AN EFFICIENT ALGORITHM FOR QUANTUM COMPUTING WITH QUANTUM KEY DISTRIBUTION WITH SECURE COMMUNICATION

SATHIYA KUMAR C.1,*, PRIYA V.2, SRIRAM V. P.3, SANKAR GANESH K.4, MURUGAN G.5, DEVI MANI6, SUDHAKAR S.7

1Department of Computational Intelligence, Vellore Institute of Technology, Vellore
2Department of CSE, Mahendra Institute of Technology, Namakkal
3Acharya Bangalore B-School, Bengaluru
4School of Management and Commerce, DMI St. John the Baptist University, Malawi, Central Africa
5Department of Computer Engineering, Vidyalankar Institute of Technology, Wadala (East), Mumbai
6Department of Computer Science, King Khalid University, Sarat Abedha Campus, College of Science and Arts, Kingdom of Saudi Arabia
7Research Supervisor, Anna University, Chennai
*Corresponding Author: csathiakumar@yahoo.com

Abstract

The key formation is a crucial primitive for constructing secure networks: in a multi-party setting, it permits two parties using public authenticated communication to create a secret session key, which used to encrypt messages. QKD is an innovative technology that exploits the laws of quantum mechanics to generate and distribute unconditionally secure shared key for use in cryptographic applications. Currently, many symmetric key cryptographic tools, which are known to be quantum-safe. They all share secret symmetric keys, through untrusted communication, which finished with public-key systems, which are prone to quantum attacks. One of the recommended solutions to the key distribution problem is Quantum Key Distribution (QKD). QKD can be used to generate secret keys that are secure against any future algorithmic/computational improvements. QKD utilizes an authenticated communication channel along with a quantum communication channel so that a secret key generated. Whatever may be the protocol to implement proposed QKD, they all need both a quantum channel and an authenticated classical OTP (One Time Pad) is a randomly generated key. Therefore, this key length is equal to the message. The proposed QKD result is 35.67% smaller keys for quantum security. The performance of a QKD system against a modeled photon number splitting attack analyzed in simulation results and standard key agreement protocols can be secure.

Keywords: Cryptography, One-time pad, Quantum channel, Quantum key distribution, Secret key.
1. Introduction

Cryptography, which called "secret writing," safeguards the communication data, which is highly sensitive. If not for cryptography, no message is private, and anyone can access any message. A process called encryption is involved in transforming the messages from "plaintext" into highly secret "ciphertext," which are, in turn, converted to plaintext by decryption. Cryptography—the oldest writing style was called secret-key cryptography during olden days as it shared one secret key amid the communicating parties. Here, both encryption and decryption used. It is evident that the possession of the same secret key by both parties is very crucial, that explains the fact that secret-key cryptography was in use thousands of years ago with the advent of technology, the technique modified to suit the developments.

Quantum Cryptography (QC), being very recent, is still in the development stage. However, the challenges brought to the prevailing cyberspace and its safety cannot remain unnoticed by the work. The quantum algorithm, which forms the basis of QC, was proposed in 1994 by mathematician Shor. Here, the polynomial-time very efficiently solves the integer factorization problem and the discrete logarithm problem. We cannot ignore the fact that we are yet to find the classical algorithm with which the significant integer decomposition and the discrete logarithm problem can be solved effectively in the Turing machine model. Here comes the role of quantum computers in aid of the traditional cryptosystems.

Cryptography and network security are the two eyes of the information security that are assured by Heisenberg’s uncertainty principle and quantum no-cloning theory. The study’s objective has been to analyse the QC and design cryptographic algorithms and protocols, in contrast to quantum computing attacks. In this paper, the prime focus lies in the study and analysis of the QKD properties, which is the focus for future cyberspace security. As said earlier, quantum cryptographic protocols and their in-depth report is the prime focus of cyberspace security issues for the future internet.

The need for the hour is a highly safe and secure channel to communicate and to fulfil this need proposing a secure communication scheme to encrypt messages at a high rate. Its focus is to facilitate speedy encryption investigating the purpose of QC in attaining quantum security on the internet. The Diffie-Hellman key exchange currently used in the quantum world broken as the quantum computers can breach the asymmetric cryptography that does not exist. It cannot apply to cut the authenticity of key exchanges protected by Digital Signature (DS). Here focus on DS confidentiality of the QKD's key exchange system. It used an arbitrated DS and not the directed DS for avoiding the refusal that the sender did not send a message or pretending the sender's key has stolen/lost or a forged signature. This work recommends the OTP operation for avoiding any fall in the probability of the channel eavesdropping. It requires an extension of the key exchange secure from attackers to implement the QKD cryptosystem on the internet.

