Advanced Secure Communication: Exploring Quantum Key Distribution, the BB84 Method

Badukuri Hemalatha, Badukuri Premalatha, Buduri. Reddaiah

***Abstract:** One promising way to use quantum information to secure everyday communication is through the distribution of quantum keys. By exchanging a secret key, the Quantum Key Distribution (QKD) approach allows two parties to communicate securely.BB84 protocol is among the most well-known QKD protocols. In this protocol, qubits are exchanged via a quantum channel between the sender and the receiver. This enables them to produce a shared key that is impenetrable to eavesdroppers and illustrate the fundamental ideas of QKD using current simulations and implementations. The results of this study demonstrate that the BB84 protocol is a highly secure QKD technique that has been investigated in great detail and used in a variety of contexts. Additionally, over the enhancements made to the BB84 protocol such as the use of advanced error correction techniques and decoy states to increase its security and usability is discussed. With an emphasis on the BB84 protocol in secure communication technologies, this study offers an extensive analysis of QKD systems overall.*

***Keywords:** Quantum Cryptography, Quantum Key Distribution, BB84, RSA, Eavesdropping.*

I. INTRODUCTION

The two key concepts of quantum physics are quantum superposition [1][14][15] and quantum entanglement [5] which are distinct from those of classical physics theory. Quantum information is a vast field that facilitates ultra quick computation [1] as well as fast and secure message transfer [4]. Traditional encryption techniques that rely on computational complexity are less safe as quantum computing advances. Since quantum communication has inherent security aspects, the fundamental idea is based on quantum physics [6] and has shown promise as a future channel for safe communication [2][13].

One of the most significant applications of quantum communication at the moment is secure communication via quantum key distribution (QKD). The quantum key distribution mechanism provides a consistent and secure key to both parties, which they then use to encrypt the communication content one-to-one and accomplish complete secure communication [3]. Systems for distributing quantum keys nowadays are built using BB84 protocol. The key information is modulated by the transmitter in the polarization state of the photon before being communicated to the receiving end via the optical cable, as demonstrated by a polarization-encoded quantum key distribution system [7][16]. A photon's polarization state may alter as a result of outside noise or outside listening devices [8][17], which could lead to a bit mistake in the key that the receiver receives.

Manuscript received on 27 March 2024 | Revised Manuscript received on 05 April 2024 | Manuscript Accepted on 15 April 2024 | Manuscript published on 30 April 2024.
***Correspondence Author(s)**

Badukuri Hemalatha, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: hemagoud2002@gmail.com, ORCID ID: 0000-0002-5851-2194

Badukuri Premalatha, Department of Computer Science, PVKN Government College, Chittoor, India. Email: prema7489@gmail.com

Buduri. Reddaiah*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: prof.reddaiah@yvu.edu.in, ORCID ID: 0000-0002-5851-2194

II. LITERATURE

Xiaodong Zhong, Ge Jin (2020) proposed work related to quantum key distribution system. In this work an error correction technique based on the Hamming code is presented and validated. With variable length coding, the technique can be adjusted to various bit error rate conditions. Author also discussed about integrating the key interleaving technique, the algorithm may rectify the random error and burst error in the original key [9].

Fangzhou Gao (2020) worked on Discrete variable quantum key distribution (DVQKD) and it is examined along with the BB84 protocol development. A performance comparison is made for ideal and real-world Poisson sources. The concept of quantum superposition and entanglement is also thoroughly described, along with the introduction to quantum information. Author also made an extensive study on the fundamentals of quantum cryptography and how quantum key distribution works in real environment. In adition to the study author also examined the setup and technical processes of the well-known BB84 technique. Matlab is used to compute the BB84 key rate and in assessing the performance [10].

Xinyi Lin, Gonghua Hou, Wei Lin, Chen Kangjie (2020) proposed a partially-trusted based routing algorithm (PT-RA). It is a method of quantum key distribution in ring networks under the constraint of the coexistence of trusted and untrusted repeaters. The security issue of key distribution in ring is backbone of networks and is effectively resolved by this technique. Based on simulation results, it is observed that PT-RA, as opposed to the original trusted relay technology, can improve key distribution success rate greatly [11].

