Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 1, pp. 25–33, DOI 10.12694/scpe.v25i1.2152

A SECURE METHOD OF COMMUNICATION THROUGH BB84 PROTOCOL IN QUANTUM KEY DISTRIBUTION

CHUNDURU ANILKUMAR *, SWATHI LENKA †, N. NEELIMA ‡, AND SATHISHKUMAR V E §

Abstract. Security awareness is one of the most pressing topics in today's globe. The idea of cryptography is introduced when the subject is information security. Conventional cryptography-based security techniques rely on the presumption that keys are shared before secure connections. The most crucial factor to consider when integrating cryptographic operations into account when integrating cryptographic operations in with any system is the safe key management strategy required for sending and transferring a secret key between two entities The systems will be vulnerable to bugs and possibly fatal external assaults if the fundamental management methods are poor A method for securely encrypting data sent between parties is quantum cryptography. and spotting eavesdroppers trying to overhear the conversation. Quantum cryptography may be the solution to these issues a quantum cryptography application, Quantum Key Distribution (QKD), refers to the production of a cryptographic key with unconditional security assured by physical rules. Quantum cryptography is a kind of encryption. We examine the quantum key exchange protocol (BB84 protocol) in this study and the way that it significantly improves data transfer security when compared to standard encryption techniques. The main objective of quantum cryptography is to offer a trustworthy way to provide a secure method of communication between the intended peers only and to detect the Eavesdropper presence.

Key words: Security, Cryptography, Quantum Cryptography, Rivert Shamir Adleman Algorithm, Shor's Algorithm, Quantum Key Distribution, BB84 protocol.

1. Introduction.

The emergence of the implementation of quantum computers brings significant risks to current encryption methods; for example, the implementing the Shor algorithm can obsolete in a very short period. This has probably led us to seek alternative methods of encrypting data with a greater degree of safety. To encrypt messages, provable secure cryptosystems (for example, OTP) rely on the exchange of a secret key between sender and receiver. Quantum cryptography, sometimes referred to as quantum encryption, uses quantum physics to encrypt communications so that only the end user can decipher them.

Photons and their inherent quantum characteristics are used in quantum cryptography to create a secure cryptosystem. While the quantum state of any entity cannot be determined without destroying it, quantum cryptography relies on the usage of photons and their intrinsic quantum features to create an unbreakable cryptosystem. These are the optical fiber cable data transmitters, a trustworthy channel for communications with extremely high bandwidth. The fundamentals of quantum physics indicate that noticing a quantum state causes disruption. Because of the various QKD techniques, any possible listener intending to track the delivered photons will interfere with the communication. This interference will cause transmission issues, which authorized users would be capable of identifying. That has been done to guarantee the safety of the given keys.

1.1. Quantum Cryptography vs. Traditional Cryptography.

A classical bit is the fundamental element of traditional computation and information systems. Similarly, the basic element of quantum information as well as quantum computation systems is the qubit, a term invented by Benjamin Schumacher.

In a traditional system, a bit can be either 0 or 1. A qubit has two basic states in quantum systems, which are expressed as $|0\rangle$ or $|1\rangle$, where $|\ \rangle$ is Dirac notation.

*Department of Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh, 532127, India, ORCID ID:0000-0002-3537-127X (anilkumar.ch@gmrit.edu.in)

†Department of Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh, 532127, India, ORCID ID: 0009-0004-8240-2560 (swathi.l@gmrit.edu.in)

‡Department of Information Technology, RVR & JC College of Engineering, Guntur, Chowdavaram, Andhra Pradesh, India (neelimanalla1979@gmail.com)

§Department of Computing and Information Systems, Sunway University, 47500, Petaling Jaya, Selangor Darul Ehsan, Malaysia (sathishv@sunway.edu.my)

$$|\Psi 00 = |0\ ,$$
$$|\Psi 10\ = |1\ ,$$
$$|\Psi 01 = |+ = 1/\sqrt{2}|0\ + 1/\sqrt{2}|1\ ,$$
$$|\Psi 11 = |- = 1/\sqrt{2}|0\ - 1/\sqrt{2}|1\ .$$

The traditional form of cryptography is the method of mathematically encrypting the message so that only one person with the correct key can read it. There are two types of key distribution in traditional cryptography: symmetric key and asymmetric key [4]. Asymmetric cryptography encrypts communications using a public key and decodes them employing a private key, in contrast to symmetric key algorithms that decrypt and encrypt data with a unique secret key. Traditional cryptography techniques have been trusted because it would take classical computers an impractical amount of time to factor the required large numbers, that are required to make up both private and public keys [18].

