0\rangle)$ is the probability of the qubit being measured in the $|0\rangle$ state and $P(|1\rangle)$is the probability of the qubit being measured in the $|1\rangle$ state. These probabilities are determined by the amplitudes α and β, which are used to encode the information. Because the qubit exists in a superposition, the exact state remains unknown until measured, making it resistant to interception and ensuring the security of the transmitted data.

IV. RESULTS AND DISCUSSION

The proposed quantum cryptographic mechanism was implemented and tested using MATLAB R2023a on a system equipped with an Intel Core i7 processor and 16 GB of RAM. To evaluate the mechanism's performance, key parameters including QBER, fidelity, and R_{QKD} were analyzed. Additionally, the system's resilience to eavesdropping and its throughput in secure key generation were assessed. These metrics offered a comprehensive view of the system's security, efficiency, and robustness against potential quantum attacks.

Figure 1 illustrates the impact of distance on OBER for both traditional QKD and the Enhanced Quantum Key Distribution (EQKD) methods. As the distance between communicating parties increases, QBER also rises for both methods due to signal degradation. However, the EQKD method consistently maintains a lower QBER, indicating improved accuracy in preserving secure communication over greater distances.

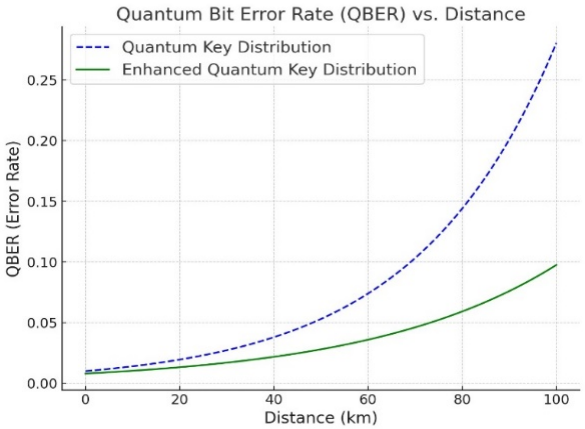

Fig. 1. Comparison of quantum bit error rate versus distance.

Fidelity, which measures the preservation of the quantum state, declines as distance increases for both methods, as shown in Figure 2. Nonetheless, the EQKD method maintains higher fidelity across all distances reinforcing its effectiveness in providing more reliable and secure communication in quantum networks.

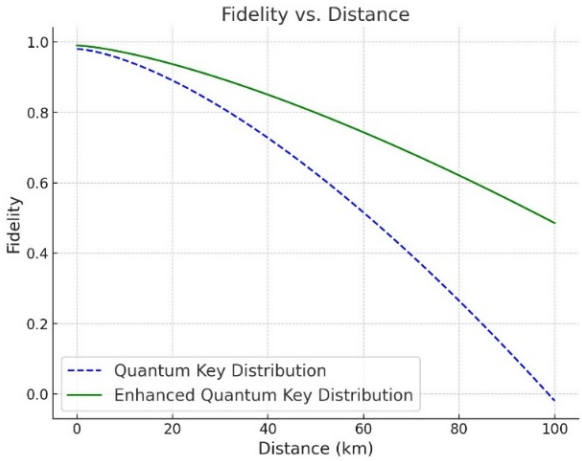

Fig. 2. Comparison between fidelity and distance.

Figure 3 compares how R_{QKD} changes as distance increases, showing a decrease in the key distribution rate for both methods. The EQED method again outperforms the traditional approach by maintaining a higher R_{QKD} across all distances.

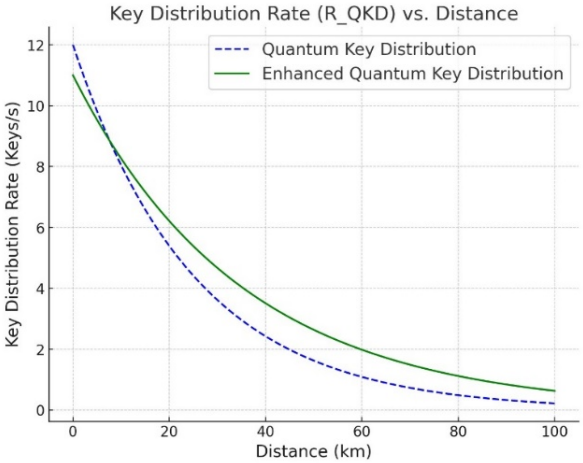

Fig. 3. Comparison between key distribution rate and distance.

