Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/30/20230065

Secure method of communication using Quantum Key Distribution

Surya Prakash Yalla[1], Archana Uriti[1], Abhisek Sethy[2], Sathishkumar V. E.[3,4]

[1]Department of Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh, India
[2]Department of Computer Science & Engineering, Silicon Institute of Technology, Bhubaneswar, odisha, India
[3]Department of Software Engineering, Jeonbuk National University, Jeonju-si, Jeollabuk-do, Republic of Korea

[4]sathish@jbnu.ac.kr

Abstract. Secure communication plays a vital role now-a-days. Modern-day secure communication is made possible via cryptography. Modern cryptographic algorithms are based on the process of factoring large integers into their primes, as they are intractable. But the cryptography nowadays is vulnerable to technological advances in computing power like quantum computing and evolution in math to quickly reverse one-way functions like factorization of large integers. Incorporating quantum physics concepts into cryptography is the answer, which results in an assessment of quantum cryptography. A unique type of cryptography known as quantum cryptography makes advantage of quantum mechanics to provide complete protection against the transmitted message. Quantum Key Distribution (QKD), a random binary key distribution used in quantum cryptography, enables communication participants to recognize unauthorized listeners. Quantum Key Distribution (QKD) is likely the most advanced quantum technology currently accessible with full stack systems already in use. This project's goal is to develop secure and encrypted communication between the parties with the help of a web application using the BB84 protocol.

Keywords: Cryptography, Quantum Computing, Quantum Key Distribution, BB84 Protocol.

1. Introduction

Quantum computing has given computers the ability to compute large amounts of data in fraction of seconds. These computations would require thousands of years for a normal computer to perform. So the basic cryptographic algorithms are getting cracked and the secret messages are getting exposed using quantum computers. These quantum computers use quantum mechanics especially superposition, interference and entanglement, in order for faster computation. So, here proposing a quantum cryptography algorithm in order to solve this issue. Since the quantum cryptography uses the same techniques as quantum computing, this makes even the quantum computers incapable to crack the encrypted message. It is a very specific key generation technique called Quantum key distribution (QKD). QKD is generally the use of quantum cryptography, entails the development of a cryptographic key with unconditional security assured by the rules of physics. Here in QKD two individuals, lets name

DOI: 10.54254/2755-2721/30/20230065

them Alice and Bob, use quantum signals known as quantum bits, or simply qubits, to generate the key. Any attempt by an eavesdropper (let's say Eve) to learn the key, results in a disturbance of the quantum signal, which causes errors and, ultimately, Eve's detection. Consideration of these physics-related repercussions then aids in creating a quantum key safely. The quantum key can be used to encrypt transmitted data once it has been generated securely.

2. Related work

This essay is further broken into several pieces. The Literature Review section describes relevant studies on many of the algorithms used in our study and the methodology of the algorithms used for encryption of data. Then, after discussing the advantages and disadvantages, a comparison table is used to draw conclusions. They proposed a solution employing symmetric and asymmetric encryption techniques for safe and secure data or information transmission for satellite communication. The secure communication method uses the following algorithms IDEA, RSA, and MD5. [1]. They explained the key generation process as well as the procedures and protocols used in the QKD secure optical network. Then, a general definition of QKD is given, covering qubits, fundamental QKD systems, QKD schemes, and protocol suites. Detailed descriptions of the QKD procedures based on the Bennett and Brassard-84 (BB84) protocols are also presented. The most common QKD protocol in this is The BB84 protocol is used to provide a detailed description of the point-to-point QKD process via fiber. [2]. Security is guaranteed by QKD, Unfortunately, the Private key rate is too low, limited transmission distance. To overcome these key challenges, they advised using QKD just during the initialization phase to build up the necessary cyber security protocols. Both PQC protocols and computational security are covered by the suggested concept. The QKD-enhanced cyber security protocol that is being suggested is resistant to attacks started by quantum computers. The suggested idea is universally applicable. Computational Security Protocol explains how RSA, SRK, and public key distribution protocols can be altered to fend off assaults based on quantum computing. [3]. They aim to use quantum cryptography to exchange secrets, secure computing, and secure direct communication. The system aims to implement existing solutions and possible applications of quantum cryptography over the Internet. This system contains modules such as Quantum Secret Sharing and Quantum security Direct Communication [4].