Unlike conventional encryption, quantum cryptography is based on the ideas of quantum physics. And, unlike traditional cryptography, which is rooted in mathematical equations and calculations quantum cryptography is considerably more difficult to decrypt because perceiving the involved photons alters the expected outcome, alerting both the sender as well as the recipient to the involvement of an eavesdropper [15]. Because the process requires fiber optic cables, as well as repeaters, as well as repeaters distributed out to boost the signal, quantum cryptography usually has a distance or field of view associated with it.

Existing encryption systems, on the other hand, are threatened by quantum algorithms. Another quantum approach capable of defeating symmetric encryption is the Grover algorithm. For instance, the popular Shor method can decipher asymmetric encryption schemes like Elliptic Curve and RSA. Whereas key exchanges are protected by quantum physics in quantum cryptography [8]. Moreover, the security of ordinary encryption is threatened by insecure random key generators, increases in CPU power, innovative attack strategies, and the development of quantum computers. Such encrypted information has no significance in the case of quantum computers. In the future, quantum computers will be able to intercept and preserve encrypted data for decryption [6]. Quantum cryptography has the advantages of "unconditional security" and Eavesdropper detection. These qualities may be useful in addressing cyberspace security issues for the next-generation internet and associated applications like the internet of things as well as smart cities.

- RSA algorithm is implemented as an example of a Conventional Key Exchange algorithm.
- The Shor's algorithm is implemented to show how Quantum algorithms (Shor's) breaks Conventional algorithm.
- Quantum Key Distribution in conventional cryptography provides a secure method of communication.
- Data transmission security is elevated to a greater level via QKD.
- Python tools like Qiskit are used to implement QKD using the BB84 protocol.

The remaining sections of this paper are demonstrated as follows: Introduction to Quantum Cryptography, Section 2: Using the BB84 protocol for quantum key distribution and then the comparison of Quantum cryptography and traditional cryptography, Section 3: The related work needed to the paper, Section 4: The process for distributing quantum keys is described, Section 5: The results are analysed and explained, section 6: It encloses the conclusion.

1.2. The BB84 Protocol for Quantum Key Distribution (QKD). The four-state BB84 protocol is integrated with the quantum key distribution (QKD) technique, a quantum cryptography technique, by assuming an ideal quantum channel atmosphere in which the eavesdropper is the only factor contributing to QBER greater than zero. N binary bits are first generated by Alice and must be transferred to Bob. Alice randomly selects a polarization basis from the diagonal () or rectangle (+) to encrypt a binary bit into a qubit.

Binary data 0 and 1 might be represented on the rectangular basis, for instance, by a qubit having polarizations. As a result, a qubit having polarizations can diagonally denote 1 and 0, respectively. The no-cloning theorem, which states that any arbitrarily defined unknown quantum state cannot be flawlessly copied, ensures this.

The data is encoded as non-orthogonal qubits, which is essential for detecting eavesdropping. Naturally, Eve may try to capture those quantum carriers and measure them. She is unaware of the precise group of carriers Alice pre-selected for each important component, just like Bob. She could be unable to distinguish

Table 1.1: BB84 protocol polarization scheme

Basis	Bit	Polarization of Photon
Rectangular (+)	0	→
	1	↑
Diagonal (x)	0	↖
	1	↗

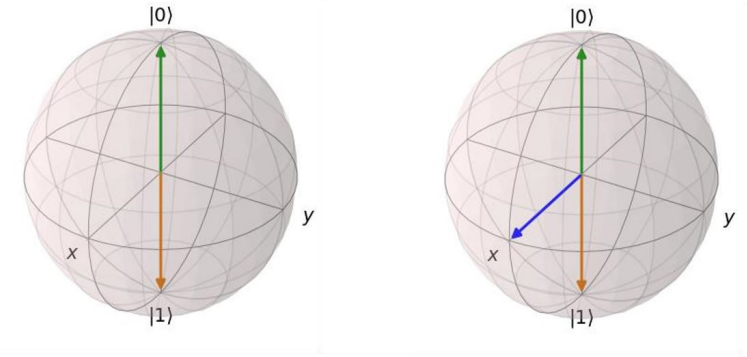

Fig. 1.1: Representation of Qubits as Bloch sphere

between $|0\rangle$ and $|1\rangle$, when Alice encrypts a bit as $|+\rangle$ or $|-\rangle$, or vice versa, just like Bob. But in contrast quantum cryptography, this usually involves Alice (A) and Bob (B) wishing to exchange confidential details while eavesdropper Eve (E) tries to intercept the message without even being detected. The main objective of quantum cryptography is to offer an effective means of detecting Eve's activity.

