



Breaking Barriers in Conventional Cryptography by Integrating with Quantum Key Distribution

A. Ahilan¹ · A. Jeyam²

Accepted: 15 October 2022 / Published online: 15 November 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Security techniques based on conventional cryptography assume keys are disseminated prior to secure communications in traditional security mechanisms. The essential function of transmitting and sharing a secret key between two entities is the safe key management technique, which is the most important components to be concerned about when incorporating cryptographic activities into any system. If the key management procedures are ineffective, the system will be vulnerable to vulnerabilities and potentially lethal outsider attacks. Quantum cryptography is a method of securely encrypting information sent between parties while also detecting intruders attempting to listen in on the discussion. Quantum cryptography holds promise as a solution to these and other issues. In this paper, we discuss the Quantum key distribution (BB84 protocol) and how when integrated with conventional cryptography algorithms it increases security in data transmission to a remarkably high level. We also compare the cryptography algorithms for different file sizes and measure their performance by calculating the Encryption, decryption, throughput and Avalanche effect of the algorithms with and without QKD. The elapsed time of the conventional algorithm with QKD achieve 56.8%, 58.6% and 54.3% less time than AES, 3DES and Blowfish respectively.

Keywords Quantum cryptography · Classical cryptography · QKD · Eavesdropping · Key refinement

1 Introduction

Quantum cryptography [1], also known as quantum encryption, makes use of quantum mechanics principles to encrypt messages so that no one other than the intended receiver can read them. Quantum cryptography varies from conventional cryptography systems in that physics plays a fundamental role in its security concept whereas in conventional cryptography, mathematics plays a key role. Quantum cryptography depends on the utilization of photons and their integral quantum properties to produce an cryptosystem that is

✉ A. Ahilan
listentoahil@gmail.com

¹ Department of ECE, PSN College of Engineering and Technology, Tirunelveli 627 152, India

² Lord Jeggannath College of Engineering, Anna University, Chennai, Tamil Nadu 627 106, India

unbreakable—principally since any system's quantum state cannot be measured without disrupting it. They're the data carriers of optical fiber cables, which are used for extremely high-bandwidth communications as a reliable medium. According to the fundamentals of quantum physics, observing a quantum state causes disturbance. Any eavesdropper attempting to track the transmitted photons will cause the transmission to be interrupted thanks to the various QKD mechanisms. This interference will cause transmission failures that authorized users will be able to identify. This is used to ensure that the distributed keys are secure. Quantum computers are quickly evolving, with the potential to provide major computer science capabilities capable of handling a wide range of critical, even life-saving, computing problems that regular computers cannot. Regrettably, Quantum computers can create new dangers at an unprecedented pace and scale. Hackers that use quantum computing as part of their attack arsenal will be able to quickly decipher today's encryption methods. Some types of computing issues will be much easier to tackle with this technology than with today's traditional computers. Quantum computing poses two threats, which will be addressed using two pillars. There is a need to develop classical algorithms that can survive quantum computers in the first place. In computing, these algorithms are referred to as post-quantum algorithms.

1.1 Quantum Versus Conventional Cryptography

In conventional cryptography [2], the original text is encrypted to ciphertext, which is then sent through a channel controlled by a key data string. Only if the receiver has this key will he be able to retrieve the original information and understand the original text. There are two primary techniques in classical cryptography: symmetric and asymmetric cryptography. Algorithms like AES, Triple DES and Blowfish algorithm are used as convolutional cryptographic algorithms.

Among the most popular and commonly used symmetric block cypher algorithms is the Advanced Encryption Standard (AES) algorithm [3]. This method, which is used worldwide in hardware and software, has a unique structure that makes it ideal for encrypting and decrypting sensitive data. Three distinct key sizes—AES 128, 192, and 256 bit—can be handled by AES, and each of these cyphers has a 128 bit block size. Without creating a completely new cryptosystem, the Triple Data Encryption Standard (3DES) algorithm [4] was created to overcome the blatant vulnerabilities in DES. The 56-bit key used by the Data Encryption Standard (DES) is regarded as insufficient to secure sensitive data. 3-DES simply increases the DES key size by running the algorithm three times consecutively with three distinct keys. Thus, 168 bits make up the total key size. A symmetric block cypher that employs the Feistel network, simple encryption and 16 iterations of decryption is called the blowfish algorithm [5]. There are many benefits to each Feistel structure, especially in hardware. The only prerequisite for decrypting the cypher text is to flip the key schedule. Quantum algorithms, on the other hand, pose a danger to existing cryptography systems. The Grover algorithm, another quantum technique, is capable of breaking symmetric cryptography. The famous Shor algorithm, for example, can decrypt asymmetric cryptography schemes like RSA and Elliptic Curve.

While Quantum cryptography makes use of quantum mechanics to safeguard key exchanges. Furthermore, weak random key generators, advancements in CPU power, new attack techniques, and the development of quantum computers all challenge the security of traditional encryption. Such encryption is rendered worthless in the case of quantum computers in particular. Data that is encrypted today can be intercepted

and saved in the future for decryption by quantum computers. The benefits of quantum cryptography include "unconditional security" and sniffer detection. These features may be useful in addressing cyberspace security issues for the future internet and applications like the internet of things and smart cities.

The 127-qubit Eagle processors are the latest addition to IBM Quantum's systems, which also have 27-qubit Falcon and 65-qubit Hummingbird processors. Eagle, a 127-qubit quantum processor from IBM Quantum, is based on the transmon superconducting qubit architecture. In general, we use three measures to compare our three major performance qualities across these devices: Measure scale in terms of the number of qubits, quality in terms of quantum volume, and speed in terms of CLOPS, or circuit layer operations per second. For superconducting quantum computers, "classical cross-talk" is a significant source of errors. The major contribution of this paper is given as follows;

- QKD is integrated with classical cryptography algorithms it increases the security in transmitting data to a high level
- Quantum key distribution (QKD) allows users to safely exchange conventional keys, which can then be utilized for secure communication.
- Key distillation procedures is used for bit error estimation.
- The Cascade technique is used to identify and fix all key transmission defects in noisy quantum channels.
- QKD using BB84 protocol is implemented using Python packages like QuTip. The BB84 protocol is compared with different implementation platforms like C++ Sim and OMNeT++.

