IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.15

Quantum Key Distribution Using Hadamard & CNOT Gates with Reduced Bit Consumption

N.J.Dev Nikeathan
The Gandhigram Rural Institute
(Deemed to be University),
Gandhigram, India
devnikeathan@gamil.com
Kalavathi Palanisamy
The Gandhigram Rural Institute
(Deemed to be University),
Gandhigram, India
pkalavathi.gri@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.12/Issue12/DCAE10094
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.12/Issue12/DCAE10094
Received:20, November 2025,Revised:29,November 2025,Accepted: 01,December 2025,Published Online:12,December 2025. https://www.ijirae.com/volumes/Vol12/iss-12/15.DCAE10094.pdf
ArticleCitation:N.J.Dev,Kalavathi(2025),Quantum Key Distribution Using Hadamard & CNOT Gates with Reduced Bit Consumption, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 12, Issue 12 of 2025 pages 777-781 **Doi:>** https://doi.org/10.26562/ijirae.2025.v1212.15
BibTeX Key: N.J.Dev@2025Quantum
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2025.v1212.15 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract : In Cryptography, the Key Distribution methods is a secure way to transmit the keys.To transmit the key,the usage of the bits is high in Classical computers, where as in Quantum Computing it take fewer qubits than classical computers. In this work, we introduce a QKD (Quantum key Distribution) method that combines the Hadamard (H) gate and the Controlled-NOT (CNOT) gate to increase randomness and attack detector. The Hadamard gate creates superposition qubits, giving random outcomes that cannot be predicted unless the measurement is made. The CNOT gate uses entanglement in qubit pairs, so if anyone attempts to intercept or disturb one qubit, it can be detected immediately. Compared to classical key exchange, which often needs many bits and strong computational power this quantum approach generates secure keys using fewer bits because superposition and entanglement naturally provide randomness and correlation. Simulations of the proposed circuit show stronger security and faster key generation, making this method suitable for future lightweight and highly secure communication systems.
Keywords: Cryptography, Quantum Key Distribution, Hadamard Gate, Controlled NOT Gate.

1. INTRODUCTION

In today's modern world, information is generated and shared at an unprecedented scale through cutting-edge digital innovations. To effectively transmit, process, and store this growing volume of data we require faster computing speeds and larger storage capacities that can be met through the power of quantum computing [1]. Quantum computing is advancing rapidly and powerful software frameworks like Qiskit are becoming essential for supporting research, enhancing education and enabling users to execute complex computational tasks on quantum machines [2]. The rise of quantum computing technologies is often depicted globally as a "Quantum Computing Race", increasing across studies, research and industry [3]. Quantum Computing is appearing as a transformative force, set to reshape modern industries and have far-reaching impacts [4]. The foundational laws of quantum mechanics provide Quantum Key Distribution (QKD) with unconditional security. A well-designed QKD protocol enables two distant users commonly referred to as Alice and Bob to exchange a truly random and secure key using quantum communication device [5]. Quantum logic gates form the backbone of Quantum Computing and information processing [6]. The participants obtain the encoded quantum state and corresponding classical information through the use of an enhanced Hadamard gate operation [7]. It is widely recognized that any quantum operation can be built using a CNOT gate paired with Single-qubit transformation methods that have been developed to realize the CNOT gate on diverse quantum systems, including atoms, ion traps, quantum dots, NV centres, superconducting circuits and NMR platform [6]. In this paper, we explore a simple and secure way to share secret keys using quantum mechanics. It uses the Hadamard gate to place qubits into superposition, creating natural randomness that attackers cannot predict. The method also utilizes the CNOT gate to generate entangled qubits, which reveal any tampering that may have occurred during transmission. By combining these two gates, the system can detect eavesdropping more effectively than classical methods. The approach requires fewer bits because quantum states themselves provide strong security features. This proposed method is an attempt to show how the circuit improves both safety and efficiency.