1.3. Qubits Representation and their Properties. The BB84 protocol is a well-known quantum key distribution (QKD) protocol that enables secure communication between two parties using the principles of quantum mechanics. It uses qubits, the fundamental units of quantum information, to encode information in a secure and tamper-evident manner. This report aims to explain the representation of qubit states through the BB84 protocol and discuss their properties[4].

In the BB84 protocol, qubit states are used to encode information. A qubit can exist in a superposition of two basis states, usually denoted as $|0\rangle$ and $|1\rangle$. These basis states correspond to the classical bit states 0 and 1, respectively. The qubit states can be represented as linear combinations of the basis states, such as $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex probability amplitudes that satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

The BB84 protocol involves the following steps: Qubit Preparation: The sender (Alice) prepares a series of qubits in random states. These qubits can be in either the $|0\rangle$, $|1\rangle$, or superposition states. Qubit Transmission: Alice sends the prepared qubits to the receiver (Bob) through a quantum channel, which can be a physical medium like optical fibers. Measurement Basis Selection: Bob randomly chooses a measurement basis for each received qubit from two possible options, denoted as the computational basis ($|0\rangle$, $|1\rangle$) and the Hadamard basis ($|+\rangle$, $|-\rangle$). d. Measurement: Bob measures each qubit in the chosen basis and obtains classical measurement outcomes [5]. Basis Announcement: Alice and Bob publicly communicate the bases they used for each qubit transmission but not the measurement outcomes. Key Generation: Alice and Bob retain the bits for which their measurement bases matched, forming a shared secret key for secure communication.

In the BB84 protocol, different qubit states are used to encode information. These states have specific properties that contribute to the security of the protocol: $|0\rangle$ and $|1\rangle$ States: These are the computational basis states and represent the classical bit states. They are orthogonal and form the basis for secure key generation in the protocol.

B $|+\rangle$ and $|-\rangle$ States: These are the superposition states in the Hadamard basis. They are also orthogonal and provide a second basis for key generation. The $|+$ state represents an equal superposition of $|0\rangle$ and $|1\rangle$, while the $|-\rangle$ state represents their difference [6].

Randomness and Security: The security of the BB84 protocol relies on the randomness of the qubit states chosen by Alice and the measurement bases chosen by Bob. The random choice of states ensures the security of the key against eavesdropping attempts.

2. Related Work. The application of a unique quantum key distribution (BB84 protocol) and the way it may be utilized with conventional encryption methods to increase the security of data transmission. Moreover, it compares the encryption, decryption, avalanche impact, and performance of both QKD free versions - and QKD of these operations to assess the performance of various cryptographic techniques for a variety of file sizes. This work explores quantum cryptography is possible uses in secure communication systems, building on earlier research into the subject [5, 9, 25]. Solid evidence that uses a communicative architectural model and execution to mimic the concepts of quantum physics. It employs both the presence and absence of an eavesdropper in the quantum key distribution (QKD), implemented with BB84 protocol. Heisenberg's uncertainty principle and no-cloning principle can be utilized to find an eavesdropper, according to simulation findings. according to simulation results, although the chances of them accurately guessing which polarization state to listen in on is quite tiny [1, 13]. Quantum computing's current status of development and its uses in cryptography. It looks at the resistance of current encryption techniques to quantum computing and how the quantum computer can be employed to predict secret keys for communication decryption. The development of an application that enables users to utilize this technique to decode encrypted communications is also covered [17, 12]. Quantum computing algorithms, particularly Shor's algorithm, will be examined in this session to see how they may be used instead of conventional techniques to break encryption systems. In order to evaluate the efficacy of various quantum computing techniques, it will also examine the topics of storage capability, computation time precision, correctness, integrity, availability, and efficiency [14]. Factorial quantum technique for RSA cracking is presented in this paper without specifically calculating the modulus of n. Its foundation is the phase estimation and quantum inverse Fourier transform. The Shanks' SQUARE Form Factorization method, the Lehman methodology, and there have been several investigations on the RSA Quantum Polynomial-Time Fixed-Point Attack and compared to this strategy as approaches to the Integer Factorization Problem (IFP) [23]. Extensive overviews of cutting-edge QKD-protected optical networks that will have an impact on communication networks in the coming decades. The fundamental setup technique is described, as well as the procedures and methods used in QKD-protected optical networks. It contains a full explanation and comparison of the many ways proposed in the literature to manage networking-related difficulties [24]. The application of wireless body sensor networks (WBSN) for remote medical surveillance during the COVID-19 pandemic. Following an examination of the most recent security vulnerabilities to WBSN data, a unique upgraded BB84 Quantum Cryptography Protocol (EBB84QCP) is proposed as an effective way for safe key distribution without the direct exchange of secret keys [10]. Current state of research in post-quantum cryptography and quantum key distribution (QKD) approaches. This work employs QKD to improve current encryption protocols such as Rivest-Shamir-Adleman (RSA) and render them more resistant to quantum computer assaults. The paper also discusses how utilizing a QKD protocol to initialize may assist avoid brute force attacks by trying to prevent Eve from learning N and breaking the protocol via a brute force technique [20].

