Enhanced Quantum Key Distribution Protocol to Improve Robustness and Error Minimization

1. Kartheek Ravipati

Student - M Tech**,** Department of Computer Science and Engineering. Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur Dt, Andhra Pradesh, India.

email id: **ravipatikartheek@gmail.com**

2. Dr. Srikanth Vemuru

Professor, Department of Computer Science and Engineering. Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur Dt, Andhra Pradesh, India

email id: **vsrikanth@kluniversity.in**

Abstract

Quantum cryptography represents a swiftly advancing discipline with the capacity to fundamentally transform the landscape of data security. A prime application in this domain is quantum key distribution (QKD), which facilitates secure communication by leveraging the principles of quantum mechanics to generate and disseminate cryptographic keys. This study is concentrated on the methodologies for safeguarding communication and data transfer against cyber-attacks through the utilization of quantum cryptography, particularly focusing on the quantum key distribution protocol known as BB84. BB84 is the first protocol for QKD in the year 1984. In this paper we simulated a new way to enhance quantum key distribution protocol BB84 by introducing multi-basis encoding, enhanced error correction, and built-in authentication. The additional basis Y provides increased robustness against intercept resend attacks, and the authentication mechanism ensures secure classical communication and hence there will be no loss of information. Finally, the experimental outcome confirms that the proposed protocol delivers efficient results comparing with the original BB84 protocol.

Keywords : Quantum Computing; Quantum Cryptography; Algorithms; Quantum Key Distribution; BB84 Protocol; Communication Security.

1 Introduction

In the contemporary era, the domain of cybersecurity has attained paramount significance due to the swift proliferation of digital platforms coupled with the escalating intricacy of cyber threats. Its importance is rooted in the safeguarding against these threats, the preservation of individual privacy, the security of enterprises, the mitigation of financial losses, and the sustenance of public safety. A noteworthy advancement in the sphere of cybersecurity is the emergence of Artificial Intelligence (AI) as a revolutionary force. The capabilities of AI encompass the analysis of extensive datasets, the adaptation to novel information, and the precise anticipation of potential threats. These attributes render it an indispensable element of cybersecurity protocols.

Amid the digital transformation, a multitude of challenges has surfaced, particularly within the realm of cybersecurity. Traditional protective measures, such as antivirus programs and firewalls, are demonstrating insufficiency when confronted with an ever evolving and increasingly intricate landscape of cyber threats. There exists an escalating demand for dynamic, robust, and effective cybersecurity solutions.

Quantum cryptography represents a revolutionary paradigm for the protection of information, employing the fundamental principles of quantum mechanics to enhance security protocols beyond traditional methodologies. Through the utilization of Quantum Key Distribution (QKD), it ensures that any attempt to intercept or alter information is detectable, thereby establishing a robust framework for data security across a multitude of contexts, including cloud computing infrastructures. The forthcoming sections elucidate the critical components of quantum cryptography and its implications for data security. It incorporates advanced methodologies such as single photon protocols and employs quantum programming languages to facilitate effective encryption and decryption, thereby maintaining data integrity.

Quantum cryptography utilizes the postulates of quantum mechanics to enhance secure communication, effectively preventing unauthorized access to sensitive information. It encompasses mechanisms intended for the detection of eavesdropping and emphasizes the importance of quantum key distribution. It involves the mathematical modeling of quantum states, operations, and measurements, thus enabling secure communication networks and applications across various sectors, including finance, governmental operations, and emerging technologies such as the Internet of Things (IoT) and fifth generation (5G) networks. This research endeavors to undertake a thorough examination of quantum key distribution, with a specific emphasis on the enhancement of the BB84 Protocol within the domain of data security.

The BB84 protocol, initially proposed by Bennett and Brassard in 1984, serves as a foundational element of quantum cryptography, enabling secure key distribution via quantum mechanics. Its significance is rooted in its capacity to provide unconditional security grounded in the principles of quantum physics, rendering it an indispensable instrument for the protection of communications, particularly within the framework of the Internet of Things (IoT) and various other applications.