2. RELATED WORKS

The authors in [7] introduce a multi-dimensional secret sharing procedure, which employs generalized Hadamard and SUM gate to share quantum and classical data among multiple parties. Comparatively, this future study will be on quantum key distribution, which builds on only Hadamard and CNOT interactions to constitute lightweight Bell state correlations. Their strategy emphasizes such features as participant management and cheating detection, but our work is focused on speed, simplicity, or less use of bits when generating keys. Consequently, our approach provides a more efficient and fast solution that is specifically targeted to secure QKD and not complex group based secret sharing. A method in [8]Group focuses on how Clifford circuits work internally and presents a new canonical form that uses Hadamard-free layers, permutations, and Hadamard gates to describe any Clifford operator. It is mainly about optimizing quantum circuits, reducing gate cost, and generating random Clifford operators efficiently. While the other paper studies high-level mathematical structures and gate decompositions.

It was started that Clifford circuits can be rewritten using special layers that remove the need for repeated Hadamard gates, focusing mainly on circuit structure, optimization, and efficient Clifford generation[10]. In contrast, our proposed work is not about circuit simplification but about building a lightweight and practical QKD protocol. The article [5]dwells upon the three-dimensional QKD system where a 3D Hadamard gate and ternary states are used to enhance security and noise resistance in high-dimensional communication. It primarily discusses the ways in which ternary logic, mutually unbiased bases, and multi levels measurements can improve the QKD performance. In the article Secondary Key Integration for Secure Data Transfer in SDN [10], the authors speak about the possibility of enhancing the safety of the data transfer with the help of Software-Defined Networking, which provides an additional authentication key during communication. It focuses on the enhancement of classical network security, using controller smartness and secondary-key authentication.This is what makes our approach radically different with the goal of future quantum-secure communication instead of better existing SDN systems. A Research work on A Scalable Transversal CNOT [11] addresses the problem of making large-scale quantum computing by studying the behaviour of transversal CNOTs in the context of surface code blocks as well as how correlated errors propagate throughout deep quantum circuits, which is much more reliable and scalable for fault-tolerant systems. Unlike the above-mentioned research, this proposed work does not focus on developing techniques for reducing errors or building large-scale fault-tolerant quantum logic circuits, but instead provides an easy-to-implement, efficient technique for securely distributing keys. In [12] emphasised that enabling multi-party coordination, including secure participation in a group setting for developing a single key. X. T. Liang at [13] proposed and researchers study the thermodynamic characteristics of CNOT gates, specifically observing the transfer of heat and work during operation in both open and closed quantum systems. This research is aimed at understanding the energy exchanged while operating a CNOT gate and determining the types of Quantum Engine and Refrigerator states created, dependent upon the CNOT gate operation type. Physical Realization of the Translation Symmetry Breaking Anomaly in Quantum Circuits [14], the researchers initiated their research to investigate the relationship between symmetry breaking and the physical behaviour occurring in quantum circuits. Their inquiry consisted of both theoretical and experimental analysis validating anomalous behaviours of multiple qubit systems. The primary objective of their inquiry was to discover the impact of using circuit constructs tailored to the African American culture on translating symmetry, and how that behaviour exhibited different properties relating to Quantum States. A work on Global Perspective emphasizes existing quantum security methods as well as the progression of contemporary cryptography to solve new security problems [15]. This article also has a broader and more theoretical view on behalf of information security by outlining multiple security models available for potential use in protecting information. The author in [16] explains different controlled quantum gates such as CS, CSWAP, CNOT, CZ and multi qubit Hadamard operations, focusing on their matrices, behaviours, and how they create or transform quantum states. Its purpose is to teach gate operations and show how complex control gates work inside larger quantum circuits.