Pankaj R Chandre et al., (2023) made an in-depth analysis of the most recent advancements in quantum cryptography. It emphasizes how machine learning techniques are being applied to augment its powers. This paper gives a general review of the concepts that underpin quantum cryptography, including quantum secure direct communication (QSDC) and quantum key distribution (QKD).

The shortcomings of conventional quantum cryptography schemes are then brought to light, and machine learning techniques are presented as a means of overcoming these obstacles and enhancing security and performance. The study also explores the dangers and weaknesses that can arise from combining machine learning and quantum cryptography. Machine learning-based quantum cryptography systems are discussed in terms of adversarial assaults, model flaws, and possible responses [12].

III. QUNATUM CRYPTOGRAPHY

Charles Bennett and Gilles Brassard's revolutionary protocols, such as BB84, helped pave the way for the study of quantum cryptography in the 1980s. Due to its ability to use quantum mechanics to provide absolute security guarantees against eavesdropping attacks, it became well-known in the late 20th and early 21st centuries. Based on the fundamental ideas of quantum mechanics, quantum key distribution (QKD), also known as quantum cryptography, is a secure communication technique. It uses elements of quantum physics to build a cryptographic protocol. Because quantum states don't clone, it allows two authorized users to communicate a secret massage or an unconditionally secure key. As a result, people may communicate safely. The traditional massages are encrypted using the secure key. QKD, which is based on the essential ideas of quantum physics, provides unconditional security in contrast to traditional encryption, which does not employ a one-time pad.

By utilizing the special qualities of quantum particles, such as photons, quantum cryptography achieves unconditional security guarantees, in contrast to classical encryption, which depends on mathematical complexity for security. Quantum Key Distribution (QKD) is a crucial procedure in quantum cryptography that enables two parties to produce a secret key while reliably identifying any eavesdropping attempts. QKD systems, such as BB84, protect the confidentiality and integrity of transmitted data by encoding information onto quantum particles and detecting any illegal interception using quantum features like the uncertainty principle.

An approach to the limitations of conventional encryption techniques like RSA and AES is provided by quantum cryptography. In contrast to AES and RSA, which depend on computational complexity to maintain security and are susceptible to quantum computer attacks, quantum cryptography uses the ideas of quantum physics to ensure security beyond a reasonable doubt. Because of the intrinsic characteristics of quantum particles, protocols such as Quantum Key Distribution (QKD) guarantee secure communication channels by identifying any efforts at eavesdropping. This characteristic, along with its resilience against quantum computer assaults, renders quantum cryptography a compelling option for safeguarding confidential data. Furthermore, quantum cryptography removes the need for intricate key exchange methods by facilitating the efficient and safe transfer of keys directly between communication parties.

A. The BB84 Method

An innovative approach to quantum key distribution (QKD) is the BB84 protocol, which provides a secure channel of communication between two participants, usually identified as sender and receiver. In BB84, sender creates a random bit sequence and uses one of two orthogonal quantum states, often represented by distinct polarizations to encode each bit onto quantum particles, such as photons. Receiver receives these particles from sender. Receiver measures each photon's condition after receiving it by choosing a measurement basis at random. Sender and receiver then make their selected measurement bases for comparison available to the public.

In order to identify possible eavesdropping attempts, sender and receiver discard measurement outcomes where their bases differ. In order to create a shared secret key, sender and receiver use the remaining bits if the error rate is low enough to indicate secure transmission. The uncertainty principle, which states that any attempt to measure a quantum state disturbs it and thus reveals the presence of an eavesdropper, is central to the security of BB84. This protocol is a promising solution for protecting sensitive data in communication networks because it offers unconditional security against adversaries with infinite computing power, addressing major shortcomings of traditional cryptographic techniques.

IV. PROPOSED BB84 METHOD

Using the principles of quantum mechanics, sender and receiver can create a secure shared key over an unsecured communication channel by implementing the BB84 protocol. Using one of two possible quantum states, sender first creates a random sequence of bits and encodes each bit onto individual quantum particles, like photons. After that, sender sends these particles to receiver. Receiver chooses a measurement basis at random for each particle after it is received and determines its state based on that basis. Following this, receiver and sender make their bases for each bit known to the public. They identify differences resulting from eavesdropping by comparing their bases choices.