The original BB84 protocol works with a high bit error rate, i.e., the number of successfully agreed bits is 1/4 of the number of bits sent. In order to reduce bit error rate of the transmission in the BB84 protocol, multi-basis encoding concept will be employed. In this paper we implement this concept and review it in detail and we support it with an example. The simulation result shows that the proposed concept is more efficient comparing with the original BB84 protocol.

2 Literature Survey

The BB84 protocol, conceived by Charles H. Bennett and Gilles Brassard in the year 1984, represents a foundational quantum key distribution (QKD) protocol. QKD protocols utilize the fundamental principles of quantum mechanics to facilitate the generation of a shared random secret key that remains exclusively known to the two communicating parties, which can subsequently be employed for the encryption and decryption of messages.

The process of key generation and distribution inherent in the BB84 protocol encompasses the encoding of random bits of information onto the polarization states of individual photons, which are then transmitted from the sender, referred to as Alice, to the recipient, identified as Bob. Bob randomly selects one of two potential measurement bases to assess the

incoming photons, followed by a public discourse between Alice and Bob concerning the utilized measurement bases, all while refraining from disclosing the specific bit values.

Subsequently, they discard the bits corresponding to instances in which different measurement bases were employed, resulting in a shared sequence of bits, termed the raw key. Alice and Bob then proceed to estimate the error rate associated with the raw key and implement classical error correction methodologies to rectify any discrepancies, culminating in a corrected key. Ultimately, they employ privacy amplification techniques to eliminate any potential information that may have been acquired by an eavesdropper, thereby yielding the final key.

Alharith A. Abdullah et al. [2] introduced a modified BB84 protocol that eliminates the need for a classical channel during key negotiation. By employing the basis of the original BB84 protocol, the proposed method allows both parties to establish a shared secret key without classical communication, thereby reducing potential information loss and enhancing security.

Wen et al. [17] introduced a modified way for BB84 protocol by preparing a two-way classical communication symmetric entanglement purification protocol. This protocol provides unconditional protection and safety with a higher error rate of 20%, where this model dispenses on public announcement of the bases in the BB84 protocol.

Benletaief et al. [5] states that when the two parties transfer information without a third party, reconciliation may occur. The reconciliation is watched as a new case of coding. Their paper described the new method for reconciliation based on codes. The concept of an explicit new method for reconciliation based on codes when a new third party or eavesdropper is in between communication is focused.

3. Related Work

In 1984 Charles Bennett and Gilles Brassard proposed the first Quantum Key Distribution protocol, known as BB84 by their surnames, and the year it was published. The BB84 protocol is a cryptographic scheme, which encodes classical bits into qubits, and it has been extensively analysed and implemented. The idea is to encode every bit of the secret key into the polarization state of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be ‘fragile’ and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarization state. This will lead to errors, and again the eavesdropper will reveal herself.

The protocol employs quantum bits (qubits) that are represented by the polarization states of photons (Quantum States). It runs as follows- Alice sends a sequence of pulses (for instance, femtosecond pulses with 80 MHz rep. rate), each of which, ideally, contains a single photon polarized differently. Alice encodes zeroes into H-polarized (Horizontally) photons while unities she encodes into V-polarized photons(vertically) (red arrows in the Fig.1.).

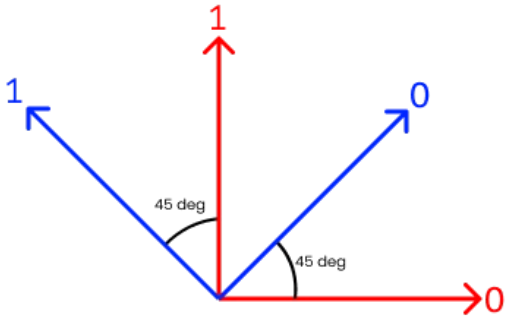

Fig.1. Representation of photon polarization for BB84 protocol

But this happens only in half of the cases. The other half of bits, chosen randomly, are encoded using a diagonal polarization basis (blue arrows in the Fig.1.). Then, the 'D' polarization corresponds to zero and the 'A' polarization, to unity. The receiver, Bob, measures the polarization using a standard setup (a PBS or a Glan prism with two single-photon detectors in the output ports, or a calcite crystal also followed by two detectors). This way Bob can distinguish between H and V polarizations if he uses the HV basis (further denoted as '+'). But in half of the cases Bob randomly changes his basis (the orientation of his prism) to AD (denoted as 'X').

