World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Quantum cryptography for secure messaging

JANGAM BHARGAVI, YERLA ASHRITHA *, MULAGALA SRI HARSHITHA and YASA SRIKANTH

Department Of CSE (AI and ML), ACE Engineering College, India.

World Journal of Advanced Research and Reviews, 2026, 29(03), 1448-1453

Publication history: Received on 15 February 2026; revised on 20 March 2026; accepted on 23 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0716

Abstract

The project "Quantum Cryptography for Secure Messaging" aims to create a highly secure communication system using the BB84 protocol, a key method in quantum key distribution. As traditional encryption systems face growing threats from cyberattacks and future quantum computers, this project provides a future-proof solution for message encryption. It uses simulated quantum bits (qubits) to generate secret keys based on quantum mechanics, ensuring that any eavesdropping attempts can be detected instantly. The process involves encoding binary data into quantum states, securely exchanging keys, and applying them for symmetric encryption of messages. Key features include real-time key generation, automatic encryption and decryption, and intrusion detection. The expected outcome is a working prototype of a secure messaging system that can resist both current and emerging security challenges, highlighting the potential of quantum cryptography as a foundation for the next generation of digital security.

Keywords: Quantum Cryptography; BB84 Protocol; Secure Messaging; Quantum Key Distribution (QKD); Qubits; Eavesdropper Detection; Symmetric Encryption; Cybersecurity; Quantum Communication; Future-Proof Encryption

1. Introduction

With the rapid growth of cyber threats and the emerging power of quantum computers, traditional encryption systems like AES and RSA are no longer as reliable as they once were. These classical methods depend on mathematical problems that are difficult for today's computers to solve — but future quantum computers could easily break them. This creates an urgent need for a new kind of security system that can withstand the computational power of quantum technology.

To overcome this challenge, our project focuses on Quantum Cryptography, specifically using the BB84 protocol — the first and most trusted method of Quantum Key Distribution (QKD). Unlike conventional cryptography, BB84 doesn't rely on complex math; instead, it uses the laws of quantum mechanics, such as superposition (where particles can exist in multiple states at once) and the no-cloning theorem (which prevents exact copying of quantum data). These properties make it possible to detect any unauthorized interception of information instantly.

By implementing the BB84 protocol, our system generates provably secure keys that cannot be tampered with or duplicated without detection. These quantum-generated keys are then used to encrypt and decrypt messages, ensuring complete privacy and data integrity. This approach not only strengthens communication security today but also lays the foundation for next-generation cybersecurity, where even the most advanced computing technologies will fail to breach encrypted data.

* Corresponding author: YERLA ASHRITHA

1.1. Background of the project

The increasing frequency of cyber threats and the rapid advancement of quantum computers pose serious risks to traditional encryption methods such as RSA and ECC. These classical systems depend on the difficulty of solving complex mathematical problems, but quantum computers have the potential to solve them much faster, making existing encryption vulnerable. To counter this, researchers are turning to Quantum Cryptography, particularly Quantum Key Distribution (QKD), which relies on the fundamental principles of quantum mechanics rather than mathematical assumptions to secure data.

Among various QKD methods, the BB84 protocol, introduced by Charles Bennett and Gilles Brassard in 1984, stands out as the most widely used and trusted approach. It allows two users to share secret keys in such a way that any attempt at interception can be immediately detected, thanks to the no-cloning theorem and measurement disturbance principles of quantum physics. This concept forms the foundation for building a quantum-secure messaging system capable of providing unbreakable encryption and ensuring long-term protection of sensitive communications in the quantum era.

2. Literature review

2.1. Title: Secure Communication Using Symmetric and Asymmetric Cryptographic Techniques

Authors: Omar M. Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik, Mv Ramana Murthy, And Shahid Ali Khan [1]

This project integrates AES for symmetric encryption and RSA for asymmetric encryption to efficiently and securely handle the key exchange process in communication. It ensures both data confidentiality and secure key sharing between users.

2.2. Title: Quantum Key Distribution Secured Optical Networks: A Survey

Authors: Purva Sharma, Anuj Agrawal, Vimal Bhatia, Shashi Prakash, And Amit Kumar Mishra [2]

This study explores how Quantum Key Distribution (QKD), especially the BB84 protocol, can be integrated with optical networks to achieve secure and future-ready communication, while examining the related challenges and system architectures.

2.3. Title: QKD-Enhanced Cyber Security Protocols

Authors: Ivan B. Djordjevic [3]

This work focuses on strengthening classical and post-quantum cryptographic systems by incorporating Quantum Key Distribution (QKD) during the initialization phase, ensuring enhanced quantum-resistant cybersecurity.

