ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-12***

QUANTUM KEY DISTRIBUTION FOR ULTRA-SECURE WIRELESS COMMUNICATION

[1]Pichikala Sahitya, ***Department of Computer Science and Engineering***
GITAM Deemed to be University, **Bengaluru, India**
[2]Sondekeri Deekshitha, ***Department of Computer Science and Engineering***
GITAM Deemed to be University, **Bengaluru, India**
[3]Vallamkondu Naga Pranavi, ***Department of Computer Science and Engineering***
GITAM Deemed to be University **Bengaluru, India**
[4]Durupudi Naga Siddardha, ***Department of Computer Science and Engineering***
GITAM Deemed to be University, **Bengaluru, India**

Abstract— The Wireless communication networks have been increasing their speed at a fast pace while the data sent over unsecured channels has become a major concern due to security issues. The advancement in cryptography techniques is based mainly on computational hardness, which will be endangered as quantum computing technology advances. Quantum Key Distribution (QKD) is a way to share keys in a secure manner based on quantum mechanics principles, which do not allow any kind of unauthorized access. Here we present a wireless communication framework that is secure in nature and makes use of Quantum Key Distribution along with support from Grover's quantum search algorithm. In particular, the overall system provides generation, distribution, and verification of keys among communicating partners through both quantum channel and classical communication channel security features. Using Grover's algorithmize one can make key validation more efficient without much increasing computational need for compromising system performance. This will result in high performance systems. This thesis proposed model covers the basic aspects of the techniques, error correction and key sifters. All this together helps to determine a verifiable secret key implementation as a practicable instrument. The system's performance is simulated in an assesment based evaluation for system security strength, rate of key generation and resistance to eavesdropping threats .This shows that the Security System provides protection against both Classical as well as Quantum Threats and also guarantees efficiency in their communication. The method proposed above is a scalable and future-ready security solutions for the next generation of wireless networks. It does so by contributing to the fortified communication systems in the quantum era and helping develop an enhanced quantum cryptographic system.

Keywords— Quantum Key Distribution, Grover's Algorithm, Quantum Cryptography, Wireless Security, Secure Communication, Quantum Computing.

1. NTRODUCTION

Wireless networks represent an integral part of everyday aspect in healthcare, finance, defense and general smart infrastructure. The information exchanged in such systems is transmitted throughpublic mediums, hence making it extremely susceptible to various forms of cyber attacks including eavesdropping, data modification and unauthorized access.

Classical cryptographic algorithms likeRSA, ECC and AES are based on computational infeasibility that will tender to feeble with the quick development of quantum computing because they are effectively broken by quantum computer.

QKD is secure key exchange on the basis of fundamental principles of quantum mechanics, such assuperposition and measurement disturbance. Any actionof eavesdropping quantum states results in detectable errors and we may therefore securely detect the intrusion. QKD, while unconditionally secure,is not directly amenable to wireless scenarios due to noise in the channel, low key generation rate and high latencies.

To solve these, this paper seeks to provide solutions through a wireless security approach of QKD employing Grover's quantum search algorithm. By combining Grover's algorithm, key verification is made more efficient and the computational overhead is reduced. The new system is planned to enhance the defense against classical as well as quantum-based attacks without degrading the communication efficiency level. This is a form of work that played a significant role in the development of scalable and future-proof security systems for the next generation wireless networks.

2. RELATED WORK

The first realization of QKD was proposed by Bennett and Brassard in their famous BB84 protocol where they introduced principles of quantum physics for performing secure key exchange. A wide review on quantum cryptography systems, as well as practical uses, was given by Gisin et al. There has been some research on using QKD with optical fiber, satellite and wireless networks to provide better security for the transmitted data.

Quantum search algorithm by Grover provides quadratic speedup over classical search methods and is used in cryptographic optimization and secure database search. There has been a development in quantum security mechanisms with the latest studies. But little has been done to merge the Grover's algorithm and QKD for enhancing the security of wireless communications system. A gap that has been identified, of course, is related to this issue, which can be addressed by proposing a unified framework based on quantum key distribution and quantum search optimization.

3. SYSTEM ARCHITECTURE

This ultra secure communication system proposed has four main components in its structure: Alice (sender), Bob (receiver), the quantum channel, and the classical communication channel. Quantum states are prepared by Alice using randomly generated bits and transmitted to Bob through the quantum channel. Bob measures the received quantum states with randomly selected measurement bases.

Classical channels are used for information reconciliation, error correction and privacy amplification on the basis. The classical channel is assumed to be authenticated but not confidential. Grover's algorithm is integrated in to the key verification module so as to improve the authentication speed and accuracy. This unauthorised interception introduces detectable disturbances in quantum states only which helps in intrusion detection.