After a certain number of bits have been transmitted (and all photons have been detected and destroyed!), Bob publicly announces which basis he used for each bit. Alice then says in which cases they used the same bases. They throw out the bits where they used different bases and leave only those where they used the same one. After this procedure (key sifting) the length of the key is reduced twice, but what remains is random and coincides for Alice and Bob.

They take half of the remaining bits and check for errors and eaves dropping. If the error rate is not below some fixed threshold set before the beginning of the protocol, then they abort the protocol. If the error rate is below the threshold, they perform information reconciliation and privacy amplification and further processing for authentication on the other bits to generate a key. Thus, the key generated is subsequently distilled through the processes of error correction, privacy amplification and authentication.

4 Enhanced Quantum Key Distribution Protocol

The Enhanced Quantum Key Distribution (EQKD) protocol builds upon the foundational BB84 protocol by integrating multi-basis encoding, advanced quantum error correction, and authentication mechanisms to bolster security and robustness. Unlike BB84, which relies solely on two bases, EQKD introduces an additional basis (Y) to enhance resilience against eavesdropping and quantum attacks.

Quantum states are prepared using a combination of Pauli bases (Z, X, Y), providing an increased degree of randomness. The protocol includes quantum error correction techniques, leveraging Hadamard and CNOT gates to mitigate channel noise and enhance transmission fidelity. Additionally, privacy amplification is enforced via a universal hash function to reduce the potential information gain of an adversary.

The authentication phase integrates a pre-shared key and a message authentication code (MAC) to ensure classical communication security. By combining these enhancements, EQKD not only increases key distribution security but also addresses potential vulnerabilities inherent in

traditional QKD systems, making it a more robust candidate for real-world quantum cryptographic applications.

4.1 Algorithm: Enhanced Quantum Key Distribution (EQKD)

The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal.

Algorithm 1 Enhanced BB84 Quantum Key Distribution Protocol (EBB84)

Step 1: Alice generates a random bit string $B = \{b_1, b_2, \dots, b_n\}$
Step 2: Alice chooses random bases $BA = \{\beta_1, \beta_2, \dots, \beta_n\}, \beta_i \in \{Z, X, Y\}$
Step 3: Alice encodes each b_i *into quantum state* $|\psi_i\rangle$ *using basis* β_i
Step 4: Alice sends qubit sequence $\{|\psi_i\rangle\}$ *over quantum channel*
Step 5: Bob randomly selects measurement bases $BB = \{\beta_1', \beta_2', \dots, \beta_n'\}$
Step 6: Bob measures each qubit in his chosen basis and stores results $M = \{m_1, m_2, \dots, m_n\}$

Step 7: Bob publicly announces basis choices; Alice compares and sifts key bits where $\beta_i = \beta_i'$
Step 8: Alice and Bob apply Quantum Error Correction (Hadamard and CNOT) to correct bit and phase errors
Step 9: They estimate Quantum Bit Error Rate (QBER); abort if QBER exceeds threshold
Step 10: Apply SHA-256 as universal hash function: $K_{final} = H(K_{corrected})$
Step 11: Use pre-shared authentication key K_{auth} *to compute MAC:* $MAC = H(K_{auth} \| message)$
Step 12: Verify MAC on classical channel to prevent man-in-the-middle attack
Step 13: If authentication succeeds, accept K_{final} *as shared key*
Step 14: Else, abort and restart protocol
Step 15. Securely store K_{final} *for encrypted communication*

The Enhanced BB84 (EBB84) algorithm works at improving the resilience and security of the original QKD model by integrating several enhancements within the key distribution phase. Different from the two-quantum basis used in the pure BB84 protocol, a new basis (Y) is included in the EBB84 protocol, which enhances the randomness and improves eavesdropping detection. It utilizes quantum error correction with Hadamard and CNOT gates, which enables to suppress both bit-flip errors and phase-flip errors arising in the noisy quantum channels efficiently. In addition, the protocol involves privacy amplification via a secure hash function (SHA-256) to remove any possible information leakage to a dishonest party. To defend from man-in-the middle eavesdropping attack during classical communication, the pre-shared authentic key creates a message authentication code (MAC). These improvements could lower the quantum bit error rate (QBER), achieve efficient key regeneration efficiency, and provide both quantum and classical attack resistance, which thereby make EBB84 a promising candidate for practical quantum communication systems in a post-quantum era.