3. PROPOSED METHODOLOGY

3.1. Proposed QKD Method Using H and CNOT

The proposed work utilizes the Hadamard gate & CNOT gate to transmit the secret key.The superposition is created using Hadamard gate (both'0' and '1' at once) in a qubit, which renders the first one fundamentally uncertain. Second, the CNOT gate uses entanglement to entangle a qubit with a second one. Through this entanglement, the Bell state is created, where the two qubits are perfectly associated; whatever the first qubit is, the second must be the same. When Alice sends one qubit, and both parties measure their parts, this perfect association ensures they get identical bit sequences for their key. Critically, any attempt by an eavesdropper to measure the key during transmission instantly breaks the entanglement, immediatelyrevealing the intrusion and makes the process far more secure and efficient than classical key exchange.

The steps of Figure 1 are given below:

Step 1: The first component, the Hadamard Gate, hits qubit 0. This is like spinning a coin. Before it lands, it's both heads and tails at the same time.

Step 2: The second component, the CNOT Gate, establishes entanglement. It creates a perfect link:

- If Qubit 0 is 0, Qubit 1 must be 0.
- If Qubit 0 is 1, Qubit 1 must be 1.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.15

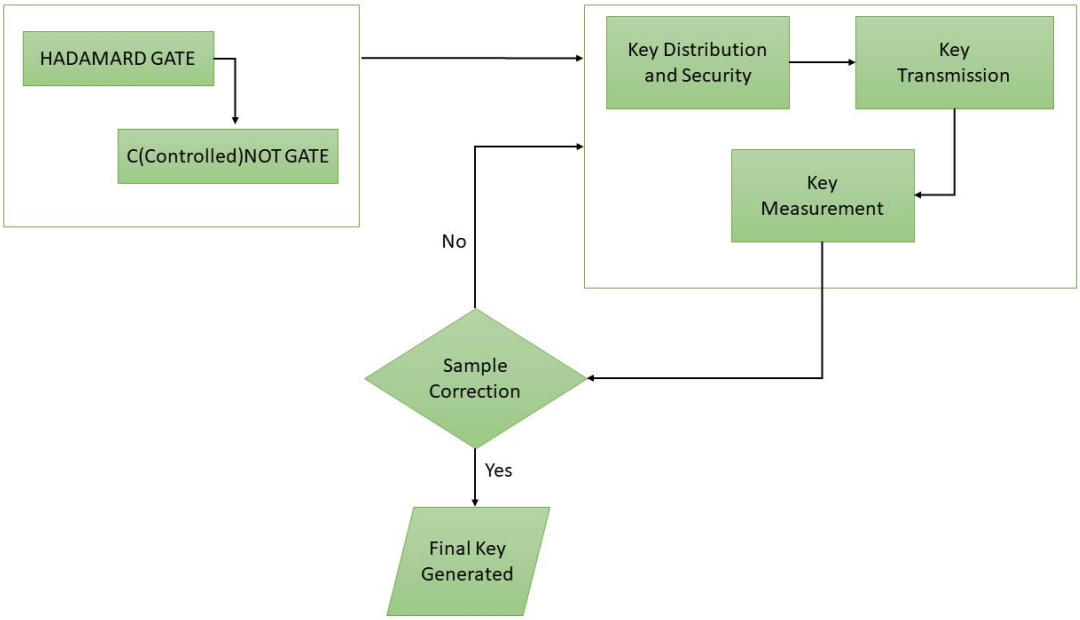

Fig 1. Workflow of the proposed methodology

Step 3: It sends the Qubits to the Key Distribution and Security.
Step 4: Then, in Key Transmission, the sender (Alice) keeps Qubit 0 and sends Qubit 1 to the Receiver (Bob) over the quantum channel. If an eavesdropper (Eve) tries to measure or copy Qubit 1 during transmission, the entanglement link is instantly broken due to quantum physics.
Step 5: Key Measurement. Both the sender and the receiver simultaneously measure their respective qubits (qc. Measure ([0,1], [0,1])), because if the CNOT gate creates a perfect link, they are guaranteed to obtain the exact same sequence of bits. This sequence is the raw key.
Step 6: Sample Correction, the sender and receiver publicly compare a small, random sample of the raw key bits just generated.