The remaining section of this research is demonstrated as follows. The quantum Key Distribution using BB84 is explained in Sect. 2. A comparison of Quantum cryptography protocols is explained in Sect. 3. Other Methods for secret key Exchange is discussed in Sect. 4. The performance outcome and their analysis are provided in Sect. 5. Section 6 encloses Conclusions.

2 Quantum Key Distribution (QKD) Using BB84 Protocol

Instead of encrypting data, quantum key distribution allows users to safely exchange conventional keys, which can then be utilized for secure communication. QKD [6] is a technique for transmitting secret keys that relies on some unusual subatomic particle characteristics and is, at least in theory, entirely unhackable. One at a time, photons are transmitted across a fiber optic wire in the land-based form of QKD. If someone is listening in, the polarization of the photons is changed, and the recipient may determine that the message isn't secure, according to quantum physics principles. Quantum key distribution (QKD) employs quantum mechanics to provide safe transmissions by allowing users to securely exchange keys to one another and enabling encrypted communication that can't be deciphered by malicious eavesdroppers. QKD protects communications but does not encrypt the information sent. QKD systems allow two linked parties to communicate securely using a stream of photons (light particles) to transmit the data and private key.

2.1 Qubits

Qubits [7], or quantum bits, are used in quantum computers. The qubit's state can be denoted as a vector $|\psi\rangle$ (Fig. 1)

$$|\psi\rangle = y|0\rangle + z|1\rangle, \quad y, z \in \mathbb{C}, |y|^2 + |z|^2 = 1 \quad (1)$$

A qubit is in one of two states: $|0\rangle$ or $|1\rangle$ or in a superposition of the two states, i.e., $y|0\rangle + z|1\rangle$. A qubit is said to be pure if it is in one of two states $|0\rangle$ or $|1\rangle$. We call it a superposition of the pure states $|0\rangle$ and $|1\rangle$ if it isn't otherwise.

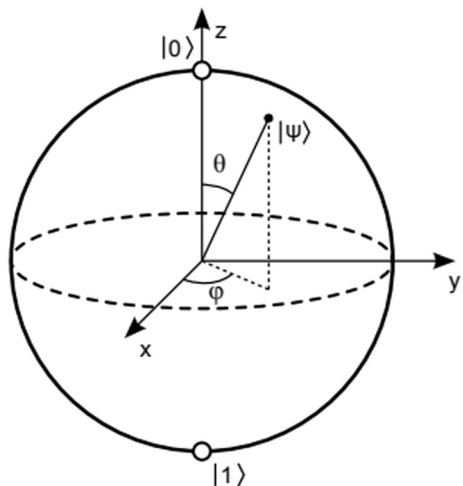
2.2 The Working Process of QKD

To exchange a secret key in the BB84 protocol [8], Alice and Bob must do the following:

Assume that Alice and Bob need to transmit information in secret to each other. Alice begins the communication by sending Bob a secret key that will be used to encrypt the data. This secret key is a series of random bits conveyed by using a specific type of scheme in which two distinct beginning values can be used to represent the same binary value (0 or 1). Alice and Bob decide to encrypt their discussion with QKD. Bob must read a sequence of polarized photons transmitted by Alice using a series of filters over a fiber-optic connection, which he must measure using two distinct types of filters. Consider that this secret key is a single-direction stream of photons, with each photon particle encoding a single data bit (either a 1 or 0).

However, these photons are oscillating (vibrating) in some way in addition to their linear trip. The photon's polarization refers to the angle at which it vibrates. Now, let's add a polarizer to the solution. A polarizer is just a filter that permits some photons to travel through in the oscillation state which is similar to before while permitting other photons to travel through a different oscillation state (it can also entirely block some photons, but that's a topic for another time). Alice is equipped with a polarizer that allows her to send photons in any of the four states: Horizontal, backward-facing diagonal, Vertical, and

Fig. 1 Bloch sphere representation of a Qubit



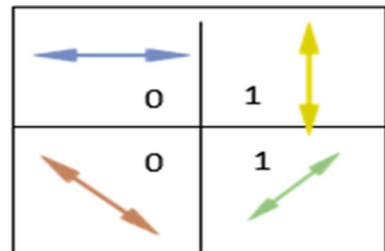
forward-facing diagonal. A diagonal spin that is vertical and facing backward represents the bit containing the state "1," whereas a diagonal spin that is horizontal and facing forward represents the bit containing the state "0." A diagonal filter can only read diagonal spin that is facing forward or backward, whereas a rectilinear filter can only read horizontal and vertical spin. Alice alternates her polarization scheme between diagonal and rectilinear filters at random for every single photon bit transmission. The broadcast can use one of the two polarizations to denote a single bit in any system she uses, either 0 or 1 (Fig. 2).

Bob must select whether to read each photon bit using his rectilinear or diagonal polarizer when he receives the photon key: sometimes the correct polarizer will be chosen by Bob, and at other times he will choose the incorrect one. Each polarizer is chosen at random by him, just like Alice. Bob would receive an inaccurate measurement if he had used the incorrect filter for a certain photon. Alice and Bob have established an unsafe communication channel at this stage, which means that others can listen in. After that, Alice tells Bob about the polarizer she used to transmit each photon bit, but not the way she polarized them. E.g., assume that Alice informs Bob that the photon number 6597 was transmitted using the rectilinear technique, but won't specify whether she sent a horizontal or a vertical photon. Bob then double-checks that he used the correct polarizer to receive each photon. The photon readings that he checked with the incorrect polarizer are subsequently discarded by Alice and Bob. Alice would phone Bob once the photon transaction occurred and inform him which series of filters, she used to achieve the original polarization. After removing the photons for which the improper filter was used by Bob, the remaining sequence of ones and zeros is used to encrypt their conversation (Fig. 3).

2.3 Eavesdropping

Assume we have an eavesdropper, Eve, who is trying to listen in on their conversation. Eve has the same polarizers as Bob, and for each photon, she must pick between rectilinear and diagonal polarizers at random. However, she has the same difficulty as Bob that is, she chooses the wrong polarizer half of the time. Bob, on the other hand, has the advantage of being able to validate which polarizer type was used for each photon by communicating with Alice. Eve's measurement will be rendered useless if she uses the wrong filter most of the time and misinterprets part of the photons that will generate the secret key. Suppose Eve was eavesdropping on their chat, she won't be able to figure out the secret key since she only knows the filters used by Alice and not the polarization states used. To obtain the key correctly, she'd need to know the filters which were used by Alice and Bob before sending the photons [9]. They must use the procedures outlined above to identify Eve's attack, which will result in a key sequence of 1 s and 0 s that is identical and in case someone has been eavesdropping, there will be some variations.