4.1.1 Quantum Key Exchange Phase

Initially, the key is distributed between Alice and Bob. This is the only quantum part of quantum key distribution. The key consists of qubits that are transmitted from Alice to Bob.

1. Alice selects a random bit string B = {b_1, b_2, ..., b_n} where $b_i \in \{0,1\}$.

2. Alice randomly selects a basis string BA = {β_1, β_2, ..., β_n} where $\beta_i \in \{Z, X, Y\}$ (Pauli bases).

3. Alice encodes each bit b_i into a quantum state $|\psi_i\rangle$:

$$|\psi_i\rangle = \begin{cases} |0\rangle, & \text{if } b_i = 0, \beta_i = \mathcal{Z} \\ |1\rangle, & \text{if } b_i = 1, \beta_i = \mathcal{Z} \\ |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, & \text{if } b_i = 0, \beta_i = \mathcal{X} \\ |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{if } b_i = 1, \beta_i = \mathcal{X} \\ |R\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}, & \text{if } b_i = 0, \beta_i = \mathcal{Y} \\ |L\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}, & \text{if } b_i = 1, \beta_i = \mathcal{Y} \end{cases} \quad (1)$$

4. Alice transmits the sequence {$|\psi_i\rangle$} to Bob over a quantum channel.

5. Bob randomly selects his basis BB = {β'_1, β'_2, ..., β'_n}, where$\beta'_i \in$ {Z, X, Y}, to measure each received qubit.

6. Bob records the measurement outcomes M= {m_1, m_2, ..., m_n} where $m_i \in \{0,1\}$.

Alice and Bob decide between them which of the bits exchanged will be used for the key. This process is known as key sifting. The table below gives an example of transmitting 8 bits of a secret key. After the key sifting, only 4 bits are left.

Table 1. Example of Enhanced BB84 with 8 bits

Alice's random bit	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**
Alice's random sending basis	**Z**	**Z**	**X**	**X**	**Y**	**Y**	**Z**	**Z**
Photon polarization Alice sends	**|0⟩**	**|1⟩**	**|-⟩**	**|+⟩**	**|L⟩**	**|R⟩**	**|0⟩**	**|1⟩**
Bob's random measuring basis	**Z**	**X**	**X**	**Y**	**Z**	**Y**	**X**	**Z**
Photon polarization Bob measures	**|0⟩**	**|+⟩**	**|-⟩**	**|R⟩**	**|0⟩**	**|R⟩**	**|-⟩**	**|1⟩**
Shared secret key	**0**		**1**			**0**		**1**

4.1.2 Error Detection Using Quantum Error Correction Codes

This process is done to find out the errors introduced in the transmission and hence to find information leaked to Eve. If the information leakage to Eve is too big, the protocol is aborted and restarted again.

EBB84 uses Hadamard & CNOT gates to correct errors, reducing the number of discarded bits. EBB84 is more resilient to noise. Error correction via CNOT gate prevents bit-flip errors. Hadamard gate reduces phase errors in noisy channels.

(2)

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}|\psi\rangle$$

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

(3)

4.1.3 Privacy Amplification

This is done to further strengthen the security of the raw key bits generated. This process ensures that the key generated is completely secure and reduce the amount of information Alice has about the key.

A hash function (SHA-256) distills the final secure key, removing any potential knowledge gained by Eve. Alice and Bob apply a universal hash function H to the corrected key to reduce Eve's information:

$$K_{final} = H(K_{corrected}) \quad (4)$$

4.1.4 Authentication Phase

This is done to ensure that Alice and Bob are not victims of man-in-middle attack. Eve poses as Bob to Alice and as Alice to Bob. All information exchange is redirected from a third party without Alice and Bob knowing them. A Message Authentication Code (MAC) ensures the integrity of exchanged messages.