For authentication, QKD employs the PRF (Hash, Once) MAC paradigm. Because of the variety of functionality it offers, this MAC is suited for QKD. Yet, PRF is more important than the Wegman-Carter paradigm, one of most popular MAC approach in QKD (Hash, Nonce). It ensures eternal security, which implies that even with unlimited computational power, the attacker cannot learn any additional knowledge about the generated keys as far as authentication is not interrupted during QKD execution [19, 16, 11]. The Bennett-Brassard-84 (BB84) quantum key distribution (QKD) protocol's upper bounds on false-negative and false-positive ratios for eavesdropping detection are examined in this study. In order to deal with the constantly shifting quantum channel circumstances, it additionally offers a clustered BB84 protocol and a combinatorial eavesdropping detection method. The authors conducted a detailed simulation analysis to evaluate their proposed methodologies. The results showed that they can detect eavesdroppers with a minimum of 99.92% accuracy in such situations [22, 21].

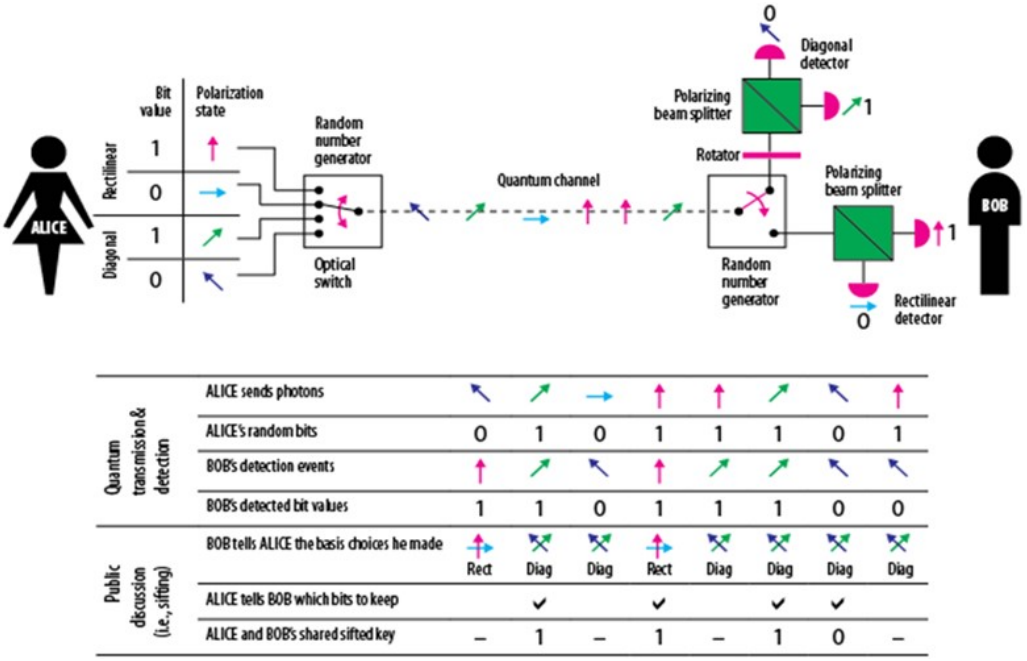

Fig. 2.1: Working process of the bb84 protocol

3. Proposed Methodology. The Quantum Key Distribution is integrated with the BB84 protocol to focus more on security proof. To generate the key, two people, Alice and Bob, employ quantum signals known as quantum bits, or simply qubits. Each attempt by an eavesdropper (say, Eve) to obtain the key causes a disturbance in the quantum signal, which eventually leads to 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 major steps involved in this methodology are:

1. Key Generation
2. Key Sifting
3. Key distillation

Key Generation.