- If the key matches perfectly, then no detectable eavesdropping occurred. The protocol proceeds.
- If the key mismatches, the entanglement was disturbed. The key is discarded, and the process restarts.

Step 7: Final Key Establishment, if the sample was clean, the remaining uncompared bits become the final, secure Secret Key.

3.2. Mathematical Background

3.2.1. Hadamard Gate

The Hadamard gate converts standard basis states into equal superpositions.
Its matrix representation is:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Effect on basis states:

$$H|0\rangle = \frac{1|0\rangle+|1\rangle}{\sqrt{2}}$$
$$H|1\rangle = \frac{1|0\rangle-|1\rangle}{\sqrt{2}}$$

These states carry built-in randomness and cannot be measured by an attacker without introducing detectable errors.

3.2.2.CNOT Gate

The CNOT gate flips the target qubit when the control qubit is $|1\rangle$. Matrix from:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Using H on the first qubit and then applying CNOT produces the Bell state:

1. Create a superposition:

$$H|0\rangle = \frac{1|0\rangle + |1\rangle}{\sqrt{2}}$$

2. After CNOT:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

This entangled state allows Alice and Bob to share perfectly matching results. Any eavesdropping breaks this correlation, making tampering obvious.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 12, December 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1212.15

4. RESULTS AND DISCUSSION:

In classic computers, Alice wants totransmit a security key to Bob,which will use around 8 bits (Classical shared key: [1, 1, 0, 1, 1, 0, 0, 0]). While the same process takes 5 qubits in a Quantum Computer (Quantum shared key (BB84): [1, 1, 0, 0,1]. By comparing a quantum computer with a classical computer, the qubits are reduced to 5 bitsas shown in Figure 3.Further, the use of Hadamard gate in the circuit of a quantum computer will reduce the qubits to 2 bits,as illustrated inFigure 4. Then CNOT is used to increase the randomness and detect eavesdropping with the same 2 bits instead of increasing the bits as given in Figure 4.As shown in Figure 4, when using the Hadamard Gate, the frequency of randomness is approximately 45. If we use the CNOT Gate, the frequency of the randomness is near 50. If we apply both the Hadamard Gate and the CNOT Gate, the frequency of the randomness increases to nearly 100.

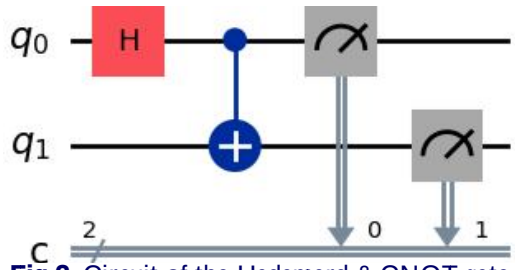

Fig 2. Circuit of the Hadamard & CNOT gate

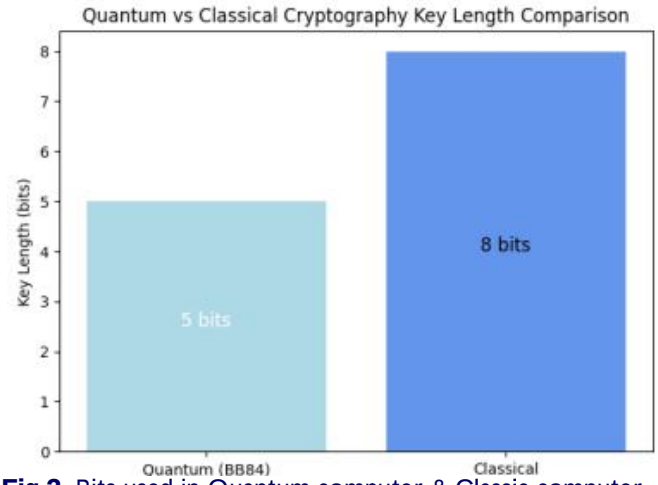

Fig 3. Bits used in Quantum computer & Classic computer.