1. Alice and Bob use a pre-shared authentication key Kauth to verify their classical messages using a Message Authentication Code (MAC):

$$MAC = H(K_{auth}||Message) \quad (5)$$

2. If authentication fails, they abort the protocol.

3. If authentication succeeds, K_{final} is used as the secured shared key.

4.2 SIMULATION RESULTS

To validate the enhancement algorithm, it is required first to simulate the protocol BB84 and then simulate the enhancement protocol EBB84 which is proposed in this work, then compare the results of simulation for both of them. We used qiskit module (developed by IBM). This module is specially developed for use in quantum computing.

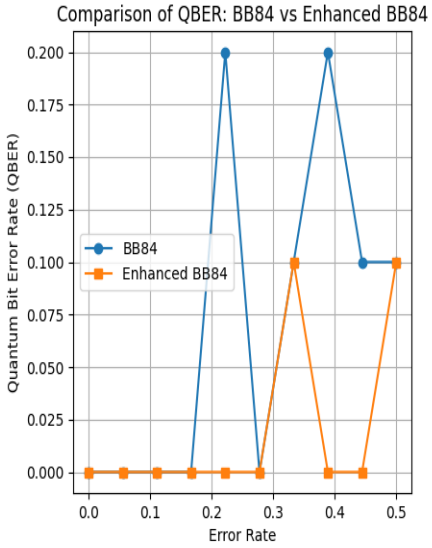

Fig.2. Comparison between the BB84 protocol and EBB84 protocol

The above figure shows the comparison of Quantum Bit Error Rate (QBER) between the BB84 protocol and EBB84 protocol where we note the relationship between the QBER and the error rate (noise in the quantum channel). It is clear that the QBER for the BB84 protocol is more compared with the EBB84 protocol and vice versa. QBER is defined as the ratio of Number of error bits (N_{error}) to the total number of bits received, i.e., QBER= N_{error}/ ($N_{correct}$ + N_{error}).

Table 2: Efficiency Metrics and Error Reduction Comparison between BB84 and Enhanced BB84

Metric	BB84	Enhanced BB84	Reduction in Error (%)	Interpretation
Initial Bits Sent	1000	1000	0	Base input bits
Bits Retained	250	480	92	Usable key bits post sifting
Efficiency (%)	25	48	92	Better bit usage efficiency
Error Bits	115	34	70.43	Bit loss due to noise
Correct Bits	135	446	230.37	Error-free bits used for key

Table 2 shows a comparison of major efficiency indicators of the conventional BB84 and the proposed Enhanced BB84. Even though both the protocols start with 1000 bits and Enhanced BB84 has relatively more (480 bits than 250 bits), the Enhanced BB84 is able to retain more than twice of BB84 with 92% retention improvement. The final efficiency increases from 25% in BB84 to 48% in the enhanced protocol, corresponding to better key generation. In this case the error bits are greatly decreased from 115 to 34, which corresponds to a 70.43% reduction in

transmission errors caused by the quantum noise. In particular, the amount of correct, usable key bits is increased by more than 230%, from 135 in BB84 to 446 in Enhanced BB84. This shows that the consideration of the above-mentioned improvements multi-basis encoding, error correction and privacy amplification have not only led to a smaller fraction of bits lost, but also to an enhanced QKD quality and security of the final key.