Figure 4 displays the eavesdropping detection probability as the number of qubits increases, showing a clear rise in this parameter. The enhanced method reaches a higher detection probability more rapidly, reflecting its superior sensitivity to eavesdropping attempts. The proposed system excels in Faster Eavesdropping Detection, Improved Sensitivity, and Real-Time Monitoring.

Figure 5 illustrates the relationship between fidelity and QBER for QKD and EQKD. As the rate increases, fidelity declines, indicating a degradation in the quantum state quality due to increasing errors. Nevertheless, the EQKD consistently maintains higher fidelity across the full range of QBER values, demonstrating its improved ability to preserve the quantum state's integrity even in the presence of errors.

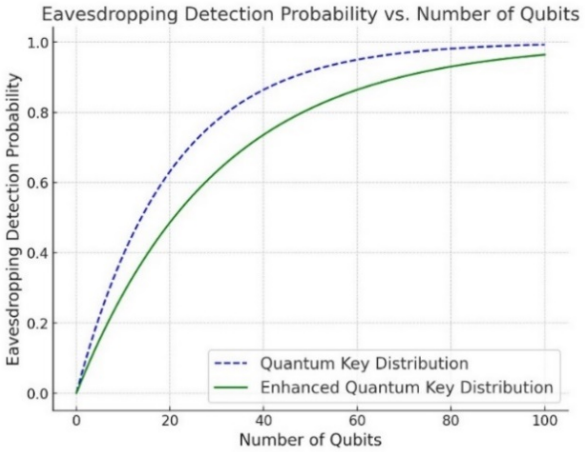

Fig. 4. Comparison between eavesdropping detection probability and number of qubits.

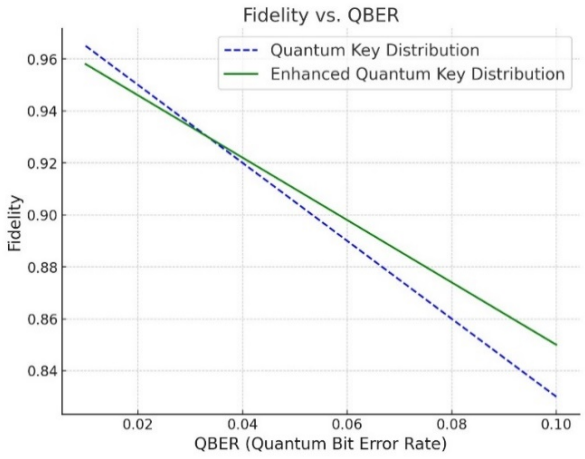

Fig. 5. Comparison of eavesdropping detection probability versus number of qubits.

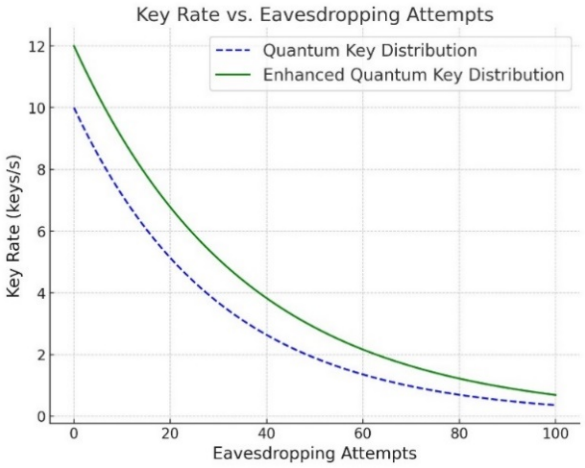

Fig. 6. Relationship between key rate and eavesdropping attempts for QKD and EQKD.