- The emitter transmits a photon whose polarization is chosen at random among the four states for each bit. He keeps track of the orientation in a list.
- The photon is sent across the quantum channel.
- The receiver sets the direction horizontal or diagonal of a filter that allows it to differentiate between two polarization states at random for each incoming photon. He keeps track of these orientations as well as the results of the detections — photons deflected to the right or left.

Key Sifting. This information is used by the emitter to compare the orientation of the photons he has delivered with the matching filter orientation. He informs the recipient in which circumstances the orientations are compatible and which are not. As seen in the BB84 protocol diagram, following sifting, the two parties have a sequence of bits known as the sifted key, that are identical in the absence of an eavesdropper. and can function as a secret key.

Key Distillation. If no eavesdropper was present during the transmission and the apparatus utilized was optimal, the key should be error-free after Key Sifting. To avoid risking the key's security, these mistakes are all attributed to the eavesdropper. Following that, a post-processing procedure called as Key Distillation is carried out.

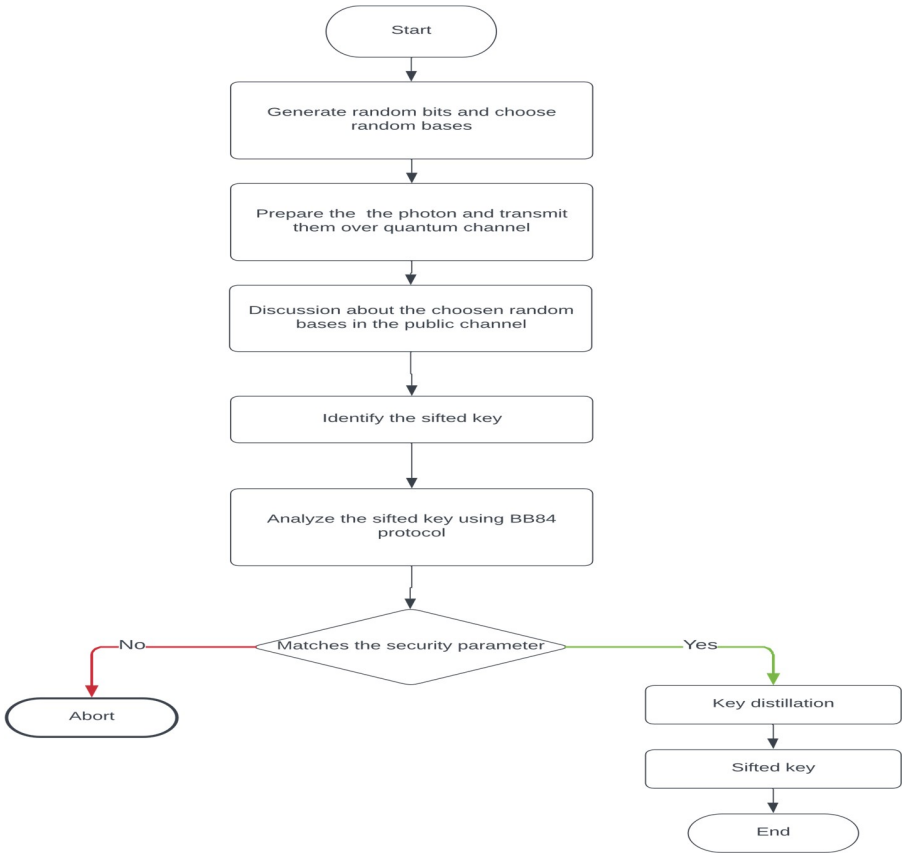

Fig. 3.1: Flow chart of the QKD Methodology using BB84 Protocol

4. Results and Discussions.

4.1. Shor's Algorithm Breaking the RSA Encryption. Shor's algorithm has successfully deciphered the RSA algorithm, by finding the factors of the given N value and also finding the private key. The below Fig.4.1 is the results shown after the implementation of Shor's algorithm. Here, the time taken to crack the factors of N value is increasing with the value of N linearly.