Fig. 2 Polarization States



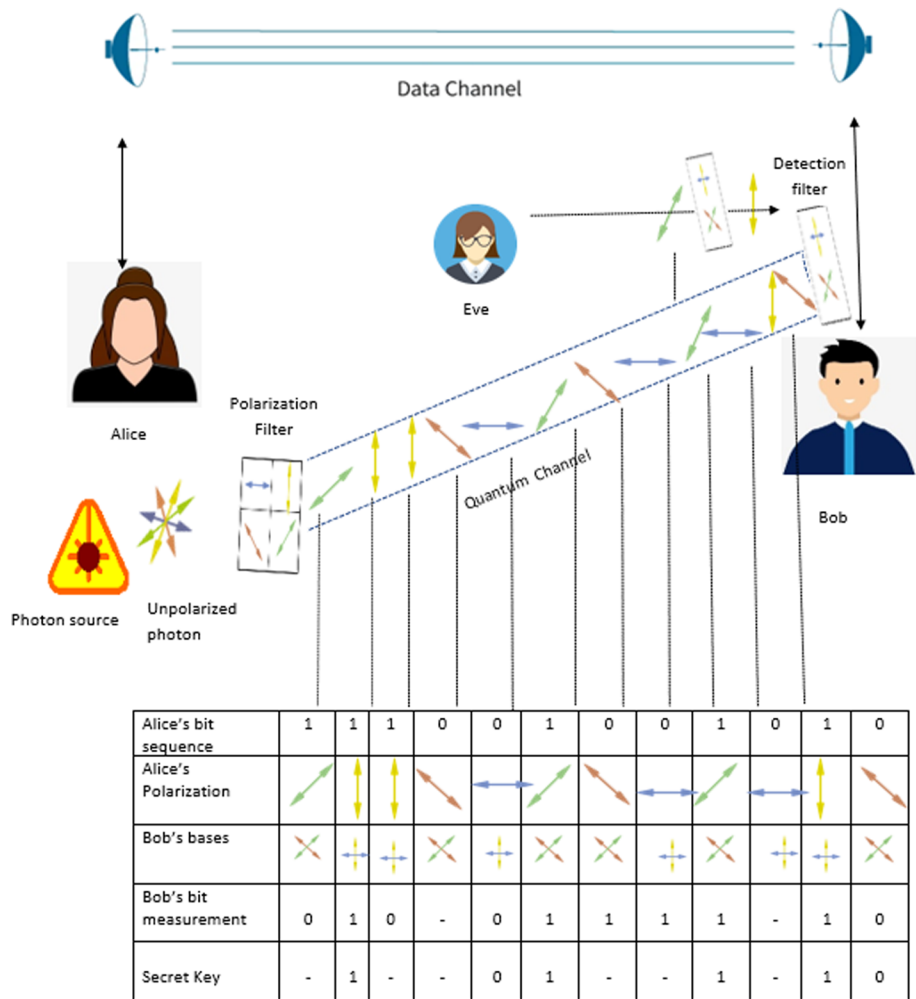


Fig. 3 Working process of the BB84 protocol

Then, they must next take additional steps to ensure that their secret key is valid. It is unnecessary to compare all of the binary digits of the final key via the insecure route explained above. Eve has to go through her filter sequence to read the spin of the photon which Alice passed through the line. If she uses the incorrect filter for a particular photon, the spin of that photon will change. As a result, as soon as Alice tells Bob the filter sequence she used, both of them will be aware that their key has been hacked because their bit sequences do not match. Bob would then receive a new key that has not been compromised from Alice, which he could use to read the message. Assume the final key is 2000 binary digits long. What Alice and Bob need to do is pick a part of these digits at random, say 100 digits, in terms of both digit state and digit state (0 or 1). If Alice and Bob's answers are identical, Eve probably wasn't listening.

2.4 Key Refinement

Alice and Bob converse while exchanging quantum keys via both the public/classical channel and the quantum channel. Quantum mechanics is used to coding the information in the quantum channel states. Alice and Bob send data while monitoring the open channel to see if Eve is listening. There are other parties to blame for the quantum channel issues besides Eve. Quantum channel disruptions, optical defects, and other factors can all lead to errors in quantum communication. In detectors, there may be a misalignment or noise. In today’s QKD systems, mistakes account for only a small percentage of all bits. This is in stark contrast to the Bit Error Rate (BER) in normal communication networks, which is typically about 10^{-9} . The number of errors in QC is measured by the Quantum Bit Error Rate (QBER), which is calculated by dividing the number of erroneous bits by the total number of bits shown in Eq. (2).

$$QBER = \frac{\text{Number of errors}}{\text{Total number of bits}} * 100\% \tag{2}$$

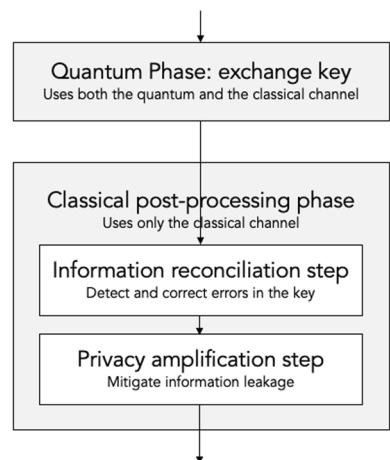
Alice and Bob must calculate QBER and establish whether or not an eavesdropper exists due to errors. In reality, they only compare a small fraction of the raw key dispersed over the classical channel to calculate the QBER. Eve has eavesdropped when the QBER exceeds a specific threshold. Alice and Bob will continue to distill the key if the mistake rate is low enough. They must, of course, remove the raw key’s compared component. Following the bit error estimation, Alice and Bob use key distillation procedures. There are usually 2 parts to these protocols: key reconciliation and privacy amplification [10]. Figure 4 shows steps in key refinement.