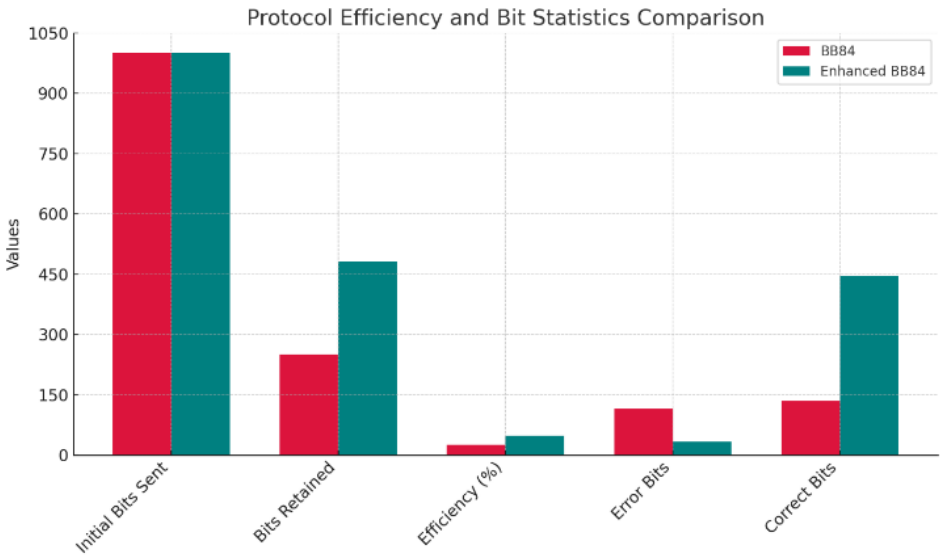

Fig.3: Protocol Efficiency and Bit Statistics Comparison

This bar graph compares two aspects of BB84 and Enhanced BB84 using 5 metrics: Initial Bits Sent, Bits Retained, Efficiency (%), Error Bits, Correct Bits. Although both protocols begin with the same number of bits (1000), the number of retained bits in the Enhanced BB84 protocol is much larger (480 vs 250) and the efficiency of this protocol also advances from 25% to 48%. In Enhanced BB84 the number of error bytes is significantly reduced, indicative to a better noise resistance and the number of correct bytes is more than 3 times increased, proving the higher reliability of the protocol. As a whole, the Enhanced BB84 resources retention and the key accuracy are substantially improved when compared with BB84, verifying the enhancement effects.

Table 3: Comparative Analysis of Security Features in BB84 and Enhanced BB84 Protocols

Security Parameter	BB84	Enhanced BB84	Impact	Enhanced Impact
Eavesdropping Detection	Basic detection	Advanced with multi-basis	Limited detection capability	Improved due to ZXY basis usage
Channel Noise Resilience	Low	High (with QEC)	Susceptible to quantum noise	Uses Hadamard & CNOT for robustness
Key Leakage Risk	High	Low (with SHA-256)	High probability of partial interception	SHA-256 ensures minimal leakage
Authentication Strength	None	Strong (MAC)	Vulnerable to man-in-middle	MAC ensures identity and message integrity
Post-Quantum Resistance	Moderate	High	Moderately future-proof	Suitable for future quantum threats

Table 3 provides a comprehensive security-level comparison between the conventional BB84 and the proposed Enhanced BB84 protocols with respect to five critical parameters. The Enhanced BB84 outperforms the BB84 because of its advanced functionalities including multi-basis encoding (for better eavesdropping detection rates) and QEC (quantum error correction) whose gates are the Hadamard and the CNOT to provide better noise resilience. SHA-256 is used to reduce key leakage, MACs are employed to guarantee secure classical communication, and man-in-the-middle attacks are thwarted. Moreover, Enhanced BB84 exhibits a more robust post-quantum security and it is therefore a secure method in subsequent applications. Together, these improvements substantially reinforce the security of the protocol, and thus the protocol's security is validated better than the BB84 standard.