4.2. Analysis of the generation of Quantum keys' Time Complexity. There are three steps in Quantum Key Distribution: key creation, key filtering, and key distillation. The below fig.4.2 describes the time taken for key generation through the Quantum key distribution. The below results discuss that the time that quantum key generation takes is very small with respect to the number of bits and less when compared with the other conventional key generation algorithms such as RSA.

4.3. Quantum Key Distribution without Eve's Presence:. At the first step of Quantum key distribution Alice generates the random bits and chooses the random bases to transmit them to Bob. This key transmission process is n happens through the quantum channel. And then Bob will choose the random bases(filters) to receive the bits sent by Alice. The below Fig.4 discusses the random bits, basis, and polarised photons sent by Alice and the corresponding bits and basis received by Bob. Here in Table 4.1: $h = \rightarrow$; $v = \uparrow$; $r = \nearrow$; $l = \nwarrow$

In Table 4.1 shows the sifted key after the key generation and key sifting process. The actual secret key will be generated after the key distillation process. Below is the secret key of 16 bits that is distributed between Alice and Bob with the restriction that an eavesdropper does not exist between the communicating peers

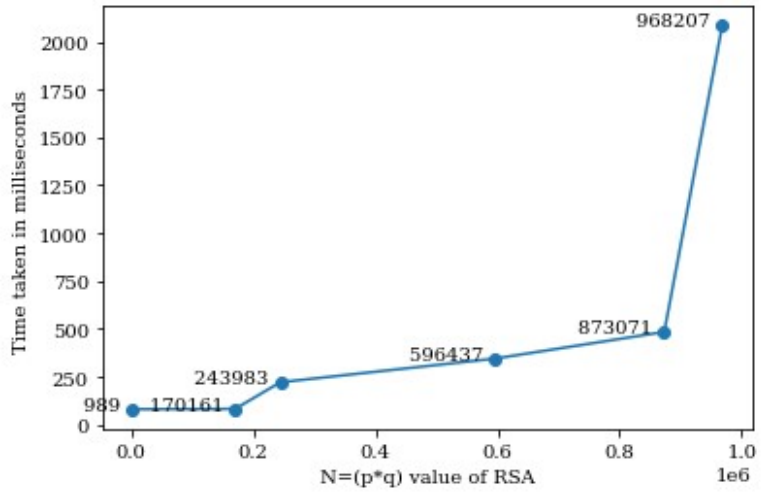

Fig. 4.1: Time Required for Shor's Algorithm to Defeat the RSA Scheme.

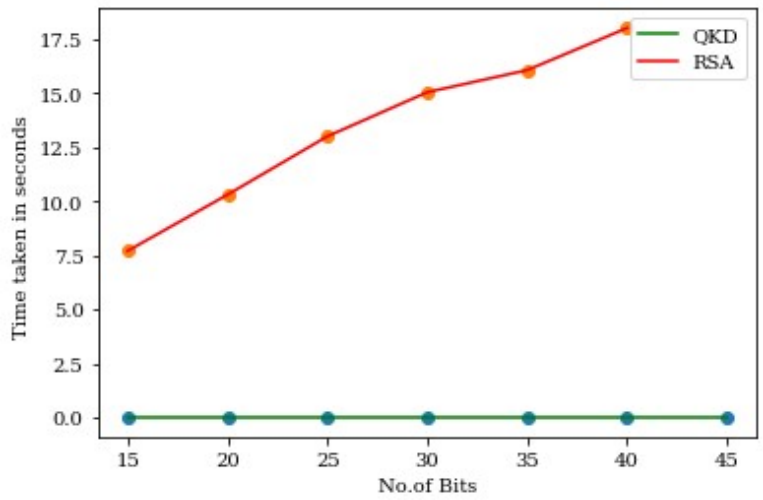

Fig. 4.2: Analysis of the Time Complexity of Quantum Key Generation

Table 4.1: Alice and Bob's Bitstream along with bases and identifying the sifted key

A_bits	1	1	1	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0	1	1	1	0	1	0	0	1	1	1	1	0	0	0
A_basis	+	x	x	x	+	+	x	x	x	x	+	+	+	+	+	+	x	x	x	x	x	x	x	+	+	x	x	x	x	+	x	x
A_photons	h	l	l	l	h	h	l	r	l	r	h	v	h	h	h	h	r	r	l	l	l	r	l	v	v	l	l	l	l	v	r	r
B_basis	x	+	+	x	x	x	+	+	x	x	+	+	+	x	+	x	x	x	+	x	+	x	+	x	x	x	+	+	x	+	+	+
B_bits	1	0	1	1	0	1	1	1	1	0	1	0	1	0	1	1	0	0	1	1	0	0	0	1	1	1	0	0	1	0	0	
Sifted key				1					1	0	1	0	1		1		0	0		1						1			1	0		