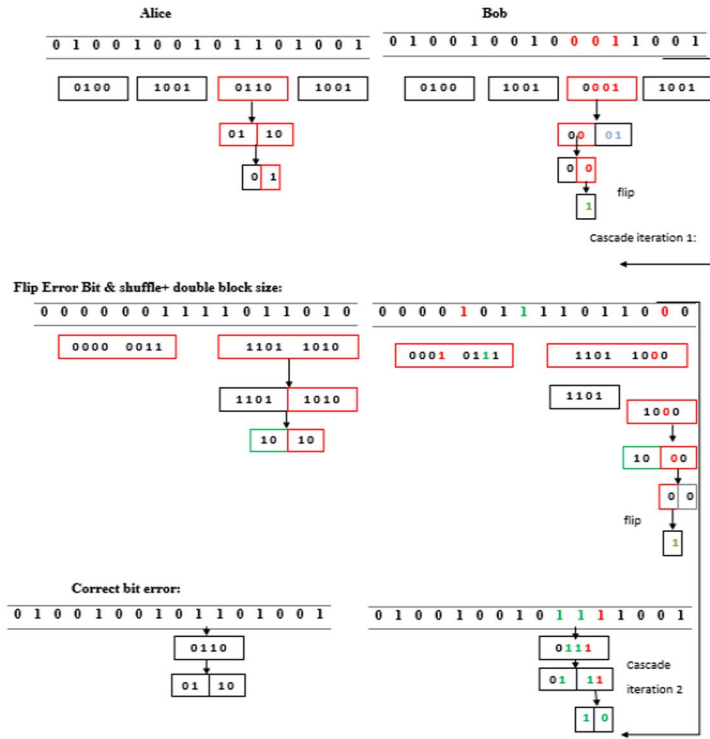
2.4.1 Key Reconciliation

The reconciliation phase’s purpose is to remove any errors (natural or manufactured by an eavesdropper) so that Bob and Alice can share the same key. Figure 5 shows Error Correction using Cascade Protocol.

This can be done using the traditional channel, which means that an eavesdropper could learn something from this channel if they listen to it. To limit the knowledge of prospective

Fig. 4 Steps in key refinement





Alice's and Bob's key after error correction:

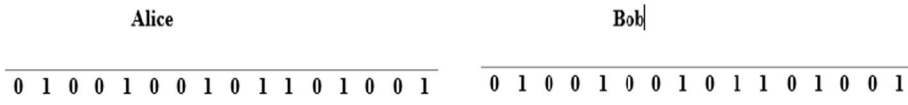


Fig. 5 Error correction using cascade protocol

eavesdroppers, privacy amplification will play a role. The topic of reconciliation and privacy amplification is discussed in Experimental Quantum Cryptography. The idea is to do parity checks on the sifted key blocks. Alice and Bob can choose a random permutation of the key ahead of time. They then divided the sifted key into blocks based on the length of the sifted key and an estimate of the mistake rate, expecting zero or one error in each block. If the blocks are too large, the errors may not be detected appropriately, and if the blocks are too small, too much information will be leaked. If there are an even number of 1 s in a bit string, the parity is 0, and if there are an odd number of 1 s in the string, the parity is 1. The flip of the parity is the result of a one-bit flip on the string. If there are an even number of errors in a string shared by Alice and Bob, they will have the same parity. If there are an odd number of errors, on the other hand, they will have different parity.

They can then detect an error by comparing the parities if the blocks are split correctly, with zero or one fault in each block (if the parities are the same, there is no error and if the parities are different there is one error). If there are two faults in a block, they will have the same parities and the user will believe there is no issue. We must keep in

mind that revealing the parity of blocks reveals some information. Alice and Bob agree to erase the last bit of the block to reduce information leaking. It will remove a zero with a probability $\frac{1}{2}$ and a one with probability $\frac{1}{2}$ if the bits are random. As a result, it will keep the parity unchanged with probability $\frac{1}{2}$ and flip it with probability $\frac{1}{2}$, making the parity random once more. As a result, Alice and Bob filtered the key into blocks and checked the parity. If the parity is different, they believe there is only one error and conduct a binary search to find it. In 1994, BRASSARD and SALVAIL presented the cascade protocol, which had an optimal and a little less optimal algorithm that was significantly more practical in practice.

The CASCADE protocol [11] accepts a noisy key and an estimated error rate as input and outputs a reconciled key as well as some information that was leaked over the public channel. Iterations are used in the protocol. Bob shuffles the key at the start of each cycle except the first. The public channel can be used to announce the shuffle. The key is then divided into equal blocks b by Bob. The error rate Q and the pass i determine the number of blocks k (i, Q). Top blocks are the name for these blocks. Bob then computes the parity for each top block and requests the correct parities from Alice. He checks the correct and present parities, then applies the BINARY primitive to each block with varying parities. All top blocks will have the right parity after using the BINARY primitive. The cascade effect is then used by Bob to fix bits from the preceding iterations.

2.4.2 Privacy Amplification

After the completion of the key distillation phase, finish the privacy amplification step [12]. Because Eve may have obtained critical data about the secret key, Alice and Bob must enhance their secrecy (to prevent eavesdropping during bit error estimation in the quantum channel and key reconciliation in the public channel). They can disassemble some parts and precisely reassemble the final key. The secret key that can be utilized for symmetric encryption will be less if Alice and Bob accomplish all of the aforementioned steps. All quantum key distribution protocols provide this key shortening capability. Assume that the key size from the QC is K and the key size after estimating the error is C and the key size after reconciliation is R and the final key size is B .

$$K > C > R > B \quad (3)$$

The QKD's performance diminishes as the key gets shorter with each level. When we want to guarantee a high level of security, this reduction is significant.

2.5 QKD Features

Quantum key distribution (QKD) presents a potential alternative for a quantum-proof cryptography solution and has fundamentally secure security that has been demonstrated. The QKD technique enables two different devices to agree upon a shared sequence of random bits, thereby greatly reducing the possibility of others (eavesdroppers) being able to determine the values. The following are the desirable characteristics of QKD, including its resistance to traffic analysis, location independence, robustness, rapid key delivery, and confidentiality.

2.5.1 Key Confidentiality

The secrecy of QKD is a major factor in its appeal. For public key systems, the theoretical intractability of decryption continues to be a challenge. Because of this, key agreement primitives like Diffie-Hellman, which are frequently used in today's Internet security architecture, could one day be broken, which would not only hinder communication in the future but could even reveal communications from the past. Traditional secret key systems have worried about insider threats and the practical difficulty of disseminating keying material. Automatic key distribution using QKD techniques may be more secure than those of its competitors if properly integrated into a larger security system. [13].