QKD also has specific cons, the most important one is its large public key size, and hence, it is not in use. This algorithm proposed to perform both the encryption and decryption processes using QKD [1]. Apart from this, here introduced the new quantum gates, which are analysed and studied during cryptographic methods. A couple of complementary steps offered to alleviate the difficulties faced by QKD with large public keys. The first step includes the analysis of the quantity Grover’s algorithm can speed up existing attacks on QKD and what parameters of QKD can
An Efficient Algorithm for Quantum Computing with Quantum Key . . . . .79

This paper organized as follows. Section 2 provides background information on the QKD cryptosystems. The definitions of the key generation, encryption, and decryption methods review what codes are suitable for QKD and give an overview of existing attacks against QKD. In Section 3, analyses the impact of quantum computing on existing attacks against QKD to optimize parameters by using quantum security. Section 4 explains how QKD implemented on the internet and how a key caching mechanism used to minimize network handshake time. In Section 5, evaluate the solution by benchmarking the quantum-secure network against the conventional system. Finally, in Section 6 is providing Conclusions and recommendations.

2. Related Works

Quantum Cryptography is a term coined from quantum money, a concept put forth by Wiesner in 1969. Lack of technology and other means had limited the publication of this new and innovative idea until 1983. It was Bennett and Brassard, in 2011, who first proposed the practical QKD protocol. The implementation finished using single-photon polarization. In later days, many efforts have put into improving security and efficiency by enhancing QKD. Ekert suggested a bells theorem based protocol in 1991 where pair of quantum bits (qubits) was employed, in the following year, an improvised version proposed by Bennett. He employed any two non-orthogonal states resulting in a more comfortable and better enhancement [4]. The coming years saw many successive QKD protocols using the basic principles of quantum mechanics.

The oblivious transfer protocol, which is also a significant but necessary cryptographic procedure, considered a vital technology for protecting cryptographic privacy. Here, though the sender sends much potential information to the receiver, he is unaware of the content specifics. Shen et al. [5] mentioned that the Quantum Oblivious Transfer (QOT) that has many works to its credit was first put forward by Crepeau; Mayers and Salvail demonstrated the “oblivious transfer” security against any specific measurement spared by quantum mechanics. This protocol proved in 1998, which the protection of the QOT protocol acts as an eavesdropper. Quantum Authentication (QA) protocol belonging to the quantum cryptographic protocols as proposed in 2001. Post this, many QA protocols have recommended with numerous branches. Apart from these (i.e., QKD/QOT/QA protocol), QC protocols also include Quantum Bit Commitment (QBC) and Quantum Signature (QS) [6] protocols.
3. Impact of Security in Quantum Computing for Computer Internet

3.1. Quantum computing

Bits are the fundamental units of computing, and a single bit is storing a binary digit value (0/1). Quantum computing has a superposition of two states where the primary unit is holding 0/1’s importance in the same period. Such bits are called as qubits and need to select or “collapse into” while measuring its state. Strangely, if a string of qubits of similar lengths prepared similarly, the resulting bit string is not always the same. It provides an upper hand to the quantum computers over traditional computers as they can accomplish better with fast parallel computations.

To have a secure electronic communication, need cryptography, which plays a vital role by ensuring authenticity amid parties and messages exchanged [7]. The safety and security of communication are at stake due to quantum computing. It achieved by predicting secret cryptographic keys, which is not possible by an ordinary computer. A quantum computer [8] can break any cryptographic keys enabling an eavesdropper to eavesdrop private communications and pretend to be someone else. That does not mean that a quantum computer can break all types of cryptographic keys. Presently many cryptographic algorithms cannot be reached. Below explains the various kinds of cryptography that are safe from multiple attacks. It is the need of the hour to have secure cyberspace as it is the compilation of all data and very essential for human survival. With so many threats, QC has become the first option for cyberspace. The following Fig. 1 represented the classic cryptosystem.