Table 4.2: Secret key of 16 bits that is Distributed between Alice and Bob

Secret Key	0	0	0	1	0	0	0	0	1	0	1	0	1	0	1	0

Table 4.3: Alice and Bob's bitstream in the presence of Eavesdropper

A_bits	1	1	0	1	0	1	0	1	1	1	1	0	0	1	1	1	0	0	1	0	1	1	1	1	0	1	0	1	0	1	1	0
A_basis	+	+	x	x	x	x	+	+	x	+	x	+	x	+	+	x	+	x	+	+	+	+	x	+	+	x	x	+	x	+	+	+
A_photons	h	h	r	l	r	l	h	h	r	v	l	v	r	h	h	r	h	l	h	v	v	v	l	h	h	l	l	v	l	h	h	h
E_photons	r	l	r	l	h	l	h	l	h	v	v	v	v	h	h	h	l	l	h	v	v	v	l	h	r	l	l	v	l	h	h	h
E_bits	1	1	0	1	0	1	0	1	1	1	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0	1	0	0	1	0
B_basis	x	+	+	x	+	x	x	+	x	+	+	+	x	x	+	x	+	x	+	x	+	x	x	x	+	+	+	+	+	+	+	x
B_bits	0	1	1	0	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1	1	0	1	0	1
Sifted key		1							1				0		0													1		1		

4.4. Quantum Key Distribution During Eavesdropper Presence:. Here is the other case, which involves the distribution of quantum keys while being monitored by an Eavesdropper. To get the value of the bit, he must witness the photon, which will disrupt the conversation and betray his existence. A more sophisticated technique would be for the eavesdropper to detect the photon, register the bit value, and prepare a new photon based on the result to broadcast to the receiver. The two legitimate parties collaborate in quantum cryptography to prevent the eavesdropper from doing so by compelling him to create mistakes. Eve tries to intercept the quantum channel's qubit using an intercept resend attack. Bob's modified and measured qubits alter the initial shared key. Here in Table 3; $h = \rightarrow$; $v = \uparrow$; $r = \nearrow$; $l = \nwarrow$

In Table 4.3 represents the bitstream of both Alice and Bob in the Eavesdropper and demonstrates how the existence of the Eavesdropper causes Quantum Bit Error Rate to rise. Thus, the provided need to be discarded and the whole process need to be started again.

5. Conclusion. In this work, the proposed method and the Quantum Key distribution Using protocol were implemented. Here, the primary exploit in the traditional cryptographic key exchange technique has been exposed, namely the ability to defeat the RSA algorithm's fundamental building blocks using Shor's algorithm. The time required to produce the key using a quantum cryptography method and a conventional cryptographic algorithm were compared and analyzed. Quantum Key Distribution takes less time to generate the key for the encryption of the data. As computer power grows, cyber security becomes more complex. This project provides a comprehensive model of QKD communication. This is a huge and encouraging step towards a day when we may feel more confident in our interactions. As a result, we may anticipate that QKD will have a profound influence on basic physics, altering our understanding of how quantum mechanics evolved. For the time being, our technology provides a reasonable solution for two-way encrypted communication. Yet, someone may soon be able to utilize sophisticated tools to breach this system, jeopardizing security. As a result, security policies and procedures must be updated on a regular basis.

REFERENCES

[1] Dariush Abbasinezhad-Mood and Morteza Nikooghadam. An anonymous ecc-based self-certified key distribution scheme for the smart grid. *IEEE Transactions on Industrial Electronics*, 65(10):7996–8004, 2018.

[2] Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Quantum key distribution: Modeling and simulation through bb84 protocol using python3. *Sensors*, 22(16):6284, 2022.

[3] A Ahilan and A Jeyam. Breaking barriers in conventional cryptography by integrating with quantum key distribution. *Wireless Personal Communications*, pages 1–19, 2022.

[4] Vaishali Bhatia and KR Ramkumar. An efficient quantum computing technique for cracking rsa using shor's algorithm. In *2020 IEEE 5th international conference on computing communication and automation (ICCCA)*, pages 89–94. IEEE, 2020.