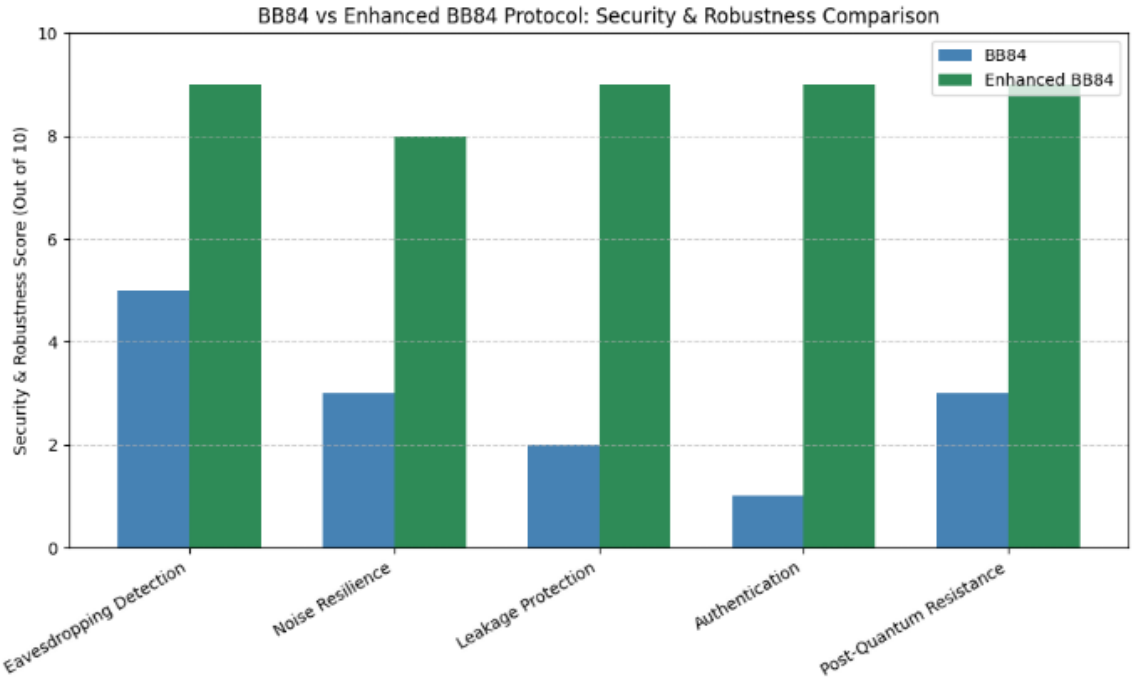

Fig.4: Protocol Robustness and Security Feature Comparison

This bar chart graphically shows the security and robustness of BB84 vs Enhanced BB84 in terms of five critical parameters. The Enhanced BB84 has always lead the pairwise comparison, obtaining its best possible scores in eavesdropping detection, noise resilience, leakage protection, authentication and post-quantum resistance. The original BB84, on the other hand, would have large limitations, especially in 'authentication' and 'key leakage protection'. This plot shows the enhanced performance of the Enhanced BB84 protocol and hence its robustness against contemporary as well as future attacks on quantum security.

5 Conclusion:

The Enhanced BB84 (EBB84) protocol is generally better than the original BB84 protocol in terms of security, resilience to errors, and efficiency. BB84 has higher QBER due to simple basis selection (Z & X) and lack of error correction. Enhanced BB84 has lower QBER because of three basis encoding (Z, X, Y) and quantum error correction (Hadamard & CNOT gates). Enhanced BB84 has lower QBER, meaning fewer errors and higher key accuracy.

BB84 has no built-in quantum error correction (QEC), so it suffers in a noisy quantum channel. Enhanced BB84 uses Hadamard & CNOT gates to correct errors, reducing the number of discarded bits making it more resilient to noise. BB84 does not include privacy amplification,

making it vulnerable to partial eavesdropping attacks. Enhanced BB84 uses a hash function (H ($Key_{corrected}$)) to eliminate leaked information. Enhanced BB84 is more secure against eavesdropping.

BB84 does not include proper authentication, making classical communication vulnerable to man-in-the-middle attacks. Enhanced BB84 uses Message Authentication Code (MAC) with a pre-shared key to verify messages. Hence Enhanced BB84 prevents tampering in classical communication. EQKD not only increases key distribution security but also addresses potential vulnerabilities inherent in traditional QKD systems, making it a more robust candidate for real-world quantum cryptographic applications.

Enhanced BB84 outperforms the original BB84 protocol in terms of security, reliability, and efficiency. By integrating Quantum Error Correction (QEC) and enhanced basis diversity, Enhanced BB84 maintains secure key distribution even in the presence of noise. Enhanced BB84 ensures a higher level of protection against potential quantum and classical attacks. The added security measures future-proof the protocol against potential attacks from quantum computers.

Enhanced BB84 achieves higher efficiency (E) by reducing the number of discarded bits during basis reconciliation. Lower QBER and improved error correction translate into a more efficient key generation process, ensuring more usable key bits with fewer transmissions.

