Proceedings of the 2023 International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/8/20230083

A secure method of communication in conventional cryptography using quantum key distribution

Chunduru Anilkumar[1,2], Bhavani Gorle[1], Kinthali Sowmya[1]

[1]Dept of Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh-532127

[2]anilkumar.ch@gmrit.edu.in

Abstract. Security knowledge is one of the foremost challenges in the present day. When the topic is about Information security, the concept of cryptography comes into the picture. Every day, people and organizations use cryptography to maintain the confidentiality of their communications and data as well as to preserve their privacy. Today, one of the most successful methods used by businesses to protect their storage systems, whether at rest or in transit, is cryptography. Yet, cryptography is an effective technique to secure the data, the modern technology can break the cryptographic techniques. But some data encryption algorithms are several times stronger than today's conventional cryptography and can be constructed using quantum computing. They are "Quantum Cryptographic Algorithms ". Quantum cryptography uses the rules of quantum physics instead of classical encryption, which is based on mathematics, to protect and transmit data in a way that cannot be intercepted. Quantum key distribution is the greatest illustration of quantum cryptography and offers a safe solution to the key exchange issue. The proposed work deals with quantum cryptography and mainly focuses on how the quantum cryptographic algorithm is more secure than traditional cryptography.

Keywords: Security, cryptography, quantum cryptography, rivert shamir adleman algorithm, shor's agorithm, quantum key distribution, BB84 protocol.

1. Introduction

The one-way nature of factoring makes RSA encryption robust. Finding the prime factors of a huge integer is far more complex than multiplying two primes together. Technology is dependent on that. And RSA encryption became quite well-known due to its ease of use. The RSA technique can be broken using the quantum cryptography algorithm known as Shor's algorithm. Rather than brute-forcing the whole key by attempting factors until one is discovered, Shor's technique uses a quantum computer to determine the phase of a function holding the RSA key and then computes the greatest common divisor conventionally.

We suggested quantum cryptography, which uses natural aspects of quantum physics, to protect and transmit data in an uninterruptible manner. By employing cryptography to encrypt and secure data, only those with the right secret key may decrypt it. Quantum cryptography, in contrast to traditional cryptographic systems, bases its security notion more on physics than mathematics. A system protected by quantum cryptography cannot be cracked without the transmitter or receiver of the message being aware of it. As a result, replicating or reading information encoded in such a quantum

DOI: 10.54254/2755-2721/8/20230083

state without informing the sender or receiver is challenging. Quantum encryption should not be hacked by quantum computer users. In quantum cryptography, data is sent across fiber optic wire using individual light particles, or photons. Binary bits are represented by photons. Quantum physics is a key component of the system's security.

The following are some of the security properties:

The existence of particles in many locations or states simultaneously.

A quantum attribute cannot be examined without causing it to change or be disturbed.

It is not possible to copy whole particles.

Any system's quantum state cannot be measured due to these characteristics without causing it to change.

Since they possess all the requirements for quantum cryptography, photons are utilized in this technology. They function as information carriers in optical fiber lines and the behavior is well characterized. One of the most well-known applications of quantum cryptography is quantum key distribution (QKD), that provides a safe method for key exchange. We use the BB84(Bennett and Brassard) protocol to implement the Quantum Key Distribution using the python packages like QuTip, to provide a secure method of communication by exchanging the secret key in a secured channel to the two intended communicating peers only and to detect eavesdropping between the communicating peers the BB84 protocol has been used.

2. Related work

To strengthen the security of data transmission, this paper explores the usage of exclusive quantum key distribution (BB84 protocol) as the way it can be used with traditional encryption techniques. Additionally, it evaluates the performance of several cryptographic methods for a range of file sizes, comparing the avalanche impact, encryption, decryption, and throughput of both QKD- and QKD-free versions of these functions. This paper builds on existing research into quantum cryptography by exploring its potential applications in secure communication systems [1].

To emulate the principles of quantum physics, this work proposes a proof-of-concept that uses a communication architectural model and implementation. In both the absence and the presence of an eavesdropper, it employs the BB84 quantum key distribution (QKD) protocol. The simulation findings show that an eavesdropper can be found because of Heisenberg's uncertainty principle and the no-cloning principle, but the likelihood of them correctly predicting which qubit or polarisation state is relatively slim [2].

This study examines the present body of knowledge on quantum computing and possible uses for it in cryptography. It examines current encryption methods, their resistance to quantum computers, and how a quantum computer may be employed to forecast secret keys for message decryption. The paper also addresses the creation of a web application that facilitates users' usage of this method to decode encrypted messages [3].

This presentation will explore the literature on quantum computing algorithms, including Shor's algorithm, and how they may be utilized to crack encryption systems than traditional methods. It will also examine the areas of storage capacity, computation time precision, accuracy, integrity, availability, and efficiency to assess the effectiveness of various quantum computing methods [4].