![Fig. 1. Model of a conventional cryptosystem.](image)

3.2. Unconditional security

Instant internet communication completed through cable and light. This communication system model presented in Fig. 2. Assume A and Bas legitimate users in the system and attacker. For the sake of security, both the parties encrypt and exchange messages on a public channel. The symmetric key cryptosystems and asymmetric key cryptosystems are the two types of cryptosystems, and their security depends on the complexity of computing. Still, the latest hardware and advanced algorithms [9] have brought in extraordinary developments in the protection of cryptosystems. Besides, the increasing growth and popularity, quantum computing has solved numerous problems in classical mathematics in the field of quantum physics. Hence, researching and studying quantum cryptographic protocols is going to be an essential part of cyberspace security issues in the future.
Sniffing detection

Figure 3 indicates an exchange of data/messages between Alice and Bob in the public channel. To maintain a security message is encrypted. Even then, this does not assure protection from an attacker eavesdropping on the circuit. Also, just based on features like whether cable or optical fiber used, one cannot spot an eavesdropper. In the former medium, the listener can use a multi-meter to monitor while in the later, the eavesdropper received data from any part of a light signal. It observed that the fiber loss based on many environmental aspects like temperature and pressure, which make the loss caused by eavesdropping not be perceived. In the case of quantum communication, the eavesdropper detected because of quantum no-cloning theory.

When you look at Fig. 4, it clearly explains that when an eavesdropper keeps an eye on the quantum channel, a bit of quantum information helps the same measuring base with the sender with a 56% probability. Hence, able to detect the eavesdropper at a 56% probability for a bit of quantum information. It observed that, for the quantum information of bit, the likelihood of the eavesdropper detected is $1 - \left(\frac{1}{2}\right)^n$.

3.3. Quantum key distribution (QKD)

Symmetric key cryptographic tools are quantum-safe. They all share secret keys via an untrusted communication, which is usually done by public-key systems that are prone to attacks. Here comes the need to secure and safely release keys between distant parties, without depending on vulnerable algorithms. Chapuran et al. [10] commented that QKD is one of the proposed solutions to key distribution issues [11]. QKD offers individual security by the laws of physics; besides, it is a safe method for secure key establishment against arbitrary attacks like quantum attacks.
Hence, the attacker, in spite of having computational inputs such as traditional and quantum computing inputs, is stopped by QKD, which provides particular security. QKD is also tough to advanced cryptanalysis or in quantum computing. The following Fig. 4 spectacles the quantum key distribution.

3.3.1. Unique security properties of QKD

Various features of QKD followed for security, they are:

- An anonymous quantum change is measured as implied by the Heisenberg uncertainty principle.
- As per the no replicating theorem, it is physically not possible to create an exact copy of an anonymous state.
- There is the presence of quantum entanglement properties placing necessary restrictions on the data revealed to unauthorized third parties.

3.3.2. Security of QKD

In this subsection, for the sake of simulating real situations in the future internet, firstly analyse the quantum key distribution protocol in a noise-free channel. Further, search the quantum key distribution protocol in a noisy channel.

The security of QKD protocol, the encoding of quantum information, and the measurement results under various measurement bases specified in Table 1. Both the parties settle in advance that the horizontal and oblique downwards polarization represents "1," while the vertical and diagonal upward polarization represents "0."

<table>
<thead>
<tr>
<th>Output bases</th>
<th>Division</th>
<th>XOR</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>↔</td>
<td>1</td>
<td>0.50%; 1.50%</td>
<td></td>
</tr>
<tr>
<td>↑</td>
<td>0</td>
<td>0.50%; 1.50%</td>
<td></td>
</tr>
<tr>
<td>↗</td>
<td>0.50%; 1.50%</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>↘</td>
<td>0.50%; 1.50%</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Measurement of QKD.
4. Proposed Methodology for Quantum Key Generation

The steps to generate quantum key generation:

- The parameters \( n, k, d, a \) random selection of linear code \( C \) of length \( n \), rank \( k \), and minimum distance \( d \).
- Create an \((n-k) \times n\) parity check with the matrix of \( H \).
- Choose \((n-k) \times (n-k)\), binary matrix \( S \times n \) Permutation \( P \) matrix. The public key is \( H_{pub} = SHP \), with correctable errors \( t = \lfloor d-1/2 \rfloor \). The private key is \((S, P)\). Here \( C \) is encoding algorithm.

\( S \) not selected randomly, but a standard form is forming \( SHP \). Moreover, \( P \) assumed to be the identity matrix, as the binary goppa code-based cryptosystem chooses a random \( P \) matrix [12], it becomes equivalent to using a uniformly random support-vector.