Quantum shared key (BB84): [1, 1, 0, 0, 1]
Classical shared key: [1, 1, 0, 1, 1, 0, 0, 0]

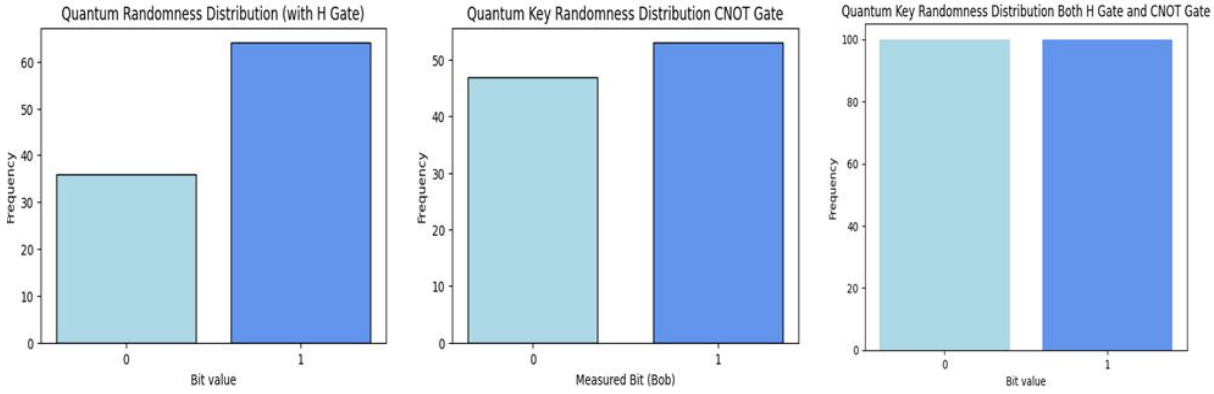

Fig 4. Qubits Randomness Detection

5. CONCLUSIONS AND FEATURE ENHANCEMENTS

This work demonstrates that a Quantum computer use fewer bits than a classical computer in combining Hadamard and CNOT gates,making the key a simple yet powerful approach to QKD. By creating both superposition and entanglement, this protocol naturally produces strong correlations between the sender (Alice) and receiver (Bob) while making eavesdropping attempts easy to detect.

Overall, the proposed design successfully reduces bit usage without reducing the level of security. In the feature thismethod can beimproved by exploring additional entanglement operations to increase key generation speed. Through

the advanced error correction methods, this protocol can be applied to noisy or real-world quantum networks. To transmit the key over long distance, we can improve the integration scheme with modern quantum repeaters. In feature work this may involves implementing this system on real-worldquantum hardware to compare practical result. These enhancements could help shape a more robust and scalable version of the protocol for a future quantum-secured communication environment.