2.5.2 Authentication

Authentication is not provided by QKD on its own. Two contemporary methods for providing authentication in quantum systems are positioning the secret keys at device pairs earlier for use in hash function-based authentication or a hybrid of public key-QKD schemes. But both of the approaches are not particularly appealing. On the other hand, hybrid public key-QKD methods determine how vulnerable public key systems are to being broken by quantum computers or unexpected mathematical breakthroughs.

2.5.3 Robustness

The Quantum key distribution community has not historically taken robustness into account. An attacker who has mastered the art of cunning must not be able to run out of keying material accidentally. QKD has so far offered an extremely brittle service because QKD technologies have only been implicitly used via a single point-to-point link. If the link was broken due to a fiber cut or eavesdropping, all of the keying material would stop flowing. We believe that a meshed QKD network is much stronger than a single point-to-point link as it contains several important distribution pathways.

2.5.4 Traffic Analysis Resistance

Opponents may be able to take on the valuable analysis of traffic on a QKD system, such as finding a huge flow of keying material among 2 locations indicating that a high volume of secret data is passed, or will pass, among them. As a result, it is advantageous to obstruct such kind of analysis. QKD has a relatively feeble approach in this field because most configurations require dedicated, pt-to-pt QKD links among communicative objects that set out the underlying key distribution relationships.

2.5.5 Fast Key Delivery

The secret keys must be transmitted quickly to the encryption devices to ensure that you do not run out of key bits. Data encryption and decryption rates compete with the rate

of installing keying material. It is both desirable and feasible to considerably improve upon the current QKD technology's rates.

2.5.6 Distance- and Location-Independence

In an idyllic world, any object can agree on keying material with other (authorized) objects in the world. Surprisingly, the security design of the Internet allows for this – any machine connected to the Internet can generate a secure communication with another, agreeing on keys using the Internet IPsec protocols. This characteristic is glaringly absent in Quantum key distribution, which needs a clear and unimpeded path for photons to go between the two objects and it can work only for a few kilometers over optical fiber.

2.6 Challenges in QKD

In QKD, relays are necessary [14]. Unless the sender and destination construct a conduit that goes directly between their offices and the distance is low enough that the messages do not deteriorate—roughly 60 miles or fewer with present technology—hackers will have plenty of opportunities. When communications travel great distances, QKD networks will require repeaters, which could cause information to be hacked and the key stolen." Quantum cryptography, despite the protection it provides, has a few flaws. One of the major problems in quantum cryptography's its ability to provide security. Interference is the reason for the short length of quantum cryptography capacity.

3 Comparison of Quantum Cryptography Protocols

The QKD protocol is a mechanism for generating a secret key based on the principles of digital and photon measurements and based on the law of physics. To illustrate the reliability of QKD protocols [15], several protocols were established. Some QKD techniques can be processed in an acceptable amount of time and have proven to be resistant to quantum attacks. Furthermore, QKD protocols can be implemented using an existing security system. These QKD protocols were created in a variety of ways, and some of them required specific hardware. The next section provides a quick overview of various intriguing QKD techniques (Table 1).

4 Other Methods for Secret Key Exchange

The quantum key distribution (QKD) is a perfect illustration of the value of quantum effects in the creation of provably secure techniques for exchanging secret keys in cryptography. A lot of work is being done to increase QKD's security and effectiveness. Some of those techniques are briefly explained in this section.

4.1 Quantum One Time Pad

The encryption of the qubit using a one-time pad [16] is shown here. E.g., Alice sends a quantum bit $|\psi\rangle$ to bob using the key K. And Eve is the intruder between Alice and Bob

Table 1 Comparison of quantum cryptography protocols

Protocols	Quantum principles	States count	Polarization	Man in the middle attack	Dos attack
BB84	Heisenberg uncertainty	4	2 orthogonal	Vulnerable	Vulnerable
BB92	Heisenberg uncertainty	2	1 non-orthogonal	Robust	Vulnerable
SAR04	Heisenberg uncertainty	4	Coded bits	Robust	Vulnerable
COW	Quantum entanglement	Time slots	Using DPS	Robust	Vulnerable
KMB09	Heisenberg uncertainty	2	No	Robust	Vulnerable
EPR	Quantum entanglement	3	No	Robust	Vulnerable
DPS	Quantum entanglement	4	4 non-orthogonal	Robust	Robust
S13	Heisenberg uncertainty	4	2 orthogonal	N/A	N/A
SSP	Heisenberg uncertainty	6	–	–	–
E91	Quantum entanglement	3	–	–	–
S09	Public private key	–	–	–	–
OTP	Quantum entanglement	–	–	–	–
AK15	Heisenberg uncertainty	n	2 orthogonal	Robust	N/A

who tries to listen to their communication but cannot learn anything about $|\psi\rangle$. Alice performs some changes on $|\psi\rangle$ based on K and then sends the message to bob. Eve does not know about the key k but sees a state. Bob uses a decryption function to the state P and obtains the state $|\psi\rangle$ based on the key K . Consider the classical bit m as a quantum state in Eq. (4)

$$|e\rangle = Y^K |m\rangle \tag{4}$$

where Y is the bit flip operation. Bob uses the decryption function to obtain the message which is given in Eq. (5)

$$|m\rangle = Y^K |e\rangle \tag{5}$$

Sender	M: 0 1 0 0 1 0 0 1	Receiver	C: 1 1 0 1 0 0 0 0
	K: 1 0 0 1 1 0 0 1		K: 1 0 0 1 1 0 0 1
	1 1 0 1 0 0 0 0		0 1 0 0 1 0 0 1

Since Eve does not know anything about the key K . The probability of $k = 1$ is $\frac{1}{2}$ and $k = 0$ is $\frac{1}{2}$.

$$P = \frac{1}{2} |m\rangle\langle m| + \frac{1}{2} |m\rangle\langle m| Y \tag{6}$$

Considering the standard bases, we obtain the maximum mixed state as,

$$P = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{7}$$

The maximum mixed state is independent of m , so eve cannot obtain anything about m .