Encryption for quantum key generation

A public key \( H_{pub} = SHP \) and the correctable errors \( t \), and an encoded message as an error vector \( e \in Fn \) of weight \( t \) calculate the syndrome of \( E \): \( c = H_{pub} e^T \).

Decryption for quantum key generation

The steps for decrypting the quantum key generation:

- A ciphertext \( c \) and a private key, (i.e., \( S: S^{-1}c = HP e^T \)).
- Decode \( HPe^T \) to \( Pe^T \).
- The decoded error vector \( Pe^T \) to obtain (i.e., \( P^{-1}Pe^T = e^T \)).
- Typically, \( e \) decoded to the original message \( m \).

This cryptosystem is exclusively high for significant message transfers as it quickly generates random error vector of any given weight. Implementation of QKD for important transmissions, creating an error vector while encrypting the code. A key-derivation function, a shared secret, is conventional from the error vector, and the sequence of key exchange indicated the following Fig. 5.

![QKD System](image)

Fig. 5. Quantum key exchange an authenticated channel.
4.1. The procedure of quantum key distribution

OKD utilizes a whole communication network along with a quantum communication channel so that a secret key generated. Whatever may be the protocol to implement QKD [13], they all need both a quantum medium and an authenticated traditional. The quantum channel uses optical fibers links for sending photons (quantum states of light) with A and B, while the conventional channel is an authenticated telephone line that A and B use to communicate with each other. Strangely, both the medium is public. It is presented by the quantum channel [14] regarding A and B and an eavesdropper listening. QKD protocols can broadcast the traditional channel publicly with no compromise in security. A QKD process start as A decides to share some Cryptographic keys to B. To create a quantum channel, both A and B require the specialized optical equipment. For sending a photon stream sequentially, Alice uses a light source, where each photon treated as an information bit. While sending photon one-by-one, they are randomly chosen by her for preparing them in one of two “bases.” The basis is a view from which a photon measured in the following Fig. 6.

![Fig. 6. Typical prepare/measurement of QKD.](image)

Protocol functions as the below method:

- \( A \rightarrow \) data with \( k_1 \); sends to \( B \) data.
- \( B \rightarrow \) data with \( k_2 \); sends to a trusted party.
- \( B \rightarrow A \) data with shared key \( k_3 \). \( B \rightarrow A \).
- \( B \rightarrow \) shared key \( k_3 \); \( A \rightarrow k_1 \). \( A \rightarrow B \) with key \( k_2 \) to a trusted party.
- \( A \rightarrow B \) with \( k_2 \).

4.2. Mathematical model of QKD

Data \( \psi \rightarrow \) qubits encrypted with the key that has scaled with measurement operation. The algorithm (1) as follows: \( \psi_i \rightarrow QB_i \otimes K_i \).

\[
\begin{align*}
\text{for } i & = 1 \text{ to } 4 \\
Q \_ K(i) = & \text{kron}(M \_ \text{op} \_ KA)
\end{align*}
\]

where the \( Q \_ A \) is A’s four qubits, and \( M \_ \text{op} \_ KA \) is the measurement operator is a private key of \( A \). Pauli-Y gate is Eq. (1):
\begin{equation}
Y = \begin{cases}
0 & -i \\
i & 0
\end{cases}
\end{equation}

It is the revocable and unitary gate and used for cryptographic processes. $H$ matrix, as follows in Eq. (2):

\begin{equation}
H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
\end{equation}

In the case of the $H$, an array is crucial in the network as it finds the shift from one to another basis. There are three inputs and outputs in the Fredkin gate, namely, the control $i/p$ set at 0. With respective $o/p$ is always the same followed by the 2nd $o/p$ and the same as the $i/p$ and at last, the 3rd $o/p$ is the same as the $i/p$. If the control bit set to 1, then the $o/p$ is reverse. The Fredkin gate [15] is as follows (4):

\begin{align*}
0, x, y &\rightarrow 0, y, x, \\
1, y &\rightarrow 0, y, x.
\end{align*}

### 4.3. Definition of one-time pad

It was Gilbert Vernam, who patented OTP in 1919, and hence, it is sometimes called “Vernam’s cipher.” However, an earlier version of OTP by banker Frank Miller in 1882 recently discovered in Figs. 7 and 8.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{OTP_system.png}
\caption{One time pad (OTP) system.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{OTP_key_gen.png}
\caption{Key generation for encryption and decryption.}
\end{figure}

OTP keys, PT/CT, which are all $\lambda$-bit, i.e., basics of $(0, 1, \lambda)$. The choice of $\lambda$ (length of PT, CT, keys). The OTP is as in Fig. 9:

\textbf{KeyGen:} \quad \text{Eny}(k, m, (0, 1)) \quad \text{Dey}(k, c, (0, 1)).