Sender and receiver use photon polarizations in the BB84 protocol to safely encode and measure data bits. For every bit value of zero, sender chooses at random one of two mutually orthogonal quantum states to represent it either diagonal (45 degrees) or anti-diagonal (135 degrees) polarizations for a bit value of 1, or horizontal (0 degrees) or vertical (90 degrees) polarizations. After that, sender gets ready and sends these photons to the recipient, who chooses a measurement basis at random for each photon that is received. Receiver can use a diagonal/anti-diagonal or horizontal/vertical measurement basis. Receiver gives each measurement result a bit value based on his chosen basis and measurement outcomes. Receiver assigns the corresponding bit value to the data bit if the measurement basis matches the one sender selected; if not, he discards the measurement result. By doing this, sender and receiver detect any possible eavesdropping attempts and come up with a shared secret key. The security of the protocol is based on the uncertainty principle of quantum mechanics, which guarantees the key's confidentiality.

Sender wish to send a bit of string: 10101010. Sender and receiver both uses filter.

The rectilinear basis of quantum key distribution protocols such as BB84 is the measurement of polarization states along the horizontal and vertical axes, denoted as 0 and 90 degrees, respectively. On the other hand, the diagonal basis measures the polarization states along the 45-degree and 135-degree diagonal and anti-diagonal axes, respectively as shown in table-I. Because the measurement results for these two sets of measurement bases are independent of one another, they are mutually unbiased. This feature, which enables sender and receiver to compare their measurement bases in order to identify any possible eavesdropping efforts, is essential to the security of quantum key distribution. The security and dependability of quantum communication channels are largely dependent on the rectilinear and diagonal bases.

Table- I: Measurement of Polarization

	Basis	0	1
Rectilinear basis	+	↑	→
Diagonal basis	X	↗	↘

A. Algorithm for BB84 Method

Algorithm-1: Working of BB84 Protocol

1. Sender's Steps:
   I. Sender selects a haphazard sequence of 0s and 1s.
   II. For each bit, sender randomly selects to encrypt it using either:
      a. vertical polarization for 0 and Horizontal polarization for 1, or
      b. Diagonal polarization for 0 and anti-diagonal polarization for 1.
   III. Sender sends these polarized photons to Receiver.
2. Receiver's Steps:
   I. Receiver chooses at random how to measure every photon that enters:
      a. Receiver either measures its polarization with a horizontal/vertical filter or with a diagonal/anti-diagonal filter.
      b. For each measurement, receiver registers the result as a 0 or 1.
3. Public Announcement:
   I. Receiver shares with sender the kind of filters receiver used for each photon after receiver has measured them all, but they do not share the results.
4. Error Detection:
   I. Receiver and Sender maintain the measurement result if they both used the same kind of filters.
   II. They discard the outcome if they employed different filter types.
5. Key Extraction:
   I. Receiver and sender compare the kinds of filters they applied to each photon.
   II. They only save the measurement results for the photons that were subjected to the same kind of filter.
   III. Their shared secret key is formed by these matching results.

B. Flow Chart of BB84 Method

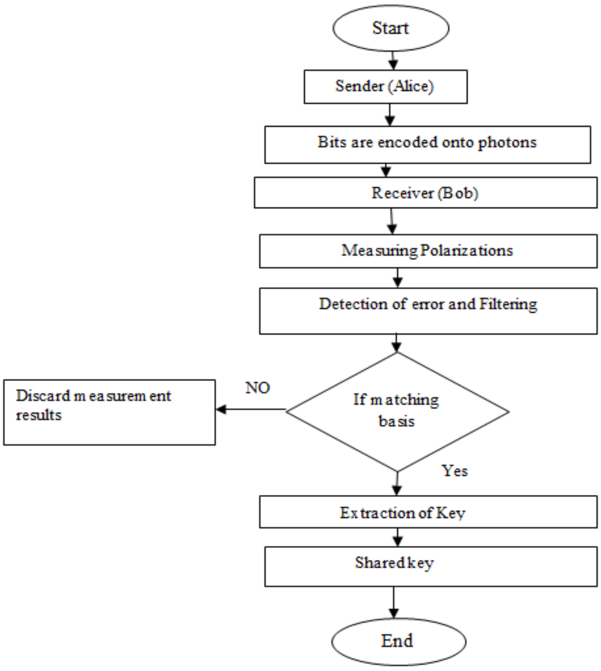

Fig. 1: Working of BB84 Method

C. Sifted Key

Sender and receiver store bits where used same basis as a Sifted Key. In the BB84 protocol, the "sifted key" is the subset of bits that sender and receiver retain after comparing their measurement bases and removing the bits corresponding to bases that don't match as shown in table-II. Their shared secret key is derived from this filtered key. It consists of the bits that receiver and sender both utilized as their measurement basis, meaning that there was no eavesdropping or interference throughout their secure transmission via the quantum channel. Sender and receiver compare the measurement bases they used for each relevant bit in order to create the filtered key. They keep the matching bits as part of the filtered key if their bases line up. They reject the matching bits if their bases don't match.