4.2 Entanglement-Based QKD

To demonstrate how entanglement [17] is utilized to generate a safe distribution of keys, consider some properties of a polarization-entangled photon pair. A single photon’s polarization state is given in Eq. (8)

$$|\psi\rangle = y|\uparrow\rangle + z|\leftrightarrow\rangle \tag{8}$$

where $y|\uparrow\rangle + z|\leftrightarrow\rangle$ denote rectilinear polarization states constituting a set of orthogonal bases. The normalization condition is $\alpha\alpha^* + \beta\beta^* = 1$ where α and β are complex numbers. A pure state is thought to characterize a photon’s polarization, with a definite phase relationship between the 2 basic components. The mixed state of a nonpolarized photon, on the other hand, can only be defined as a numerical mixture of base states. A superposition of four base states can also be used to define the most general polarization state (pure state) of a photon pair is given in Eq. (9).

$$|\psi\rangle = \alpha_1|\uparrow\rangle_1|\uparrow\rangle_2 + \alpha_2|\uparrow\rangle_1|\leftrightarrow\rangle_2 + \alpha_3|\leftrightarrow\rangle_1|\uparrow\rangle_2 + \alpha_4|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2. \tag{9}$$

When $\alpha_1 = \alpha_4 = \frac{1}{\sqrt{2}}, \alpha_2 = \alpha_3 = 0$, the entangled Einstein, Podolsky and Rosen photon pair is given in Eq. (10)

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2) \tag{10}$$

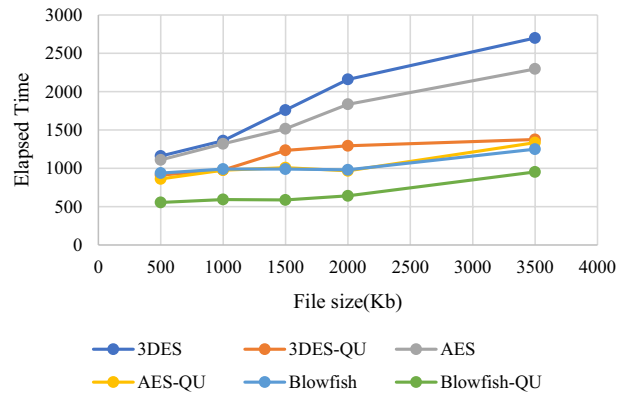
Assume we deliver one of an Einstein, Podolsky and Rosen pair’s photons to Alice and the other to Bob. With the same likelihood, Alice will detect a horizontal or vertical polarized photon if she reads her photon using the rectilinear basis. Bob’s photon will be projected to the appropriate polarisation state in accordance with the measurement result from Alice. Bob’s measurement will be entirely interrelated with Alice’s if bob reads his photon on the same bases as Alice. On the other hand, there is no correlation when Bob measures on a diagonal basis. The following rationale still holds true if Bob completes his measurement first. Between Alice and Bob, the EPR source can be put. Each EPR pair sends one photon to Alice and the other to Bob. Alice and Bob choose rectilinear or diagonal measurement bases for each incoming photon at random and independently. When they’ve finished, only the photon pairs that Alice and Bob have measured will be kept when they compare their measurement bases.

With matching bases, random bits are created. The BB84 protocol, which uses a single photon source, is similar. To generate the final safe key, they can do error repair and privacy amplification. Note that the polarization of each photon is unknown before Alice and Bob do the measurement. Each photon in the Einstein, Podolsky and Rosen pair is in a maximally mixed state, to be more specific (fully non-polarized). Because no information is encoded in the photon as it transmits from the source of the EPR to the user, the eavesdropper cannot obtain any information from it. During the measurement process, random bits are created (Fig. 6).

5 Results and Discussion

The BB84 Protocol was implemented using the Python programming language since it offers the freedom to select the necessary modules for the creation of the code and simulation of the protocol. To implement the code, support packages such as pool, random, and

Fig. 6 Elapsed time for classical cryptography algorithms with and without QKD



certain system packages were needed. This study compares the performance of three of the most used algorithms, including 3DES, AES, and Blowfish, using varied processing settings to examine different data file sizes ranging from 500 to 3500 KB. The techniques with and without QKD are evaluated in terms of decryption/encryption time, Avalanche effect, and throughput.

- Throughput* The encryption and decryption times of the files are used to calculate throughput.
- Encryption Time* The time it takes to use the secret key to convert plaintext to ciphertext. The time it takes to encrypt a message is measured in milliseconds and is dependent on the size of the key and the size of the text.
- Decryption Time* The time it took to use the secret key to convert the encrypted text to plain text. The time it takes to decrypt a message is measured in milliseconds.
- Avalanche Effect* Change one bit in the key or one bit in the plaintext and examine how the output of at least half of the bits in the cipher text changes. Table 2 shows the Elapsed time for classical cryptography algorithms with and without QKD for file sizes ranging from 500 to 3500 Kb.

Figures 7, 8 compares the performance of several classical and quantum cryptography algorithms in terms of encryption and decryption time for files ranging in size from 500 to 3500 kb. It shows that when combined with QKD, it outperforms the classical cryptography algorithms without QKD for file size = 3500 Kb.

Figure 9 compares the performance of several quantum and classical cryptography algorithms in terms of throughput for files ranging in size from 500 to 3500 kb. It shows that when combined with QKD (Fig. 9), the throughput performs well for Blowfish when compared with other classical cryptography algorithms.

Figure 10 comparative analysis of several classical and quantum cryptography algorithms in terms of Avalanche effect by changing 1 bit of the plain text for files ranging in size from 500 to 3500 kb. It shows that when combined with QKD, it outperforms the classical cryptography algorithms without QKD.

The graphical representation of the QuTip with a different platform for execution time is shown in Fig. 11. The Execution time is evaluated against the file size and the file size is varied from 100 Kb to 3500 Kb. When the file is 100 Kb the execution time of QuTip is

Fig. 7 Comparison of Encryption Time

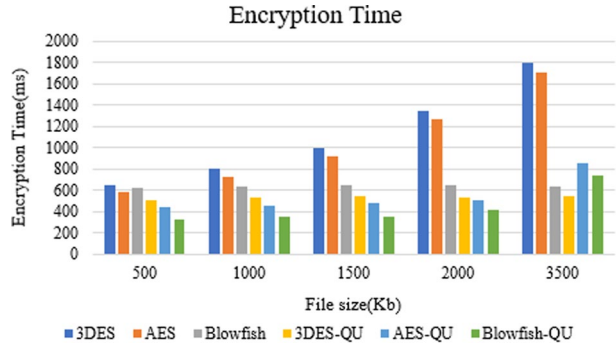


Fig. 8 Comparison of Decryption Time

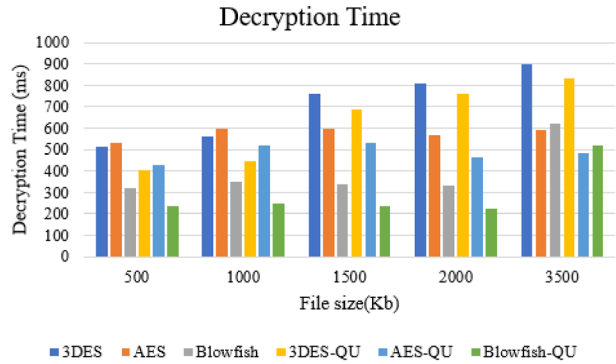


Table 2 Elapsed time comparison of quantum key integrated cryptography algorithms