\text{key} \leftarrow (0, 1, \lambda) \text{ return } k \oplus m \quad \text{return } k \oplus c.

\text{key} \leftarrow (0, 1, \lambda) \text{ means to sample } k \text{ uniformly from the set of $\lambda$-bit strings. The definition of OTP mandates that the key.}
Security in OTP

The eavesdropper does not learn about “m”; eavesdropper algorithm as follows:

Assessment \((m(0 \& 1))\):

\[ k \leftarrow (0 \& 1)^i; \]
\[ c := k \oplus m \]
\[ \text{return } c \]

4.4. Proposed algorithm for QKD by using OTP

Here recommend novel secret key sharing schemes, i.e., sender/receiver, to encrypt information and pass it through an effective quantum medium [16, 17].

4.4.1. Traditional communication process

Steps involved in the communication process:

- Sender A \(\rightarrow\) Receiver B, \((PU_x/IDA/trusted party)\). Encryption message: sender \(PR_x\) and the trusted first \(PU_x\).
- The trusted party decrypts the request message with \(PU_x\).
- Trust authority resends the message with its signature.
- A&B’s ID received by the Trust Authority, which sends with the same secret key.
- The sender and the receiver share the same secret key as a 0,1.
- The decryption process reversed in the encryption process.

4.4.2. Quantum channel steps

The steps involved in quantum channel:

- Binary secret key function \(\phi = \text{bin2vec(bin)}\).
- Pretty printed function, psi used to represent the superposition state.
- The unitary matrix \(UM = UF(f, m, n)\).
- HM is \(H = H(n)\).
- \(Psi\) is measure; \((H*U_f*H*psi)\) with psi = measure (psi).
4.5. Encryption process by using OTP

Based on studies by Sengan and Pandian [18] and Balaji et al. [19], the first group of the OTP are always used as a key indicator at the opening of the message. It is mandatory to not use the first group of the pad in the encryption process and always avoid sending an OTP along with the message as it discloses the messages sent and also the order in which they sent. The example shows the usage of the OTP key and the PT message. Moreover, it indicated in Table 2.

The message is as follows (refer to Fig. 10):

```
402 402 402
67486 35589 25626 670 98157
42872 11212 04769 61582
```

![Fig. 10. Key generation in the encryption process.](image)

Table 2. Encryption process.

<table>
<thead>
<tr>
<th>Original message</th>
<th>S</th>
<th>A</th>
<th>R</th>
<th>T</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>83</td>
<td>72</td>
<td>67</td>
<td>82</td>
<td>80</td>
</tr>
<tr>
<td>Binary</td>
<td>101010011</td>
<td>01001011</td>
<td>01000011</td>
<td>01011010</td>
<td>01010011</td>
</tr>
<tr>
<td>Prime</td>
<td>00011101</td>
<td>11111101</td>
<td>00011101</td>
<td>00010001</td>
<td>00011011</td>
</tr>
<tr>
<td>1st result</td>
<td>01110111</td>
<td>00011101</td>
<td>01011110</td>
<td>01101001</td>
<td>01101110</td>
</tr>
<tr>
<td>2’s complement</td>
<td>10010111</td>
<td>10010001</td>
<td>10100100</td>
<td>10011001</td>
<td>10010000</td>
</tr>
<tr>
<td>Decimal</td>
<td>145</td>
<td>156</td>
<td>166</td>
<td>157</td>
<td>156</td>
</tr>
<tr>
<td>Decimal subtract with ASCII</td>
<td>144-83</td>
<td>155-72</td>
<td>162-65</td>
<td>145-82</td>
<td>147-80</td>
</tr>
<tr>
<td>Cipher text</td>
<td>62</td>
<td>82</td>
<td>98</td>
<td>61</td>
<td>64</td>
</tr>
</tbody>
</table>

4.6. Decryption process by using OTP

The first group is checked against the first group of OTP to ensure that the proper OTP used. Point to be noted in this first group does not belong to the original message and a key indicator. The OTP digits are written below the CT, followed by the adding of CT and OTP simultaneously, digit by digit, from left to right, and by % 10. It means addition without carrying and showed in Table 3.