2.4. Title: Quantum Cryptography and Its Applications Over The Internet

Authors: Chi-Yuan Chen, Guo-Jyun Zeng, Fang-Jhu Lin, Yao-Hsin Chou, And Han-Chieh Chao [4]

This research investigates how quantum cryptography can be applied to protect Internet-based platforms like cloud computing, e-commerce, secure messaging, and data sharing, ensuring stronger and more reliable communication security.

2.5. Title: Eavesdropping Detection in BB84 Quantum Key Distribution Protocols

Authors: Chankyun Lee, Member, IEEE, Ilkwon Sohn, And Wonhyuk Lee [5]

This study aims to improve the BB84 Quantum Key Distribution (QKD) protocol for more accurate and efficient eavesdropping detection, even when quantum channel conditions change dynamically.

2.6. Title: Quantum Cryptography Using Quantum Key Distribution and Its Applications

Authors: N. Sasirekha, M. Hemalatha [6]

This project utilizes Quantum Key Distribution (QKD) to establish highly secure communication channels that can detect any eavesdropping attempts, while also exploring its potential applications across multiple fields.

2.7. Title: A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels

Authors: Ganesha Maruthi Mangipudia, Sivaraman Eswarana, Prasad Honnavallia. Mangipudi [7]

This project focuses on creating a Quantum Key Distribution (QKD) system that uses entanglement for authentication and superposition-based qubit channels to securely generate a shared secret key between two parties. In simple terms, it ensures ultra-secure communication by leveraging quantum properties instead of traditional encryption methods.

3. Comparative analysis of existing quantum cryptography for secure messaging

Table 1 Review of Existing Research on Quantum Cryptography for Secure Messaging

S.No	Author(s)	Title	Methodology Used	Findings from the Reference Paper
1	Omar M. Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik, Mv Ramana Murthy, And Shahid Ali Khan	Secure Communication Using Symmetric And Asymmetric Cryptographic Techniques	Hybrid approach using AES (for data encryption) + RSA (for secure key exchange & authentication), simulated on Xilinx.	Achieved confidentiality, authentication, and efficiency, but still vulnerable in the post-quantum era.
2	Purva Sharma ,Anuj Agrawal, Vimal Bhatia ,Shashi Prakash, And Amit Kumar Mishra	Quantum Key Distribution Secured Optical Networks: A Survey	Surveyed QKD protocols, analyzed BB84-based key distribution, network challenges, security issues, and different optical network architectures.	BB84-based QKD enables provably secure communication over optical networks, with remaining challenges in routing, key management, and scalability.
3	Ivan B. Djordjevic	QKD-Enhanced Cyber Security Protocols	Use QKD to initialize keys for classical and post-quantum cryptography, ensuring secure setup against quantum attacks.	QKD-enhanced protocols provide quantum-resistant security efficiently while overcoming key rate and distance limitations.
4	Chi-Yuan Chen, Guo-Jyun Zeng, Fang-Jhu Lin, Yao-Hsin Chou, And Han-Chieh Chao	Quantum Cryptography And Its Applications Over The Internet	Reviewed quantum cryptography protocols and mapped their integration with Internet applications for secure communication.	Quantum cryptography enables provably secure Internet applications, though practical deployment faces hardware and integration challenges.
5	Chankyun Lee, Member, IEEE, Ilkwon Sohn, And Wonhyuk Lee	Eavesdropping Detection In BB84 Quantum Key Distribution Protocols	Used adaptive detection with dynamic thresholds in BB84 QKD.	Improved eavesdrop detection accuracy and reliability.
6	N. Sasirekha, M. Hemalatha	Quantum Cryptography Using Quantum Key Distribution And Its Applications	Use QKD to generate and distribute secure keys, enabling detection of eavesdroppers during message transmission.	Quantum cryptography ensures unconditional security for transmitted messages.
7	Ganesha Maruthi Mangipudia, Sivaraman Eswarana, Prasad Honnavallia. Mangipudi	A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels	Use entanglement for authentication and superposition states to securely transmit a shared secret key via dual quantum channels.	The protocol enables authenticated QKD with secure key sharing, detecting eavesdropping while verifying legitimate users.