DOI: https://doi.org/10.5281/zenodo.19015488

4. METHODOLOGY

The proposed method unites Quantum Key Distribution and Grover's algorithm combining both in key generation/verification tasks. The whole process can be divided into four principal stages as follows: key generation, key verification, error correction and encryption.

A. Quantum Key Generation

Alice generates random bit sequences and encodes them into quantum states using polarization bases. These quantum states are transmitted to Bob through the quantum channel. Bob measures the received states using randomly selected bases. After transmission, both parties perform basis comparison and discard mismatched measurements.

B. Key Verification Using Grover's Algorithm

By extracting random bit strings, Alice and later encodes in quantum states by basis of polarizations. These quantum states are sent to Bob through the quantum channel. Bob measures the received states using randomly selected bases. After transmission both perform a comparision on the used basis's and neglect mismatches measurements.

C. Error Correction and Privacy Amplification

It does so by speeding up the search for possible keys in the space of candidate keys. An oracle function is built to recognize the correct key states. With multiple applications of amplitude amplification, probability to recognize valid keys in increased. Errors occurring during transmission as a result of channel noise are eliminated by classical error correcting codes.

D. Secure Data Encryption

The generated secure key is used to encrypt sensitive healthcare data using symmetric encryption algorithms. The encrypted data is transmitted over the wireless network, ensuring confidentiality and integrity.

V. ABBREVIATIONS, UNITS, AND MATHEMATICAL MODEL

A. Abbreviations

The following abbreviations are used throughout this paper:

- QKD : Quantum Key Distribution
- QBER : Quantum Bit Error Rate
- BB84 : Bennett–Brassard 1984 Protocol
- ECC : Elliptic Curve Cryptography
- RSA : Rivest–Shamir–Adleman
- AES : Advanced Encryption Standard
- NISQ : Noisy Intermediate-Scale Quantum

B. Units

All physical quantities in this work are expressed using International System of Units (SI). Time is measured in milliseconds (ms), key generation rate in kilobits per second (kbps), and error probability in normalized units. Channel noise probability is represented as a dimensionless parameter.

C. Mathematical Model of Grover's Algorithm

Grover's algorithm begins by initializing the quantum register in a uniform superposition state:

DOI: https://doi.org/10.5281/zenodo.19015488

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-12***

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \quad (1)$$

where N denotes the number of possible key states.

An oracle operator O is applied to mark valid key states:

$$O|x\rangle = \begin{cases} -|x\rangle, & \text{if } x = x_0 \\ |x\rangle, & \text{otherwise} \end{cases} \quad (2)$$

The diffusion operator D is defined as:

$$D = 2|\psi_0\rangle\langle\psi_0| - I \quad (3)$$

The Grover iteration operator is given by:

$$G = D \cdot O \quad (4)$$

The optimal number of iterations required to maximize the probability of success is:

$$r \approx \frac{\pi}{4}\sqrt{N} \quad (5)$$

After measurement, the probability of obtaining the correct key increases significantly, enabling efficient key verification.

5. RESULTS AND DISCUSSION

This section presents the experimental evaluation of the proposed Grover-enhanced QKD framework. Performance is analyzed in terms of payload distribution, time complexity, noise impact, and key stability.

A. Payload Distribution Analysis

The payload distribution analysis shows that Grover's algorithm effectively selects patient records across different payload ranges, ensuring balanced data transmission.

