International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-13 Issue-4, April 2024

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. The 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, enhancements made to the BB84 protocol, such as the use of advanced error correction techniques and decoy states, are discussed to increase its security and usability. With an emphasis on the BB84 protocol in secure communication technologies, this study provides an in-depth analysis of QKD systems as a whole.***

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

I. INTRODUCTION

The two key concepts of quantum physics are quantum superposition [1] 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].

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 are now built using the 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]. A photon's polarization state may alter as a result of outside noise or outside listening devices [8], which could lead to a bit mistake in the key that the receiver receives.

II. LITERATURE

Xiaodong Zhong and Ge Jin (2020) proposed work related to a 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 method can be adjusted to various bit error rate conditions. The author also discussed 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 examined it in conjunction with the development of the BB84 protocol. 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 an introduction to quantum information. The author also conducted an extensive study on the fundamentals of quantum cryptography and how quantum key distribution works in a real-world environment. In addition to the study, the author also examined the setup and technical processes of the well-known BB84 technique. Matlab is used to compute the BB84 key rate and to assess the performance [10].

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

Pankaj R. Chandre et al. (2023) conducted 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).

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

The shortcomings of conventional quantum cryptography schemes are then highlighted, and machine learning techniques are presented as a means of overcoming these obstacles and enhancing both security and performance. The study also examines the risks and vulnerabilities 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. QUANTUM 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 utilise quantum mechanics to provide absolute security guarantees against eavesdropping attacks, it gained widespread recognition 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 messages are encrypted using the safe key. QKD, based on the fundamental principles of quantum physics, offers unconditional security in contrast to conventional encryption, which does not utilise a one-time pad.

By utilising the special properties of quantum particles, such as photons, quantum cryptography achieves unconditional security guarantees, in contrast to classical encryption, which relies 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.

Quantum cryptography offers a solution to address the limitations of conventional encryption techniques, including RSA and AES. In contrast to AES and RSA, which rely on computational complexity to maintain security and are susceptible to quantum computer attacks, quantum cryptography utilises the principles of quantum physics to ensure security beyond a reasonable doubt. Due to the intrinsic characteristics of quantum particles, protocols such as Quantum Key Distribution (QKD) ensure secure communication channels by detecting any attempts 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 eliminates the need for intricate key exchange methods by facilitating the efficient and secure transfer of keys directly between communicating 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 parties, typically referred to as the sender and receiver. In BB84, the sender creates a random bit sequence and uses one of two orthogonal quantum states, often represented by distinct polarisations, to encode each bit onto quantum particles, such as photons. The receiver receives these particles from the sender. The receiver measures the condition of each photon after receiving it by randomly choosing a measurement basis. Sender and receiver then make their selected measurement bases for comparison available to the public.

To identify possible eavesdropping attempts, the sender and receiver discard measurement outcomes where their bases differ. To create a shared secret key, the sender and receiver use the remaining bits if the error rate is low enough to indicate a 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 the BB84 protocol. This protocol is a promising solution for protecting sensitive data in communication networks, as it offers unconditional security against adversaries with infinite computing power, thereby addressing the significant 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, the sender first creates a random sequence of bits and encodes each bit onto individual quantum particles, such as photons. After that, the sender sends these particles to the receiver. The receiver chooses a measurement basis at random for each particle after it is received and determines its state based on that basis. Following this, the receiver and sender establish their bases for each bit, making them publicly known. They identify differences resulting from eavesdropping by comparing their base choices.

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

ensures the confidentiality of the key.

The sender wishes to send the bit string 10101010. Sender and receiver both use a filter.

The rectilinear basis of quantum key distribution protocols, such as BB84, involves measuring polarisation states along the horizontal and vertical axes, denoted as 0 and 90 degrees, respectively. On the other hand, the diagonal basis measures the polarisation 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 the sender and receiver to compare their measurement bases 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. The sender selects a haphazard sequence of 0s and 1s.
   - II. For each bit, the 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. The sender sends these polarised photons to the 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, the receiver registers the result as a 0 or 1.
3. Public Announcement:
   - I. The receiver shares with the sender the type of filters used for each photon after the receiver has measured them all, but they do not share the results.
4. Error Detection:
   - I. The receiver and Sender maintain the measurement result if they both use the same kind of filters.
   - II. They discard the outcome if they employed different filter types.
5. Key Extraction:
   - I. The receiver and sender compare the types 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. These matching results form their shared secret key.