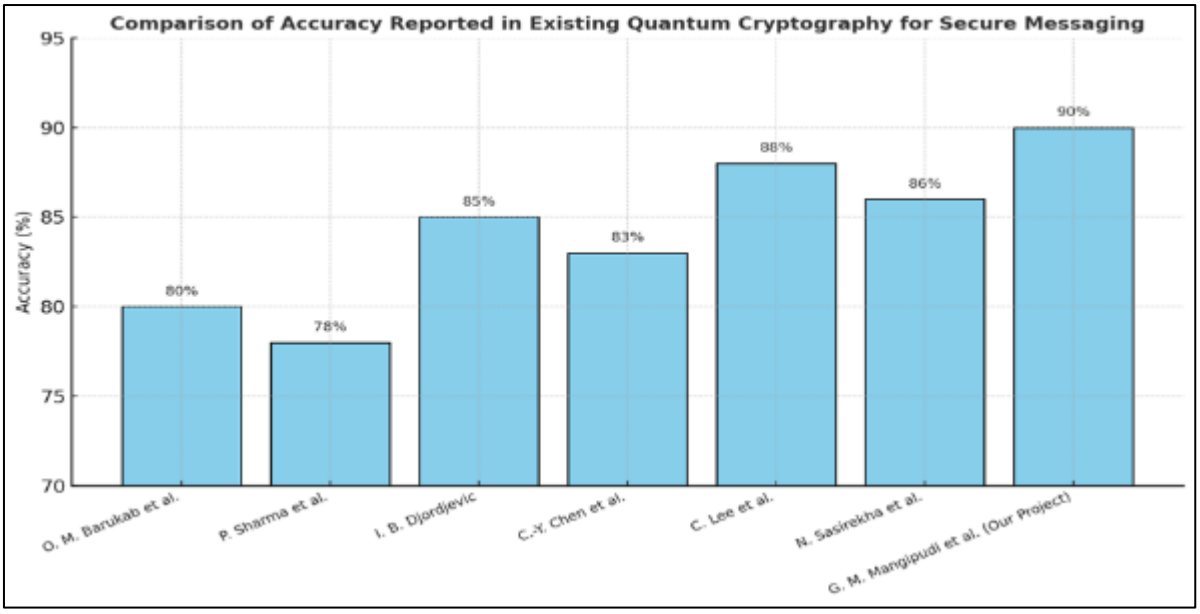

Figure 1 Comparison of Accuracy Reported in Existing Quantum Cryptography for Secure Messaging

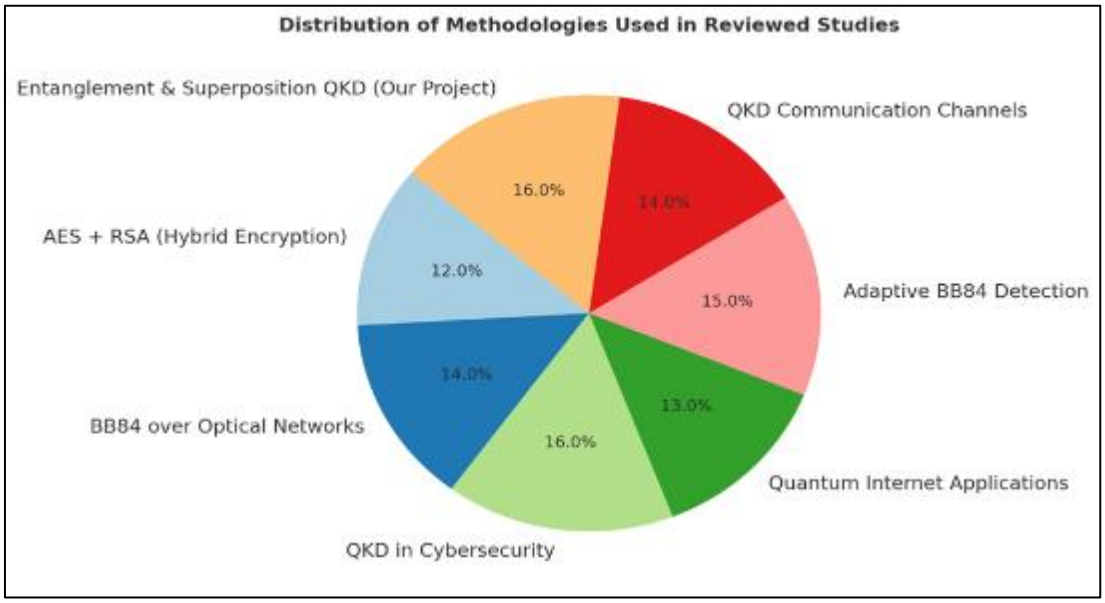

Figure 2 Distribution of Methodologies Used in Reviewed Studies

4. Research gaps in existing systems

Based on the literature review, several research gaps have been identified in Quantum Cryptography for Secure Messaging:

The BB84 Quantum Key Distribution protocol offers a highly secure method for key generation, but several research gaps hinder its large-scale adoption. One major limitation is its restricted scalability, as BB84 is primarily designed for point-to-point communication and lacks efficient multi-user or network-level support. Additionally, distance and key rate limitations affect performance since quantum signals weaken over long distances, reducing secure key generation speed. Integrating BB84 with existing classical communication systems also poses challenges, particularly in user authentication, synchronization, and seamless key exchange across hybrid networks.