Specifically, during the COVID-19 pandemic, this study evaluates the research on the use of wireless body sensor networks (WBSN) for remote health monitoring. A unique improved BB84 Quantum Cryptography Protocol (EBB84QCP) is suggested as a successful method for secure key distribution without the direct sharing of secret keys after examining the most recent security risks to WBSN data [7].

This article reviews the existing research on post-quantum cryptography and quantum key distribution (QKD) techniques. To enhance current cryptographic protocols like Rivest-Shamir-Adleman (RSA) and make them more resilient to attacks from quantum computers, this study uses QKD. The article also describes how initializing using a QKD protocol may help fight against brute

DOI: 10.54254/2755-2721/8/20230083

force attacks by preventing Eve from discovering N and cracking the protocol via a brute force approach [8].

QKD uses the PRF (Hash, Nonce) MAC paradigm for authentication. This MAC is appropriate for QKD due to the number of features it provides. . The Wegman-Carter paradigm, the most used MAC approach in QKD, is not more key-efficient than PRF (Hash, Nonce), however. It provides everlasting security, which means that even with unrestricted computational capacity; the attacker cannot discover any new information about the produced keys as long as authentication is not stopped during QKD execution [9].

The Bennett-Brassard-84 (BB84) quantum key distribution (QKD) protocol's upper bounds on false-positive and false-negative ratios for eavesdropping detection are examined in this study. To deal with constantly changing quantum channel circumstances, it also proposes a grouped BB84 protocol and combinatorial eavesdropping detection technique. To assess their suggested methods, the authors carried out a thorough simulation analysis. The results indicated that they can guarantee at least 99.92% accuracy in detecting eavesdroppers in such circumstances [10].

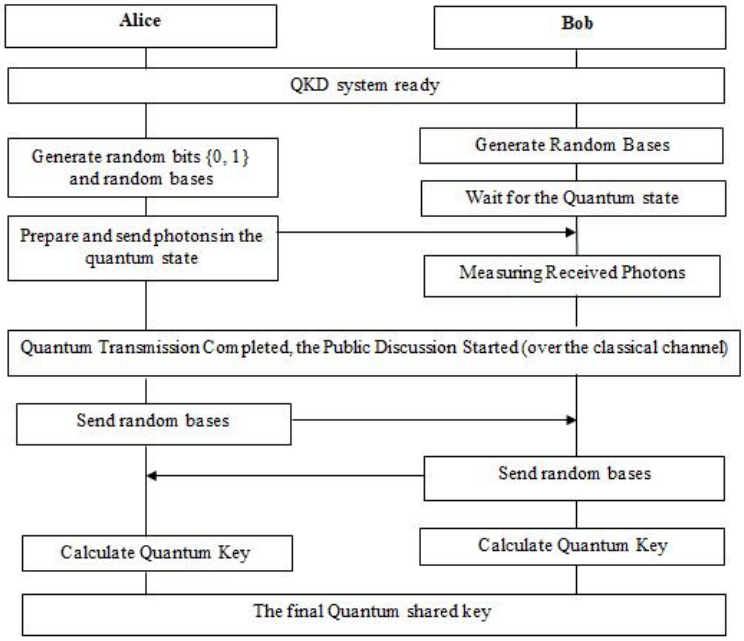

Figure 1. Flow chart for quantum key distribution using BB84 protocol.

Table 1. Comparison table.

Author	Title	Techniques	Advantages
A. Ahilan et.al (2022)	Quantum Key Distribution (BB84 protocol), throughput, the avalanche effect, encryption, and decryption.	QKD integrating with traditional encryption improves transmission security. Quantum cryptography has a high likelihood of identifying eavesdroppers and provides quick key delivery.	It is applicable for fewer miles only such that the messages will not deteriorate. When it comes to greater distance communication, QKD networks need repeaters, through which the key may be stolen.

DOI: 10.54254/2755-2721/8/20230083

Table 1. (continued).

Author	Title	Techniques	Advantages
Akwasi Adu-Kyere et.al (2022)	BB84 protocol, Heisenberg's uncertainty, and no-cloning principles.	The eavesdropping may be detected using quantum physics concepts. Also shows how unlikely it is for them to accurately guess which qubit or polarisation state is occurring.	It only provides a proof-of-principle and does not provide any real-world applications or implementations. The simulation results are based on theoretical models and assumptions which may not accurately reflect real-world scenarios.
Aayush Joshi et.al (2022)	RSA algorithm for public key cryptography, PGP for email applications, and Google's G Suite for PKC authentication.	It offers a potential solution to the problem of protecting data from quantum computers. Creating a web application for users makes it easier for users to decode encrypted messages without the need for computer knowledge or expertise.	Data sent over the internet would be less secure if it resulted in the creation of quantum computers that could decrypt RSA encryption. These sorts of computers may be costly and time-consuming to design and operate.
Vaishali Bhatia et.al (2020)	RSA algorithm, Shor's algorithm	Quantum computing algorithms can be used to break encryption algorithms more quickly than traditional methods. This could lead to improved security for data stored on computers or networks.	The usage of quantum computing algorithms is still very new. Not all businesses or people may be able to deploy quantum computing due to the complexity and expense involved.
Yahui Wang et.al (2018)	Phase estimation, Inverse Fourier transform, Polynomial-time quantum algorithm.	In this work, a novel polynomial-time quantum technique is given. It is also more dependable and effective than other existing algorithms due to its increased success probability.	It does not provide a complete solution to breaking RSA cryptographic systems.