Name	Type of cryptosystem	Quantum attack
AES-128	Symmetric encryption	Grover's Algorithm (Decreased security)
AES-256	Symmetric encryption	Grover's Algorithm (Decreased security)
Salsa20	Symmetric encryption	Grover's Algorithm (Decreased security)
RSA	Asymmetric encryption	Shor's Algorithm (Broken)
RSA	Digital Signature	Shor's Algorithm (Broken)
ECDSA	Digital Signature	Shor's Algorithm (Broken)
SHA-256	Hash function	Grover's Algorithm (Decreased security)
GMAC	MAC	None

Table 1. Examples of cryptosystems and quantum attacks on them.

The above Table 1 shows the cryptographic systems and their names and also shows the quantum attacks which can crack those systems and compromise confidentiality.

Due to the nature of quantum physics, it can detect quantum eavesdropping statistically. The false positive rate (FPR) and false negative rate (FNR) upper bounds are examined in this study. Detecting eavesdropping devices using the QKD protocol Bennett-Brassard-84 (BB84). Detect MIM when the measured QBER or qubit error rate is greater than or equal to the threshold. Eavesdropper detection accuracy and BB84 quantum protocol resource cost-effectiveness trade-offs are revealed. The central limit theorem states that 300 quantum bits (qubits) can measure QBER. This is sufficient to detect a mini-mum guarantee of 0.009% for FPR and FNR for monitoring. [5]. Quantum encryption Using the Quantum Key Distribution, a random binary key distribution (QKD) makes communicating possible. They additionally examine a few quantum cryptography application areas and their restrictions. [6]. Shortly, Quantum Computing is expected to displace its classical equivalent. Although one can presume

DOI: 10.54254/2755-2721/30/20230065

that conventional crypto-systems are secure because quantum computing is still in its in-fancy, it is nevertheless best to prepare for the potential threat. Quantum Key Distribution is a technique for securely exchanging encryption keys between communicating parties that makes use of quantum mechanics and quantum cryptography [11]. Many other protocols have been developed to carry out this key exchange that takes advantage of various quantum mechanical principles. They analyzed several such protocols and provides a broad introduction to quantum cryptography [7]. This study focuses on the use fundamental ideas of quantum mechanics ensure the perfect security of QKD. At the expense of disallowing the state of quantum boost. For this rea-son, despite the phenomenal growth of his QKD network in urban areas around the world over the past decades, long-haul fiber would not be possible without his QKD network of reliable relays. This study helps to provide a two-field secure QKD through a send-or-not-send protocol [8]. The BB84 protocol is one of the recently introduced attractive QKD protocols for creating securely shared keys. One issue that has generated much debate is authentication between interacting parties. Also, his known QKD method currently in use is not ready to detect even if the principles of physics al-ready provide security for the QKD proto-col. In this work, they present a novel QKD algorithm that uses two quantum channels to grant authorized parties access to authenticated communications. Additionally, the in-tended protocol is QKD [9]. This research focuses on analyzing the properties of quantum cryptography and studying its utility for the future Internet. Note that I am researching quantum key distribution (QKD) protocols in noise-free channels. Additionally, search for his QKD protocol on Noisy Channel to simulate real-world scenarios in the future Internet. This result demonstrates the theoretically unbreakable security of quantum cryptography. This is a good fit for the Internet, which is bound to face ever-increasing challenges in the years to come [10].

3. Proposed Methodology

- Secure communication is when two parties are communicating, they should avoid allowing a third party to overhear their conversation.
- Any leak of information will lead to the loss of confidentiality which is critical. The proposed system uses quantum cryptography for the transmission of messages.
- To be precise quantum key distribution is used for the generation of the secret key.
- The protocol used is BB84 which is not only reliable but also secure and fast.
- Later, two channels for the communication between the sender and the receiver namely Alice and bob.
- One channel is a normal classical channel while the other one is an advanced quantum channel.
- Quantum key distribution (QKD), which is the production of a secret key with uncompromising security guaranteed by the laws of physics, is one use of quantum cryptography.
- The key is created by two people, Alice and Bob, using quantum signals known as quantum bits, or simply qubits.
- Any attempt by an eavesdropper (let's say Eve) to learn the key results in a disturbance of the quantum signal, which causes errors and, ultimately, Eve's detection.