REFERENCES

1. Y.Xie, H.Luo, and A.Ding, "Design of a High-Stability QPUF and QRNG Circuit Based on CCNOT Gate," ComputSecur, p. 104694, Dec. 2025, https://doi.org/10.1016/j.cose.2025.104694.
2. A.Javadi-Abhari et al., "Quantum computing with Qiskit," Jun. 2024, [Online]. Available: http://arxiv.org/abs/2405.08810
3. Z. Yang, M. Zolanvari, and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," IEEE Communications Surveys and Tutorials, vol. 25, no. 2, pp. 1059–1094, 2023, https://doi.org/10.1109/COMST.2023.3254481.
4. R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J. M. Leimeister, "Quantum computing," Electronic Markets, vol. 32, no. 4, pp. 2525–2536, Dec. 2022, https://doi.org/10.1007/s12525-022-00570-y.
5. G. Chen, Y. Wang, L. Jian, Y. Zhou, and S. Liu,"Ternary Quantum Key Distribution Protocol Based on Hadamard Gate," International Journal of Theoretical Physics, vol. 61, no. 2, Feb. 2022, https://doi.org/10.1007/s10773-022-05041-w.
6. J. X. Zhang, X. T. Sun, L. X. Wang, H. R. Wei, and G. Z. Song, "Heralded hyper-CNOT gates for two-photon systems assisted by quantum scattering in waveguides," Commun Theor Phys, vol. 76, no. 11, Nov. 2024, https://doi.org/10.1088/1572-9494/ad696c.
7. D. Rathi and S. Kumar, "Verifiable dynamic quantum secret sharing based on generalized Hadamard gate," Quantum Inf Process, vol. 23, no. 10, Oct. 2024, https://doi.org/10.1007/s11128-024-04535-2.
8. S. Bravyi and D. Maslov, "Hadamard-free circuits expose the structure of the clifford group," IEEE Trans Inf Theory, vol. 67, no. 7, pp. 4546–4563, Jul. 2021, https://doi.org/10.1109/TIT.2021.3081415.
9. B. Wu, M. Ray, L. Zhao, X. Sun, and P. Rebentrost, "Quantum-classical algorithms for skewed linear systems with an optimized Hadamard test," Phys Rev A (Coll Park), vol. 103, no. 4, Apr. 2021, https://doi.org/10.1103/PhysRevA.103.042422.
10. M. Bataille, "Quantum circuits of CNOT gates: optimization and entanglement," Quantum Inf Process, vol. 21, no. 7, Jul. 2022, https://doi.org/10.1007/s11128-022-03577-8.
11. X. T. Sun, J. X. Zhang, Y. Y. Gu, H. R. Wei, and G. Z. Song, "Heralded high-fidelity photonic hyper-CNOT gates with quantum scattering in one-dimensional waveguides," Quantum Inf Process, vol. 23, no. 10, Oct. 2024, https://doi.org/10.1007/s11128-024-04533-4.
12. K. Sahay, Y. Lin, S. Huang, K. R. Brown, and S. Puri, "Error Correction of Transversal cnot Gates for Scalable Surface-Code Computation," PRX Quantum, vol. 6, no. 2, Apr. 2025, https://doi.org/10.1103/PRXQuantum.6.020326.
13. S. Heußen and J. Hilder, "Efficient fault-tolerant code switching via one-way transversal CNOT gates," Quantum, vol. 9, p. 1846, Sep. 2025, https://doi.org/10.22331/q-2025-09-03-1846.
14. X. T. Liang, J. Cheng, W. Z. Zhang, and X. Leng, "Work and heat in quantum CNOT gate operations," European Physical Journal D, vol. 75, no. 10, Oct. 2021, https://doi.org/10.1140/epjd/s10053-021-00270-w.
15. B. C. Mummaneni, J. Liu, G. Lefkidis, and W. Hübner, "Laser-Controlled Implementation of Controlled-NOT, Hadamard, SWAP, and Pauli Gates as Well as Generation of Bell States in a 3d-4f Molecular Magnet," Journal of Physical Chemistry Letters, vol. 13, no. 11, pp. 2479–2485, Mar. 2022, https://doi.org/10.1021/acs.jpclett.2c00172.
16. M. R. Khan, H. Khan, I. Alam, S. T. Siddiqui, H. Fatima, and M. Ali Khan, "Analysis and Implementation of Quantum Gates (X, Z, Y, Hadamard CNOT and CCNOT) by using matrices for Quantum Computing," 2025. https://internationalpubls.com
17. https://www.researchgate.net/profile/Pradosh-K-Roy/publication/343833536_Quantum_Logic_Gates/links/5f43bf32299bf13404ec15e3/Quantum-Logic-Gates.pdf