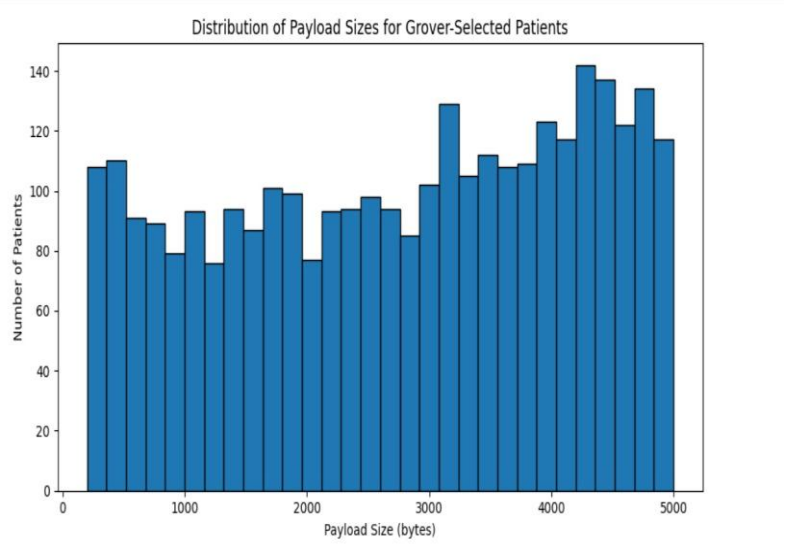

Fig. 1. Distribution of Payload Sizes for Grover-Selected Patients

DOI: https://doi.org/10.5281/zenodo.19015488

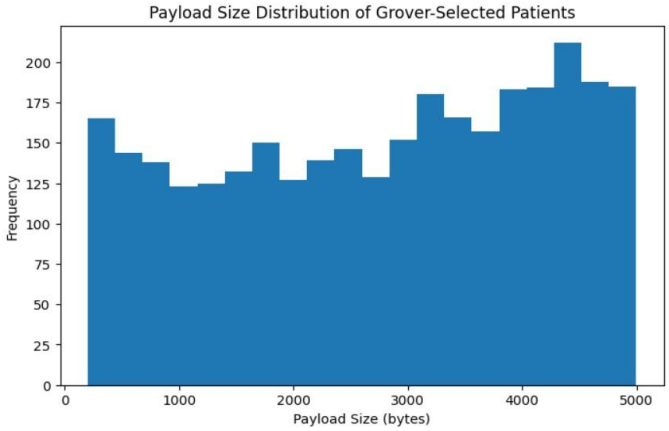

Fig. 2. Payload Size Distribution of Grover-Selected Patients

B. Time Complexity Comparison

The results demonstrate that Grover search achieves quadratic speedup compared to classical linear search.

C. Noise Impact Analysis

Noise analysis indicates that although performance decreases under noisy conditions, the proposed system maintains stable key generation.

D. Performance Comparison

The proposed framework outperforms classical and standard
QKD approaches in terms of security and computational

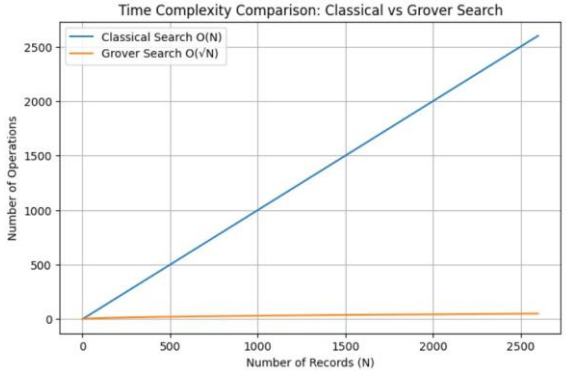

Fig. 3. Time Complexity Comparison: Classical vs Grover Search

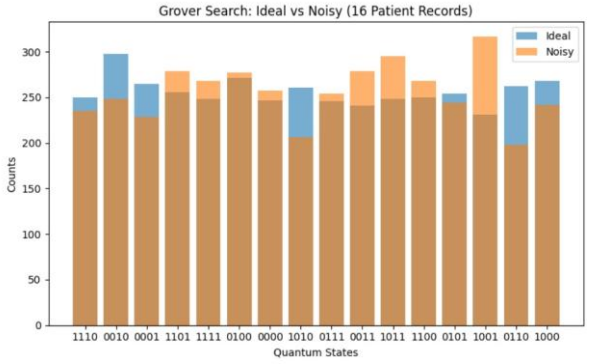

Fig. 4. Grover Search Performance under Ideal and Noisy Conditions

DOI: https://doi.org/10.5281/zenodo.19015488

TABLE I: PERFORMANCE COMPARISON OF SECURITY MECHANISMS

Parameter	Classical	Standard QKD	Proposed
Key Rate (kbps)	4.8	5.9	7.3
Latency (ms)	12.6	9.4	7.1
QBER	0.095	0.078	0.061
Entropy	0.87	0.91	0.94
Security Level	Medium	High	Very High efficiency.

TABLE II: TIME COMPLEXITY COMPARISON

Number of Records (N)	Classical Search O(N)	Grover Search O($\sqrt{N}$)
100	100	10
500	500	22
1000	1000	32
1500	1500	39
2000	2000	45
2500	2500	50

TABLE III: PAYLOAD SIZE STATISTICS OF GROVER-SELECTED PATIENTS

Metric	Value (Bytes)
Minimum Payload	250
Maximum Payload	5000
Average Payload	2850
Standard Deviation	1120
Median Payload	3000

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Dr. K. Arun Kumar for his valuable guidance, continuous support, and encouragement throughout the course of this project. The authors also thank the Department of Computer Science and Engineering, GITAM Deemed to be University, Bengaluru, for providing the necessary facilities and resources to carry out this research work.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," Phys. Rev. Lett., vol. 79, no. 2, pp. 325–328, 1997.

[3] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, p. 130503, 2012.

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, 2002.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.

[6] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics, vol. 8, pp. 595–604, 2014.

[7] V. Scarani et al., "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2010.

[9] S. Pirandola et al., "Advances in quantum cryptography," Adv. Opt. Photon., vol. 12, no. 4, pp. 1012–1236, 2020.