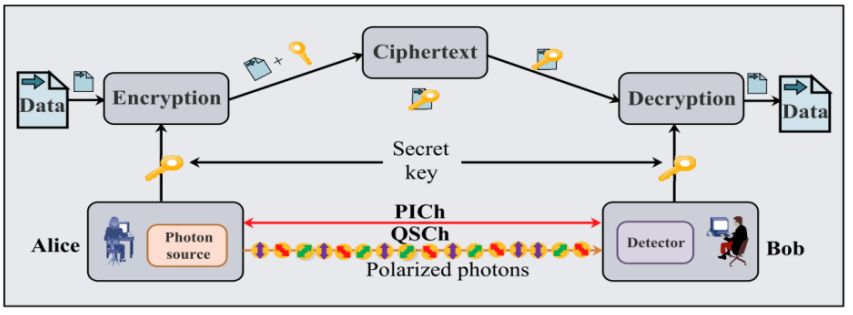

Figure 1. Architecture of Procedure.

DOI: 10.54254/2755-2721/30/20230065

The above Figure 1 gives an outline of the architecture of the QKD process and the system outline.

There are 3 steps to it:

a) A secret key is generated using BB84 protocol at both the ends.

b) Using the secret key the information which is in the form of plain text is converted to cipher text and gets transmitted to the receiver.

c) The receiver uses the same key and retrieves the plain text from the cipher text.

A classical information channel is a communication channel that can be used to communicate classical information. A light traveling across fiber-optic cables or energy moving through phone lines are two examples.

Conventional channels can be effective when used in conjunction with quantum channels. In protocols for exchanging quantum keys, a classical channel [12] is utilized in addition to a quantum channel. When a noisy quantum channel is combined with a noise-free classical channel the information rate of the noisy quantum channel can be increased in quantum communication. A quantum channel is a type of communication that can send both quantum and conventional information. The state of a qubit is an illustration of quantum information. A text file sent over the Internet is an illustration of traditional information. In more technical terms, operator spaces are mapped between fully positive (CP) traces-preserving mappings [13], or quantum channels. In other words, a quantum channel is simply a quantum operation that is seen as a pipeline designed to transport quantum information [14] rather than just the system's reduced dynamics.

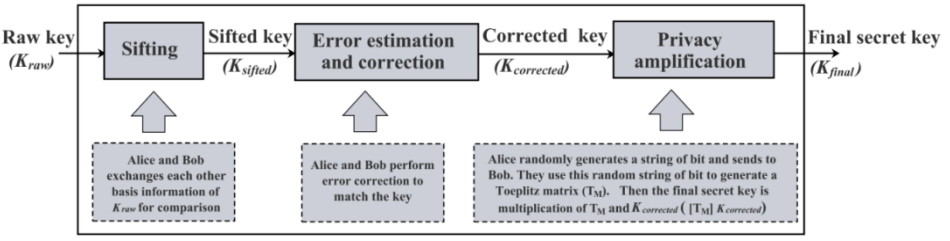

Figure 2. Flow chart of key generation in QKD.

The above **Figure 2** shows the key generation process between alice and bob using the quantum and the classical channels. The random qubits are transmitted using the quantum channel and filters are used to get the right bit. The sequences of filters are shared via classical channel and the bits which match at both senders and receivers end form the sifted key. Error correction is done using some check bits and hence the secret key is generated at both the sender and receiver end, rather than sharing the secret key.

DOI: 10.54254/2755-2721/30/20230065

4. Results and Analysis

With the help of QKD and python users able to make a secure chat application which can be used to send and receive secret messages that is shown in Figure 3, Figure 4 and Figure 5. This application has many use cases such as in transmitting secret nuclear codes in military and many more things.

Figure 3. Front end sender view.