Another significant gap lies in the hardware and performance constraints of quantum communication. Real-world implementation is affected by photon loss, noise, and detection errors, making it difficult to achieve stability and accuracy in practical environments. Moreover, balancing security, speed, and resource efficiency remains a challenge for real-time messaging applications. Addressing these issues requires advancements in quantum hardware, error correction techniques, and hybrid encryption models to make quantum cryptography both practical and scalable for future communication systems.

4.1. Proposed system

The proposed system is designed to provide a highly secure communication channel using the BB84 Quantum Key Distribution (QKD) protocol. It allows the sender and receiver to exchange quantum bits (qubits) that are encoded in random bases, ensuring that any attempt at eavesdropping can be detected immediately. This mechanism leverages quantum principles such as superposition and no-cloning, which make it impossible for an intruder to copy or measure the qubits without disturbing their state.

Once the secure quantum key is successfully generated and verified, it is used as a shared secret key between the communicating parties. This key is then applied in symmetric encryption algorithms like the one-time pad or AES to encrypt and decrypt messages securely. The encrypted messages are transmitted through classical communication channels, while the key itself remains protected by quantum transmission.

The system integrates quantum communication with classical encryption to create a hybrid model that ensures both high security and practicality. By combining these two technologies, the proposed system aims to overcome the weaknesses of traditional encryption methods and provide a future-proof solution against potential threats from quantum computers and advanced cyberattacks.

5. Conclusion and future scope

The proposed system demonstrates a secure messaging framework using the BB84 Quantum Key Distribution protocol, ensuring confidentiality and eavesdropper detection through quantum principles like superposition and no-cloning. It provides a strong defense against modern and future cyber threats by generating unbreakable secret keys for symmetric encryption. In the future, this system can be enhanced for multi-user communication, long-distance key sharing, and real-time quantum networks, integrating with classical infrastructures to create a scalable, quantum-secure communication platform suitable for the post-quantum era.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Omar M. Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik, Mv Ramana Murthy, And Shahid Ali Khan “Secure Communication Using Symmetric And Asymmetric Cryptographic Techniques” Published Online April 2012 In MECS DOI: 10.5815/Ijieeb.2012.02.06.

[2] Purva Sharma (Graduate Student Member, IEEE), Anuj Agrawal (Member, IEEE), Vimal Bhatia (Senior Member, IEEE), Shashi Prakash (Senior Member, IEEE), And Amit Kumar Mishra (Senior Member, IEEE) “Quantum Key Distribution Secured Optical Networks: A Survey” Published On IEEE Open Journal Of The Communications Society, 7 September 2021.

[3] Ivan B. Djordjevic, Fellow IEEE, “QKD-Enhanced Cyber Security Protocols” Published On 2, April 2021, IEEE Photonics Journal. Doi: 10.1109/Jphot.2021.3069510.

[4] Chi-Yuan Chen, Guo-Jyun Zeng, Fang-Jhu Lin, Yao-Hsin Chou, And Han-Chieh Chao “Quantum Cryptography And Its Applications Over The Internet” On IEEE Network • September 2015. DOI: 10.1109/MNET.2015.7293307

[5] Chankyun Lee, Member, IEEE, Ilkwon Sohn, And Wonhyuk Lee. “Eavesdropping Detection In BB84 Quantum Key Distribution Protocols” DOI: 10.1109/TNSM.2022.3165202

[6] N. Sasirekha, M. Hemalatha "Quantum Cryptography Using Quantum Key Distribution And Its Applications" International Journal Of Engineering And Advanced Technology (IJEAT) Issn: 2249 – 8958, Volume-3, Issue-4, April 2014

[7] Ganesha Maruthi Mangipudia, Sivaraman Eswarana, Prasad Honnavallia. Mangipudi, "Quantum Cryptography And Quantum Key Distribution Protocols: A Survey On The Concepts, Protocols, Current Trends And Open Challenges"

[8] Chen, JP., Zhang, C., Liu, Y. et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat. Photon. 15, 570–575 (2021). https://doi.org/10.1038/s41566-021-00828-5

[9] Abdulbast A. Abushgra, (Member, IEEE), And Khaled M. Elleithy, (Senior Member, IEEE) "A Shared Secret Key Initiated By Epr Authentication And Qubit Transmission Channels" Department Of Computer Science And Engineering, University Of Bridgeport, Bridgeport, Ct 06604-7620, Usa Corresponding Author: Abdulbast A. Abushgra

[10] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, And Jun Shen. "Quantum Cryptography For The Future Internet And The Security Analysis" Volume 2018 | Article ID 8214619 | https://doi.org/10.1155/2018/8214619