Table 1 explains the comparison over the different papers along with their advantages, title name and respective authors.

3. Methodology

A quantum cryptographic application, Quantum Key Distribution (QKD), refers to the production of a secret key with guaranteed security assured by physical laws. Two individuals, Alice and Bob, use

DOI: 10.54254/2755-2721/8/20230083

quantum signals known as quantum bits, or simply qubits, to produce the key. Any attempt by an eavesdropper (say, Eve) to learn the key generates a disruption in the quantum signal, which leads to errors and, eventually, Eve's discovery.

Our project's major goal is to offer a method of secure communication only between the two intended communicating peers namely, Alice and Bob. This communication achieves security with the secure transmission of a secret key only. The BB84 protocol is used to implement the quantum key distribution which focuses on security proof.

There are mainly three steps to it:

a) Raw Key Generation

b) Sifted Key Identification

c) Eve's Information

As the receiver exposes some information about the sequence of detections he receives across a traditional communication channel like the Internet, which is also known as the classical channel, after the raw key exchange of a significant number of qubits. The bits that do not have a perfect correlation between the bits of the emitter and the receiver are deleted during the filtering process. The sifted key, which has the same length for both the recipient and the sender, is the result of the sifting process. The information obtained via the sifting prevents an eavesdropper from learning anything about the key.

The procedure of our project involves the following steps:

Step-1: Using (4+ δ) n random bits, Alice creates the bit string d.

Step 2: Alice sends (one at a time) Bob the (4+ δ)n qubits that result.

Step 3: Bob measures with the random bases to obtain the (4+ δ) n qubits.

Step 4: Alice and Bob discuss the random bases they have used and identify the sifted key.

Step-5: The sifted key is analysed to find the presence of Eavesdropper.

The safe delivery of the key increases the security of the data being transferred since the key is crucial for both the encryption and decryption of the data at both the sender and receiver ends of the communication. Here we followed a secure method to exchange keys between the two intended communicating peers. There is a chance of detecting the presence of Eavesdroppers in the transmission. Here we followed the two concepts, one is by assuming the absence of the Eavesdropper and the second thing is in the presence of the Eavesdropper. In the absence of Eavesdropper, the key distribution is secure in general. But in the presence of Eavesdropper, the key transmission will not be secure so, it needs to be discarded and regenerated.

The Quantum Key Distribution is implemented successfully and by using the BB84 protocol Eavesdropping is detected.

4. Conclusion

Cyber security is becoming more difficult as computational power increases. This project offers a thorough model of QKD communication. This a significant and uplifting step toward a day when we may feel more secure like our exchanges. We may thus expect that QKD will have a significant impact on basic physics, which will alter our perception of how quantum mechanics originated. For the time being, our technology offers a decent option for secure communication between two parties. But soon, someone could be able to use sophisticated tools to break this system, compromising security. Therefore, it is necessary to constantly upgrade the security protocols and procedures.

References

[1] Ahilan, A., & Jeyam, A. (2022). "Breaking Barriers in Conventional Cryptography by Integrating with Quantum Key Distribution". Wireless Personal Communications, 1-19.

[2] Adu-Kyere, A., Nigussie, E., & Isoaho, J. (2022). "Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3". Sensors, 22(16), 6284.

[3] Joshi, A., Kumbhar, R., Mehta, A., Kosamkar, V., & Shetty, H. (2022). "Breaking RSA Encryption Using Quantum Computer".

[4] Bhatia, V., & Ramkumar, K. R. (2020, October). An efficient quantum computing technique for

DOI: 10.54254/2755-2721/8/20230083

cracking RSA using Shor's algorithm. In 2020 IEEE 5th international conference on computing communication and automation (ICCCA) (pp. 89-94). IEEE.

[5] Wang, Y., Zhang, H., & Wang, H. (2018). Quantum polynomial-time fixed-point attack for RSA. China Communications, 15(2), 25-32.

[6] Quantum Key Distribution Secured Optical Networks: A Survey by 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) published on IEEE Open Journal of the Communications Society, 7 September 2021.

[7] Anusuya Devi, V., & Kalaivani, V. (2021). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Personal and Ubiquitous Computing, 1.

[8] Djordjevic, I. B. (2021). "QKD-Enhanced Cybersecurity Protocols". IEEE Photonics Journal, 13(2).

[9] Bibak, K., & Ritchie, R. (2021). Quantum key distribution with PRF (Hash, Nonce) achieves everlasting security. Quantum Information Processing, 20(7), 1-18.

[10] Lee, C., Sohn, I., & Lee, W. (2022). "Eavesdropping Detection in BB84 Quantum Key Distribution Protocols". IEEE Transactions on Network and Service Management, 19(3), 2689-2701.