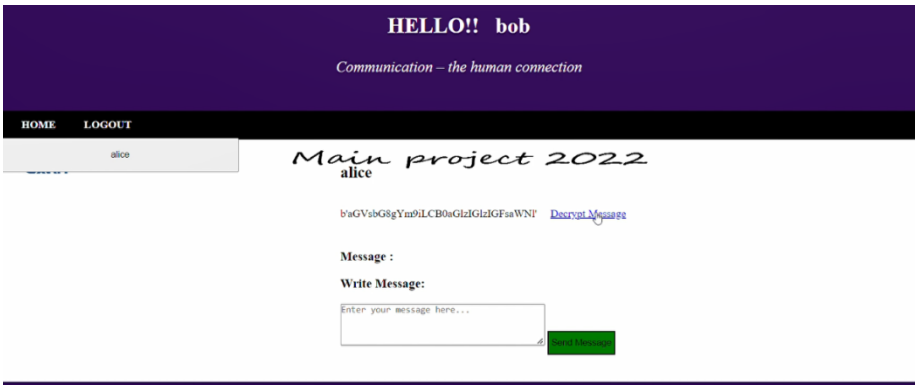

Figure 4. Front end receiver view.

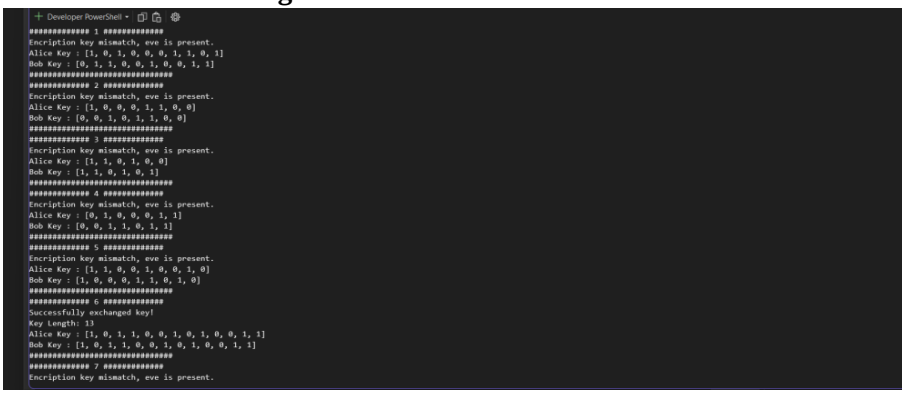

Figure 5. Backend key generation process.

5. Conclusion

With the increase in computing power, cyber security is getting complicated. This paper provides a comprehensive survey on communication using QKD and proposes a new system. The algorithm used is BB84. A powerful and encouraging step towards the future, where users can feel safer about their communication exchanges. As a result, people can anticipate that QKD will have a significant impact on fundamental physics, which will change how we see the origins of quantum mechanics. Our system comes up with a good solution for secure communication between two parties for the time being. But in

DOI: 10.54254/2755-2721/30/20230065

near future some-one may be able to crack this system with advanced tools and security will get compromised. So, this study analyses for continuous update over the security protocols and methods.

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 (Aabushgr@My.Bridgeport.Edu).

[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

[11] Yalla, S.P., Uriti, A., Sethy, A. (2022). GUI implementation of modified and secure image steganography using least significant bit substitution. International Journal of Safety and Security Engineering, Vol. 12, No. 5, pp. 639-643. https://doi.org/10.18280/ijsse.120513

[12] Chintada, K. R., Yalla, S. P., & Uriti, A. (2021, November). A Deep Belief Network Based Land Cover Classification. In 2021 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-5). IEEE.

[13] Uriti, A., Yalla, S. P., & Chintada, K. R. (2021, November). An Approach of Understanding Customer Behavior with an Emphasis on Rides. In 2021 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-5). IEEE.

[14] Y. S. Prakash, P. H. Narayan, R. Ramakrishna, G. S. Sandeep, V. S. S. Ramesh and I. Balaraju, "Digital Signatures and El Gamal Scheme Integration for Secure Data Transmission in Digital Transaction Survey," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2022, pp. 892-898, doi: 10.1109/ICAISS55157.2022.10010728.