Table-II: Sifted Key

Bits sent by sender	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**
Sender's Basis	+	x	x	+	+	x	x	+
Sender's Photon Polarization	→	↗	↘	↑	→	↗	↘	↑
Receiver's Basis	x	x	x	+	x	+	+	+
Receiver's Photon Polarization	↗	↗	↘	↑	→	↗	↘	↑
Bits received by Receiver	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**
Public Discussion of Measurement Basis								
Sifted Key	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**

V. RESULTS

In the BB84 quantum key distribution protocol, sender generates a random bit sequence that serves as the shared secret key's foundation. This is where the data flow starts. The individual quantum particles, like photons, are then encoded with this random bit sequence by selecting one of two possible polarizations for each bit. Sender uses a quantum channel to send receiver these polarized photons after they have been encoded. Every photon that is received, receiver selects at random a measurement basis for that particular photon.

Depending on the polarizations sender used, this measurement basis could be either horizontal/vertical or diagonal/anti-diagonal. Next, receiver uses the selected basis to measure each photon's polarization and logs the results. Receiver and sender make their measurement bases for each corresponding photon known to the public once receiver has measured every photon. They are able to identify any errors or discrepancies introduced during transmission or as a result of eavesdropping by comparing their measurement bases.

They keep the matching measurement results as part of the shared secret key if their measurement bases match. If not, they discard the measurement results in order to look for errors. By comparing their measurement results and keeping only those where their measurement bases matched, sender and receiver eventually extract the shared secret key as shown in figure 1. The shared secret key, which enables secure communication between sender and receiver, is derived from these matching results.

Table-II: Sifted Key

Bits sent by sender	1	0	1	0	1	0	1	0
Sender's Basis	+	x	x	+	+	x	x	+
Sender's Photon Polarization	→	↗	↘	↑	→	↗	↘	↑
Receiver's Basis	x	x	x	+	x	+	+	+
Receiver's Photon Polarization	↗	↗	↘	↑	↗	→	↑	↑
Bits received by Receiver	0	0	1	0	0	1	0	0
Public Discussion of Measurement Basis								
Sifted Key		0	1	0				0

VI. CONCLUSION

Information theory and quantum physics are the foundations of QKD protocols. The establishment of secret keys is absolutely safe with quantum key distribution. The main benefit of QKD is that it allows for secure communication and the generation of a shared key that is protected against attacks. The work " Advancing Secure Communication: Exploring Quantum Key Distribution through the BB84 Protocol" emphasizes how important the BB84 protocol is for using quantum principles to strengthen communication security. The BB84 protocol ensures secrecy and integrity in data transfer by facilitating the development of a shared secret key between participants by utilizing the special capabilities of quantum physics. Furthermore, the implementation of the BB84 protocol is a significant advancement in the field of quantum key distribution, offering a possible way for secure communication. The BB84 protocol is a crucial tool for enhancing communication channels and lowering cyber security risks in a world where organizations are striving to protect sensitive data.

Future research may concentrate on enhancing the functionality and practicality of QKD protocols such as BB84, as well as developing standards and infrastructure for quantum cryptography and investigating possible integration with quantum computing technologies for further benefits.

DECLARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Nielsen, Michael A. (210). Quantum computing and quantum information, Chuang, Isaac L. (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 978-1107002173. OCLC665137861.
2. Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, V. WaniRoychowdhury," A Proof of the Security of Quantum Key Distribution," Journal of Cryptology, 2006. https://doi.org/10.1007/s00145-005-0011-3
3. ShorP W, Preskill J, "Simple proof of security of the BB84 quantum key distribution protocol," Physical Review, 2000. https://doi.org/10.1103/PhysRevLett.85.441
4. J. Watrous, "The theory of quantum information,"(Cambridge University Press, Cambridge, 2018). https://doi.org/10.1017/9781316848142
5. R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, "Quantum entanglement, " Rev. Mod, Phys. 81, 865 (2009). https://doi.org/10.1103/RevModPhys.81.865
6. W. K. Wootters, W. H. Zurek, "A single quantum cannot be cloned," Nature, Vol. 299(5886), 802-803(1982). https://doi.org/10.1038/299802a0
7. Bennett CH, "Quantum cryptography using any two non orthogonal states," Physical Review, 1992. https://doi.org/10.1103/PhysRevLett.68.3121
8. Rende Liu et al., "Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design," Optical Fiber Technology, 2019.
9. Xiaodong Zhong, Ge Jin, "Application of Hamming Code Based Erro Correction Algorithm in Quantum Key Distribution System", IEEE 3rd International Conference on Electronics Technology, University of Birmingham, 2020.
10. Fangzhou Gao, "Practical Analysis of Discrete Variable Quantum Key Distribution", IEEE 2nd International Conference on Circuits and Systems, Bournemouth University, 2020.
11. Xinyi Lin et al., "Quantum key distribution in partially-trusted QKD ring networks", 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, September 27-29, 2020.
12. Pankaj R Chandre et al., "Machine Learning-Enhanced Advancements in Quantum Cryptography: A Comprehensive Review and Future Prospects", International Journal on Recent and Innovation Trends in Computing and Communication, Vol: 11, Issue: 11s, pp: 642-655, 2023. https://doi.org/10.17762/ijritcc.v11i11s.8300

13. Securing IOT Network through Quantum Key Distribution. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 6S4, pp. 693–696). https://doi.org/10.35940/ijitee.f1141.0486s419
14. Era of Quantum Computing- An Intelligent and Evaluation based on Quantum Computers. (2019). In International Journal of Recent Technology and Engineering (Vol. 8, Issue 3S, pp. 615–619). https://doi.org/10.35940/ijrte.c1123.1083s19
15. Kaushik, A., & Narwal, R. (2020). Integration of Quantum Computing with IoT. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 4, pp. 1307–1311). https://doi.org/10.35940/ijeat.d7931.049420
16. C.T, A., O.O, O., O.A, A., & Grace, A. M. (2023). Cryptographic Security Approach for Biometric Verification System. In Indian Journal of Cryptography and Network Security (Vol. 3, Issue 2, pp. 7–13). https://doi.org/10.54105/ijcns.c7854.113223
17. Soun, B., Saini, Dr. H. K., & Brar, Dr. K. K. (2023). Study on Properties of Sisal-Cotton Union Fabrics Developed in Handloom and Power-Loom for Textile Application. In Indian Journal of Fibre and Textile Engineering (Vol. 3, Issue 1, pp. 1–4). https://doi.org/10.54105/ijfte.a2405.053123

AUTHORS PROFILE

Badukuri Hemalatha Studying M.Sc Computer Science in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. With an illustrious career in academia, Hemalatha significantly scored good grades in studies. She is working to grow as security service provider and interested in doing research in the field of Security with real world applications. She is also interested in becoming a software developer in the field of Security. She is also interested in becoming a software developer in the field of Security. Her leadership in various activities underscores her commitment to manage resources and advancing in technological innovations. Hemalatha's contributions to this study provide a comprehensive understanding of the scalability challenges in Security.

Badukuri Premalatha Completed M.Sc Computer Science in the department of Computer Science at PVKN Government (Autonomous) College, Chittoor, Andhra Pradesh. With an illustrious career in academia, Hemalatha significantly scored good grades in studies. Her expertise and dedication to fostering a deeper understanding of technology’s role in society make him a key contributor to this study. She is very much interested in becoming a Web application developer. Her leadership in various activities underscores her commitment towards work. Premalatha's contributions to this work delivered a complete thoughtful of the scalable challenges in Security related web applications.

Buduri. Reddaiah is working as Associate Professor in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. His research interests are in security and Artificial Intelligence. With a focus on network security and Artificial Intelligence, his research endeavors to enhance data integrity and access control mechanisms. Reddaiah’s dedication to exploring the intersection of technology and security plays a crucial role in the development of robust systems. His work emphasizes the importance of methodical approaches to develop models in security and maintenance As the corresponding author, he embodies the collaborative spirit of this research team.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.