[5] Khodakhast Bibak and Robert Ritchie. Quantum key distribution with prf (hash, nonce) achieves everlasting security. *Quantum Information Processing*, 20(7):228, 2021.

[6] Ivan B Djordjevic. Qkd-enhanced cybersecurity protocols. *IEEE Photonics Journal*, 13(2), 2021.

[7] Aayush Joshi, Rutuja Kumbhar, Akshat Mehta, Vaishali Kosamkar, and Harshith Shetty. Breaking rsa encryption using quantum computer. 2022.

[8] V Kalaivani et al. Enhanced bb84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Personal and Ubiquitous Computing*, page 1, 2021.

[9] Chankyun Lee, Ilkwon Sohn, and Wonhyuk Lee. Eavesdropping detection in bb84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management*, 19(3):2689–2701, 2022.

[10] Yonghong Ma, Xiuyu Wang, and Dandan Cui. Secure communication mechanism for smart distribution network integrated with subcarrier multiplexed quantum key distribution. *Power Syst. Technol.*, 11:036, 2013.
[11] Mosayeb Naseri. Revisiting quantum authentication scheme based on entanglement swapping. *International Journal of Theoretical Physics*, 55:2428–2435, 2016.
[12] Vanga Odelu, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti. Provably secure authenticated key agreement scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(3):1900–1910, 2016.
[13] Amritha Puliadi Premnath, Ju-Yeon Jo, and Yoohwan Kim. Application of ntru cryptographic algorithm for scada security. In *2014 11th international conference on information technology: new generations*, pages 341–346. IEEE, 2014.
[14] Neetesh Saxena and Santiago Grijalva. Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication. *IEEE Transactions on Industrial Informatics*, 13(3):1482–1491, 2016.
[15] Purva Sharma, Anuj Agrawal, Vimal Bhatia, Shashi Prakash, and Amit Kumar Mishra. Quantum key distribution secured optical networks: A survey. *IEEE Open Journal of the Communications Society*, 2:2049–2083, 2021.
[16] Vishal Sharma, Kishore Thapliyal, Anirban Pathak, and Subhashish Banerjee. A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. *Quantum Information Processing*, 15:4681–4710, 2016.
[17] Jia-Lun Tsai and Nai-Wei Lo. Secure anonymous key distribution scheme for smart grid. *IEEE transactions on smart grid*, 7(2):906–914, 2015.
[18] Yahui Wang, Huanguo Zhang, and Houzhen Wang. Quantum polynomial-time fixed-point attack for rsa. *China Communications*, 15(2):25–32, 2018.
[19] M Xin, Z Liang, P Ma, N Jin, and M Zhu. Optical fiber transmission solution of measurement and control signal between substations based on quantum key distribution and one-time pad. *Automation of Electric Power Systems*, 41(12):212–217, 2017.
[20] MIAO Xin and CHEN Xi. Quantum logic circuit of quantum bit error correction coding and decoding for quantum communication in smart grid substation. In *Zhongguo Dianji Gongcheng Xuebao/Proc. Chin. Soc. Electr. Eng.*, volume 34, pages 4359–4363, 2014.
[21] Hao Yuan, Yi-min Liu, Guo-zhu Pan, Gang Zhang, Jun Zhou, and Zhan-jun Zhang. Quantum identity authentication based on ping-pong technique without entanglements. *Quantum information processing*, 13:2535–2549, 2014.
[22] Piotr Zawadzki, Zbigniew Puchała, and Jarosław Adam Miszczak. Increasing the security of the ping–pong protocol by using many mutually unbiased bases. *Quantum information processing*, 12:569–576, 2013.
[23] Baokang Zhao, Bo Liu, Chunqing Wu, Wanrong Yu, Jinshu Su, Ilsun You, and Francesco Palmieri. A novel ntt-based authentication scheme for 10-ghz quantum key distribution systems. *IEEE Transactions on Industrial Electronics*, 63(8):5101–5108, 2016.
[24] J Zhou, L Lu, Y Lei, and X Chen. Research on improving security of protection for power system secondary system by quantum key technology. *Power Syst. Technol*, 38(6):1518–1522, 2014.
[25] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, and Jun Shen. Quantum cryptography for the future internet and the security analysis. *Security and Communication Networks*, 2018:1–7, 2018.

Edited by: Achyut Shankar
Special issue on: Machine Learning for Smart Systems: Smart Building, Smart Campus, and Smart City
Received: Mar 16, 2023
Accepted: Nov 11, 2023