Once decryption completed, plain code digits, which are the outcome of the process, are converted back into plaintext using the checkerboard. When the first set of digits is 1 to 6 representing a single digit, easily distinguish them format the double-digit values. (refer to Fig. 11).
5. Results and Discussion

The successive quantum cryptographic device offers validation for the secured message over quantum and the public medium. A shared secret key between two parties sharing the data is used by the classical cryptography mechanism for bringing an authentication safeguarding the superposition of states and quantum states from all types of attacks like an alteration. According to this implementation in a simulator with QCF library (refer to Tables 4 and 5), safe and secure communication between the sender and receiver through the quantum medium. Proposed protocol the interface secured from attacks. It is achievable due to the secret key encrypted through quantum to enhance not just the security [20, 21]. A three-stage protocol is used for parties to share the initial values. Communications as follows:

$$A \rightarrow T : PU_A \parallel ID_A \parallel ID_B$$  \hspace{1cm} (3)

$$T \rightarrow A : E_{PR}[ID_A \parallel PR_A \parallel PU_T \parallel T] \parallel E_{PR}[ID_B \parallel PR_B \parallel PU_T \parallel T]$$  \hspace{1cm} (4)

$$T \rightarrow B : E_{PR}[ID_A \parallel PR_A \parallel PU_T \parallel T] \parallel E_{PR}[ID_B \parallel PR_B \parallel PU_T \parallel T] \parallel E_{PU}[E_{PR}[K \parallel T]]$$  \hspace{1cm} (5)

$$A : D[ID_A \parallel PU_A \parallel PR_T \parallel T]$$  \hspace{1cm} (6)

Matrix $A$: unitary if:

$$A^{-1} = A^*$$  \hspace{1cm} (7)
The eavesdroppers being detected in a noiseless channel explained in Fig. 12. As the transmission number crosses 40, the eavesdropper presence is almost 98.97%. Whereas, in Fig. 12, the chance of detecting eavesdropper is possible with 30.45% noise, with the transmitted photons around 70. These two figures and findings prove successful detection of the eavesdropping actions in a quantum medium. Precisely findings explain that more transmission data lead to higher chances of eavesdropping irrespective of noise interference. The error when the receiver receives the message with eavesdropping happening well explained in Fig.
The findings show 24.465% error rate of the receiver with no eavesdropper, 30.18% with 45.56% chances of eavesdropper monitoring the channel and 29.89% when the eavesdropper observes the channel.

The detection of eavesdropper while eavesdropping on the channel at various probabilities is shown in Fig. 14. In the graph, the purple line shows 100% chances of attacker monitoring the channel, the green line representing 51.15% and the red line 22.23%, respectively. The below curves explain the eavesdrop monitoring the channel and detected is nearly 100% as the number of transmitted bits is rising. Figure 15, the simulation results and discussion concludes that the QC provides absolute security along with sniffing detection properties for safe and secure communication and ensuring secure cyberspace in the future.

Fig. 12. Number of quantum states measured by attacks.

Fig. 13. Quantum key distributions with 36.66% noise.
6. Conclusions

A new version of QC has been put forth in this paper to enhance the quantum encryption using the quantum as well as classical cryptography. Here also used the quantum gates during the implementation as believing they would aide in elevating the security of classical and quantum computing. A shared secret key required between two right parties over a long distance, and this offered by OTP having a considerable benefit of complete security, which is essential in cryptography. Incorporating the OTP system where the private key equally longer as their messages along with the secret messages, so it is communicated safely over any place. This work is a combination of various approaches, thereby increasing security. A new methodology using, which secure communication is taking place between two parties using OTPs. When compared with classical cryptography is the method has certain advantages like absolute security and sniffing detection, which can solve the severe cyberspace security issues in the future - the QC, which provides security for various applications: the Internet of Things and smart cities.
Nomenclature

\( n, k, d \) Random selection of linear code
\( k_1, k_2 \) Keys
\( M \) View
\( PU_A \) Sender public key
\( PR_A \) Sender private key
\( PU_T \) Third-party, public key
\( \Psi \) Pretty

Greek Symbols

\( \lambda \) Length of plaintext and ciphertext
\( \Psi \) Key measure
\( \otimes \) XOR

Abbreviations

OTP One Time Pad
QA Quantum Authentication
QBC Quantum Bit Commitment
QKD Quantum Key Distribution
QOT Quantum Oblivious Transfer
QS Quantum Signature
VQKD Variable Quantum Key Distribution

References