B. Flow Chart of BB84 Method

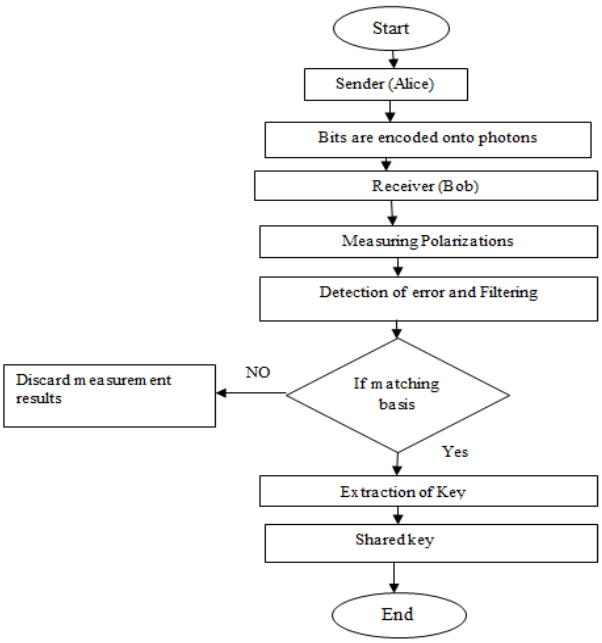

Fig. 1: Working of the BB84 Method

C. Sifted Key

Sender and receiver store bits on the same basis as a Sifted Key. In the BB84 protocol, the "sifted key" is the subset of bits that the 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 both the receiver and sender utilised as their measurement basis, meaning that there was no eavesdropping or interference throughout their secure transmission via the quantum channel. The sender and receiver compare the measurement bases they used for each relevant bit 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 the 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, the sender generates a random bit sequence that forms the basis of the shared secret key. 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. The sender uses a quantum channel to send the receiver these polarised photons after they have been encoded. Every photon that is received, the receiver selects a measurement basis for that particular photon at random.

Depending on the polarizations sender used, this measurement basis could be either horizontal/vertical or diagonal/anti-diagonal. Next, the receiver uses the selected basis to measure each photon's polarisation and logs the results. The receiver and sender make their measurement bases for each corresponding photon known to the public once the receiver has measured every photon. They can 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 to identify and correct any errors. By comparing their measurement results and retaining only those where their measurement bases matched, the 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 the 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 safe with quantum key distribution. The primary benefit of QKD is that it enables secure communication and the generation of a shared key that is protected against various attacks. The work "Advancing Secure Communication: Exploring Quantum Key Distribution through the BB84 Protocol" emphasises the importance of the BB84 protocol in utilising quantum principles to enhance communication security. The BB84 protocol ensures secrecy and integrity in data transfer by facilitating the development of a shared secret key between participants, utilising the exceptional capabilities of quantum physics. Furthermore, the implementation of the BB84 protocol represents a significant advancement in the field of quantum key distribution, offering a potential means for secure communication. The BB84 protocol is a crucial tool for enhancing communication channels and reducing cybersecurity risks in a world where organisations are striving to protect sensitive data.

Future research may focus on enhancing the functionality and practicality of QKD protocols, such as BB84, as well as developing standards and infrastructure for quantum cryptography. Additionally, it may investigate the potential integration of quantum cryptography with quantum computing technologies to further benefit from these advancements.

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 or consent to participate, as it presents evidence.
Availability of Data and Materials	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. Shor P 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 polarisation fluctuation in long-distance aerial fibre for QKD system design," Optical Fibre Technology, 2019.
9. Xiaodong Zhong, Ge Jin, "Application of Hamming Code-Based Error 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

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 academic career, Hemalatha excelled in her studies. She is working to grow as a security service provider and is interested in conducting 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 managing resources and advancing 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 academic career, Hemalatha excelled in her 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 thorough and thoughtful analysis of the scalable challenges in security-related web applications.

Buduri. Reddaiah is working as an Associate Professor in the Department of Computer Science and Technology at 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 endeavours 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 emphasises the importance of methodical approaches to developing models in security and maintenance. As the corresponding author, he embodies the collaborative spirit of this research team.