Techniques	500	1500	2500
3DES	1160	1760	2700
3DES-QU	912	1234	1376
AES	1110	1516	2296
AES-QU	862	1008	1335
Blowfish	938	990	1250
Blowfish-QU	555	587	953

Fig. 9 Comparison of throughput with and without QKD

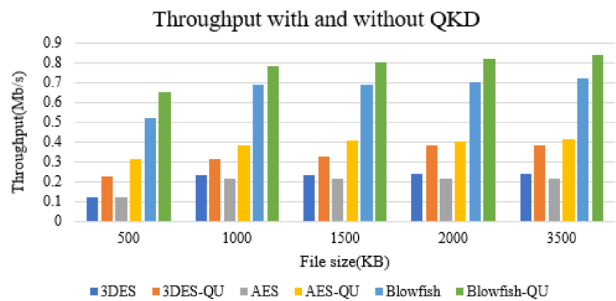
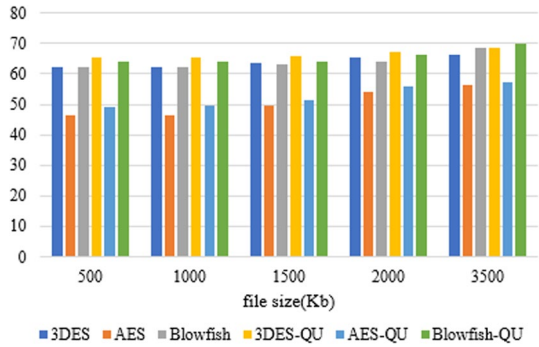


Fig.10 Comparative analysis of several classical and quantum cryptography algorithms



110 (ms) which is very less compared to the other platforms. When the file is increased the execution time also increased.

The chance of an eavesdropper being identified in a channel with 10% noise is shown in Fig. 11. When the number of transmitted photons approaches 90, the risk of the eavesdropper being detected is high. The bigger the number of transmitted data, regardless of whether there is noise interference or not, the more likely the eavesdropper will be found (Fig. 12).

6 Conclusion

This paper discusses Quantum Cryptography and how quantum cryptography is more efficient when compared with conventional cryptography algorithms and shows when QKD is integrated with classical cryptography algorithms it increases the security in transmitting data to a high level. From the results, it can be seen that QKD with classical cryptography decreases the encryption and decryption time and increases the throughput for file sizes ranging from 500 to 3500 Kb. The chance of detecting eavesdroppers in quantum cryptography is high compared to conventional cryptography algorithms.

Acknowledgements The author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding No Financial support.

Fig. 11 Comparative analysis of different platforms

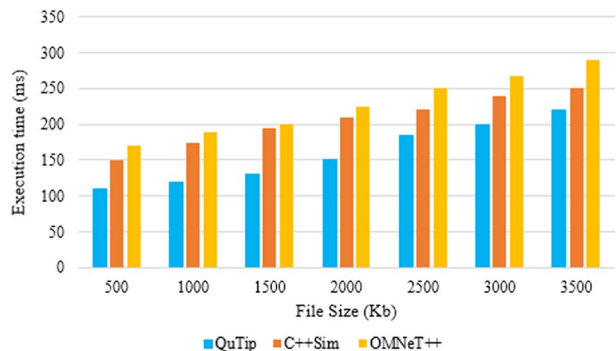
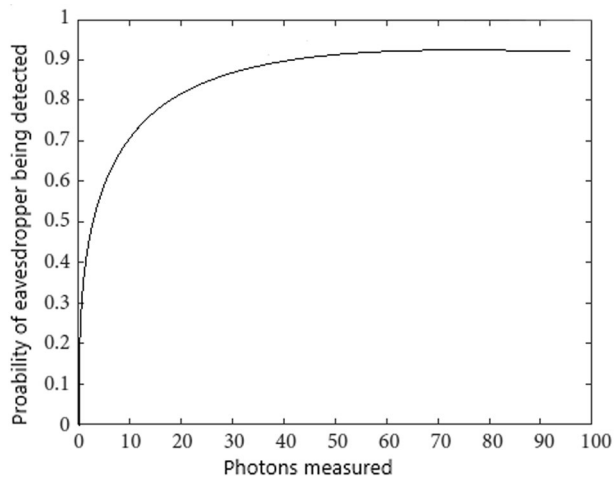


Fig. 12 QKD protocol with 10% noise



Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest This paper has no conflict of interest for publishing.

References

1. Paterson, K. G., Piper, F., & Schack, R. (2004). *Why quantum cryptography?* (No. quant-ph/0406147).
2. Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, 94(2), 025008.
3. Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16, 1–11.
4. Rao, S. (2015). Performance analysis of DES and triple DES. *International Journal of Computer Applications*, 130(14), 30–24.
5. Alabaichi, A., Ahmad, F. & Mahmood, R. (2013). Security analysis of blowfish algorithm. In *2013 second international conference on informatics and applications (ICIA)*. pp. 12–18. IEEE.
6. Chakrabarti, S., & Babu, G.S. (2020). Quantum key distribution: A safer alternate to asymmetric key exchange policies. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(3), 3910–3915.
7. Aumasson, J. P. (2017). The impact of quantum computing on cryptography. *Computer Fraud and Security*, 2017(6), 8–11.
8. Brass, D., Erdélyi, G., Meyer, T., Riege, T., & Rothe, J. (2007). Quantum cryptography: A survey. *ACM Computing Surveys (CSUR)*, 39(2), 6-es. <https://doi.org/10.1145/1242471.1242474>
9. da Silva, T. F., Xavier, G. B., Temporão, G. P., & von der Weid, J. P. (2012). Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems. *Optics express*, 20(17), 18911–18924.
10. Li, D., Huang, P., Zhou, Y., Li, Y., & Zeng, G. (2018). Memory-saving implementation of high-speed privacy amplification algorithm for continuous-variable quantum key distribution. *IEEE Photonics Journal*, 10(5), 1–12.
11. Bhandari, R. (2014). Quantum error correcting codes and the security proof of the bb84 protocol. arXiv preprint [arXiv:1409.1452](https://arxiv.org/abs/1409.1452).
12. Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2), 025002.