The Enhanced BB84 quantum cryptography protocol also secures medical sensing data by enabling secure key distribution without direct sharing, utilizing quantum theory and bitwise operators to protect sensitive information from eavesdropping and unauthorized access in wireless body sensor networks. The proposed framework is designed to allocate the shared secret key required for encryption and decryption within communication channels. In the context of a Wireless Body Sensor Network (WBSN), any attempt by an adversary to compromise this secret key could lead to severe consequences, as patient medical information is highly sensitive. Unauthorized access or intrusion into such data may result in critical health risks. Therefore, establishing a secure environment is imperative, and this is achieved through the proposed system an enhanced BB84 quantum cryptography protocol, ensuring robust protection against such threats.

In summary, EQKD offers a paradigm shift in data security, combining the power of quantum mechanics with cryptographic techniques to ensure unparalleled levels of protection. Enhanced BB84 is superior to the original BB84 in terms of lower QBER, higher efficiency, improved privacy amplification, better resistance to eavesdropping and improved message authentication. Even with the advent of quantum computers, Enhanced BB84 remains secure due to its provable security properties. In practical QKD systems, where robustness and error minimization are critical, Enhanced BB84 is the clear winner over its predecessor.

References

[1] Aggarwal, R., Sharma, H., & Gupta, D. (2011). Analysis of various attacks over BB84 quantum key distribution protocol. *International Journal of Computer Applications, 20*(8), 28–31.

[2] Alharith, A., Abdullah, A., & Jassem, Y. H. (2019). Enhancement of quantum key distribution protocol BB84. *Journal of Computational and Theoretical Nanoscience, 16*, 1–17.

[3] Anasuya Devi, K., & Kalaivani, R. (2021). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-021-01546-z

[4] Bellovin, S. M. (2011). Frank Miller: Inventor of the one-time pad. *Cryptologia, 35*(3), 203–222. https://doi.org/10.1080/01611194.2011.583711

[5] Benletaief, N., Rezig, H., & Bouallegue, A. (2011). Reconciliation for practical quantum key distribution with BB84 protocol. In *2011 11th Mediterranean Microwave Symposium (MMS)* (pp. 219–222). IEEE.

[6] Bennett, C. H., & Brassard, G. (1984, December). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175–179). IEEE.

[7] Chandra, M. A. (2024). Fortifying patient privacy: A cloud-based IoT data security architecture in healthcare. *International Journal of Research in IT and Management, 14*(4), 12–40.

[8] Guitouni, Z., Maize, S., Zrigui, M., & Machhout, M. (2024). Security analysis of the BB84 protocol in IoT networks. *International Journal of Advanced Trends in Computer Science and Engineering, 13*(4), 169–174.

[9] Jain, N., Stiller, B., Khan, I., Makarov, V., Marquardt, C., & Leuchs, G. (2015). Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics, 21*(3), 168–177. https://doi.org/10.1109/JSTQE.2014.2351871

[10] Manoharan, A., & Sarker, M. (2022). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. *International Research Journal of Modern Engineering and Technology and Science, 4*(12), 2151–2164.

[11] Mitra, S., Jana, B., Bhattacharya, S., Pal, P., & Poray, J. (2017). Quantum cryptography: Overview, security issues and future challenges. In *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)* (pp. 1–7). IEEE. https://doi.org/10.1109/OPTRONIX.2017.8340103

[12] Pacher, C., Abidin, A., Lorünser, T., Peev, M., Ursin, R., Zeilinger, A., et al. (2016). Attacks on quantum key distribution protocols that employ non-ITS authentication. *Quantum Information Processing, 15*, 327–362. https://doi.org/10.1007/s11128-015-1156-3

[13] Prashant. (2005). *A study on the basics of quantum computing* [Master's thesis, Université de Montréal].

[14] Ralegankar, V. K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., et al. (2021). Quantum cryptography-as-a-service for secure UAV communication: Applications, challenges, and case study. *IEEE Access, 10*, 1475–1492. https://doi.org/10.1109/ACCESS.2021.3139602

[15] Singh, S. K., El Azzaoui, A., Salim, M. M., & Park, J. H. (2020). Quantum communication technology for future ICT—Review. *Journal of Information Processing Systems, 16*(6), 1459–1478.

[16] Van Assche, G. (2006). *Quantum cryptography and secret-key distillation*. Cambridge University Press.

[17] Wen, K., & Long, G. L. (2005). Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications. *Physical Review A, 72*(2), 022336. https://doi.org/10.1103/PhysRevA.72.022336