Figure 6 depicts the effect of eavesdropping attempts on the key rate for QKD and EQKD methods. As the eavesdropping attempts increase, the key rate decreases for both methods, indicating a reduction in the key generation's efficiency under attack. The EQKD method sustains a higher key rate overall, even as eavesdropping intensifies reflecting its superior resilience and efficiency in maintaining secure key generation despite potential security breaches.

V. CONCLUSION

The current study investigated a novel quantum cryptographic mechanism that integrates classical encryption with quantum principles, including superposition, entanglement and uncertainty. This method, defined as Enhanced Quantum Key Distribution (EQKD) emphasizes practical implementation and enhanced security measures, aiming to overcome real-world challenges and contribute to the development of quantum-secure communication systems.

EQKD consistently outperforms existing techniques in key performance areas, including Quantum Bit Error Rate (QBER), fidelity, key distribution rate, and resilience to eavesdropping. It achieves lower QBER and higher fidelity over greater distances, ensuring more reliable quantum communication. Additionally, it demonstrates greater efficiency in key generation and a higher probability of detecting eavesdropping attempts.

These results confirm the effectiveness of the proposed enhancements in strengthening the security and reliability of quantum cryptographic systems. By addressing the shortcomings of existing methods, the EQKD method offers a more robust solution for secure communication, making it well-suited to withstand current and future quantum security challenges.

REFERENCES

[1] N. Q. Luc, T. T. Nguyen, D. H. Quach, T. T. Dao, and N. T. Pham, "Building Applications and Developing Digital Signature Devices based on the Falcon Post-Quantum Digital Signature Scheme," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10401–10406, Apr. 2023, https://doi.org/10.48084/etasr.5674.

[2] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, " Quantum Cryptography and U.s. Digital Security: a Comprehensive Review: Investigating the Potential of Quantum Technologies in Creating Unbreakable Encryption and Their Future in National Security," *Computer Science & IT Research Journal*, vol. 5, no. 2, pp. 390–414, Feb. 2024, https://doi.org/10.51594/csitrj.v5i2.790.

[3] S. Ali and B. Djaouida, "Optimizing Quantum Key Distribution Protocols using Decoy State Techniques and Experimental Validation," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15133–15140, Aug. 2024, https://doi.org/10.48084/etasr.7521.

[4] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: applications and future prospects," *Frontiers in Physics*, vol. 12, Aug. 2024, https://doi.org/10.3389/fphy.2024.1456491.

[5] B. A. Alhayani, O. A. AlKawak, H. B. Mahajan, H. Ilhan, and R. M. Qasem, "Design of Quantum Communication Protocols in Quantum Cryptography," *Wireless Personal Communications*," Jul. 2023, https://doi.org/10.1007/s11277-023-10587-x.

[6] C.-H. Liao, C.-W. Yang, and T. Hwang, "Dynamic quantum secret sharing protocol based on GHZ state," *Quantum Information Processing*, vol. 13, no. 8, pp. 1907–1916, Aug. 2014, https://doi.org/10.1007/s11128-014-0779-x.

[7] J.-L. Zhang, J.-Z. Zhang, and S.-C. Xie, "A Choreographed Distributed Electronic Voting Scheme," *International Journal of Theoretical Physics*, vol. 57, no. 9, pp. 2676–2686, Sep. 2018, https://doi.org/10.1007/s10773-018-3789-0.

[8] D. W. Leung, "Quantum Vernam Cipher," *Quantum Information and Computation*, vol. 2, no. 1, pp. 14–34, Oct. 2001.

[9] J. A. Dar, "Enhancing the data security of simple columnar transposition cipher by caesar cipher and rail fence cipher technique," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 5, no. 11, pp. 2229–3345, 2014.

[10] A. Banerjee, M. Hasan, and H. Kafle, "Secure Cryptosystem Using Randomized Rail Fence Cipher for Mobile Devices," *Intelligent Computing*, Cham, 2019, pp. 737–750, https://doi.org/10.1007/978-3-030-22868-2_52.

[11] S. Godara, S. Kundu, and R. Kaler, "An improved algorithmic implementation of rail fence cipher," *International Journal of Future Generation Communication and Networking*, vol. 11, no. 2, pp. 23–32, 2018.