13. Elliott, C., Pearson, D., & Troxel, G. (2003). Quantum cryptography in practice. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. pp. 227–238, <https://doi.org/10.1145/863955.863982>.
14. Teja, V., Banerjee, P., Sharma, N.N., & Mittal, R.K. (2007). Quantum cryptography: state-of-art, challenges and future perspectives. In *2007 7th IEEE conference on nanotechnology (IEEE NANO)*. pp. 1296–1301. IEEE, <https://doi.org/10.1109/NANO.2007.4601420>.
15. Moizuddin, M., Winston, J., & Qayyum, M. (2017). A comprehensive survey: quantum cryptography. In *2017 2nd international conference on anti-cyber crimes (ICACC)*. pp. 98–102. IEEE, <https://doi.org/10.1109/Anti-Cybercrime.2017.7905271>.
16. Kute, S. S., & Desai, C. G. (2017). Quantum cryptography: A review. *Indian Journal of Science and Technology*, 10(3), 1–5.
17. Qi, B., Qian, L., & Lo, H.K. (2010). A brief introduction of quantum cryptography for engineers. arXiv preprint [arXiv:1002.1237](https://arxiv.org/abs/1002.1237).
18. Lakshmi, P.S., & Murali, G. (2017). Comparison of classical and quantum cryptography using QKD simulator. In *2017 International conference on energy, communication, data analytics and soft computing (ICECDS)*. pp. 3543–3547. IEEE.
19. Krämer, J. (2019). Post-quantum cryptography and its application to the IoT. *Informatik Spektrum*, 42(5), 343–344.
20. Semmouni, M.C., Nitaj, A., & Belkasmı, M. (2019). Bitcoin security with post quantum cryptography. In *International conference on networked systems*. pp. 281–288. Springer, Cham.
21. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4), 1012–1236.
22. Sharma, G. and Kalra, S. (2016). A novel scheme for data security in cloud computing using quantum cryptography. In *Proceedings of the international conference on advances in information communication technology and computing* pp. 1–6.
23. Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018). Quantum cryptography for the future internet and the security analysis. *Security and Communication Networks*, 2018, 1–7.
24. Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. *IEEE Access*, 8, 142413–142422.
25. Babber, K. and Singh, J.P., (2021). Quantum cryptography and security analysis. *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1–12.
26. Jassem, Y.H., & Abdullah, A.A. (2020). Enhancement of quantum key distribution protocol for data security in cloud environment. *ICIC International*, 11(3), 279–288.
27. Marco, L., Andrew, S., Romain, A., Christopher, C., Degiovanni, I. P., Gramegna, M., ... & Zhiliang, Y. (2018). Implementation Security of Quantum Cryptography-Introduction, challenges, solutions ETSI White Paper No. 27.
28. Thayananthan, V., & Albeshri, A. (2015). Big data security issues based on quantum cryptography and privacy with authentication for mobile data center. *Procedia Computer Science*, 50, 149–156.
29. Bhatt, A. P., & Sharma, A. (2019). Quantum cryptography for internet of things security. *Journal of Electronic Science and Technology*, 17(3), 213–220.
30. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a quantum world. *IEEE Communications Magazine*, 55(2), 116–120.
31. Gabriel, A. J., Alese, B. K., Adetunmbi, A. O., & Adewale, O. S. (2015). Post-quantum cryptography based security framework for cloud computing. *J. Internet Technol. Secur. Trans. (JITST)*, 4(1), 351–357.
32. Qiu, L., Sun, X., & Xu, J. (2018). Categorical quantum cryptography for access control in cloud computing. *Soft computing*, 22(19), 6363–6370.
33. Verma, P., & Lohiya, R. (2015). A comprehensive survey on: Quantum cryptography. *International Journal of Science and Research*, 4(4), 2214–2219.
34. Dasari, V.R., Sadlier, R.J., Geerhart III, B.E. and Humble, T.S. (2018). Demonstration of provably secure quantum key distribution (QKD). In *Disruptive technologies in information sciences*, vol. 10652, pp. 65–71. SPIE.
35. Murugan, G. (2020). An efficient algorithm on quantum computing with quantum key distribution for secure communication. *International Journal of Communications*, 5, 12–23.
36. Shi, R. H., Liu, B., & Zhang, M. (2021). Verifiable quantum key exchange with authentication. *International Journal of Theoretical Physics*, 60(1), 227–242.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



A. Ahilan received Ph.D. from Anna University, India, and working as an Associate Professor in the Department of Electronics and Communication Engineering at PSN College of Engineering and Technology, India. His area of interest includes FPGA prototyping, Computer vision, the Internet of Things, Cloud Computing in Medical, biometrics, and automation applications. Served Guest editor in several journals of Elsevier, Bentham, IGI publishers. Also, have contributed original research articles in IEEE Transactions, SCI, SCIE, and Scopus indexed peer-review journals. He presented various international conference events like ASQED (Malaysia), ESREF(France). He is doing as a reviewer in IEEE Industrial Informatics, IEEE Access, Measurement, Multimedia Tools & Applications, Computer Networks, Medical systems, Computer & Electrical Engineering, neural computing and applications, Cluster Computing, IET Image Processing, and so on. He has IEEE and ISTE membership. He has worked as a Research Consultant at TCS, Bangalore, where he has guided many computer vision projects and Bluetooth Low Energy projects. Meanwhile, special Guest

lectures, Practical workshops, Hands-on programming in MATLAB, Verilog, and python at various technical institutions around India.



A. Jeyam received a Bachelor's degree in Computer Science and engineering from Lord Jeggannath college of engineering, Anna University, India in 2010. He also received his Master's in the year 2014 in Computer science and Engineering from Government college of Technology, Coimbatore, Anna University, India. He had participated AICTE sponsored National workshop and TEQIP sponsored workshops based on the research field. Also presented a Conference paper on Recent advances in computer vision and information technology. He is now working in Nuclear power corporation of India Limited.