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

G. Murugan*
Professor, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Wadala (East), Mumbai
**Corresponding author E-mail:gopalmurugan0@yahoo.com*

Abstract:-

Currently many symmetric key cryptographic tools which are known to be quantum-safe. They all share Secret symmetric keys through an untrusted medium which is usually done with public key methods which are prone to quantum attacks. One among the recommended solutions to the key distribution problem is Quantum Key Distribution (QKD). QKD utilizes an authenticated Communication channel along with a quantum communication channel so that a secret key is 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 used when two parties wish to communications have to share a key called pad. This pad is a randomly generated key and the length of the key should be equal to the message so it can be sent. The proposed QKD parameters that result in almost 35.67% smaller keys for quantum security and an implementation of QKD in network which is publicly available and usable in practice.

Keywords: Quantum Channel; Secret Key; Quantum Key Distribution; One Time Pad; Cryptography.

1. Introduction

Cryptography which is also called as *"secret writing"* safeguards the communication data which is highly sensitive. If not for cryptography, no message is private and any message can be accessed by anyone. 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– an 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 were used. It is obvious that the possession of 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 is modified to suit the developments.

Quantum cryptography being very recent is still in the development stage. But the challenges brought to the prevailing cyberspace and its safety cannot remain unnoticed by the work. The quantum algorithm which forms the basis of quantum cryptography 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 large 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 analyze the quantum cryptography 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 quantum key distribution (QKD) properties which is the focus for future cyberspace security. As said earlier, quantum cryptographic protocols and their in-depth analysis will be the prime focus of cyberspace security issues for future Internet.

The need of the hour is a highly safe and secure channel to communicate and to fulfill this need proposing a secure communication scheme to encrypt messages at high rate. It focus is to facilitate speedy encryption. The investigating the purpose of quantum cryptography in attaining quantum security in Internet. Diffie-Hellman key exchange is currently used in the quantum world is broken as the quantum computers have the capability to breach the current asymmetric cryptography that does not exist. Yet, they cannot be used to break authenticity of key exchanges protected by digital signatures. In this paper focus on digital signatures confidentiality of the QKD‟s key exchange system. It used an arbitrated digital signature and not the directed digital signature for avoiding the refusal that message was not sent by the sender or pretending the sender‟s key has been stolen or lost or a forged signature. This work recommends the onetime pad operation for avoiding any fall in probability of the channel eavesdropping. It requires an extension of the key exchange secure

from attackers in order to implement the QKD cryptosystem in Internet. QKD also has certain cons and the most important one is its large public key size and hence it is not in use. This algorithm is proposed to perform both the encryption and decryption processes using QKD [1]. Apart from this, here introduced the new quantum gates, which are analyzed and investigated during the encryption and decryption processes. A couple of complementary steps are 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 protect against these attacks. There are certain layers in this scheme; the Quantum Key Distribution (QKD) layer is launched on a Variable Quantum Key Distribution (VQKD) which is presented for secret keys distribution on an existing network link. There are three main parts in the secret key processing which are error correction, physical exchange, and privacy amplification. These provide parameters for quantum security that result in almost 35.67% smaller keys in par with the parameters currently recommended in literature. In the second step, a mechanism is introduced to lessen the network‟s handshake time in case of large QKD keys. Here the usability of this solution is demonstrated and evaluated by benchmarking [2] it against regular Internet. The stakeholders are new QKD parameters that result in almost 35.27% smaller keys for quantum security and an implementation of QKD in network which is publicly available and usable in practice [3].

This paper is 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 in order to optimize parameters by using quantum security. In Section 4, explains how QKD can be implemented in Internet and how a key caching mechanism can be used to minimize network handshake time. In Section 5, evaluate the solution by benchmarking the quantum-secure network against regular network. 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 till 1983.

It was Bennett and Brassard, in 2011, who first proposed the practical QKD protocol. The implementation was done using single photon polarization. In later days, many efforts have been put to improve security and efficiency by enhancing QKD. A Bells theorem based protocol was suggested by Ekert in 1991where pair of quantum bits *(qumbits)* (i.e., an EPR pair) was employed, in the following year, an improvised version was proposed by Bennett. He employed any two non-orthogonal states resulting in an easier and better enhancement. 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 basic cryptographic procedure is considered as vital technology for protecting cryptographic privacy. Here, though the sender sends much potential information to the receiver he is unaware of the content specifics. The Quantum Oblivious Transfer (QOT) that has many works to its credit was first put forward by Crépeau in 1994[5]; the *"oblivious transfer"* security against any specific measurement spared by quantum mechanics was demonstrated by Mayers and Salvail. This protocol was proved in 1998, which the security of the QOT protocol acts as an eavesdropper.

Quantum Authentication (QA) protocol belonging to the quantum cryptographic protocols was proposed in 2001. Post this, many QA protocols have been proposed with numerous branches. Apart from these (i.e., QKD/QOT/QA protocol), quantum cryptography protocols also include Quantum Bit Commitment (QBC) and Quantum Signature (QS) [6] protocols.

3. Quantum Computing

Bits are the fundamental units of computing and a single bit can store a binary digit with the value of 0/1. The quantum computing has a superposition of two states where the fundamental unit can hold both a 0 and a 1 value at the same time. Such bits are called as *qumbits* and need to select or *"collapse into"* while measuring its state. Strangely, if a string of *qumbits* of similar lengths were prepared in the same way; the resulting bit string is not always the same. This gives an upper hand to the quantum computers over traditional computers as they can accomplish better with very rapid parallel computations.

Currently using numerous physical systems with various implementations of quantum computers like nuclear spins, superconducting *qumbits*, traps, and optical cavity quantum electrodynamics. Every research and its outcomes has its own strength with

some being stronger compared to others for large-scale quantum computing.

3. 1 Impact of Cryptography and Security in quantum computing for Computer Internet

In order to have a secure electronic communication, need Cryptography which plays a very important role by ensuring authenticity amid parties and messages exchanged. The safety and security of communication is at stake due to Quantum computing. This is achieved by reverse calculating or guessing secret cryptographic keys, which is not possible by an ordinary computer. A quantum computer [8] has the ability to 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 there are many cryptographic algorithms that cannot be breached. Below explains the various types of cryptography that are safe from quantum attacks and also the ciphers, protocols and security systems which are most vulnerable. It is the need of the hour to have a secure cyberspace as it is the compilation of all data and very essential for human survival. With so many threats, quantum cryptography has becomes the first option for cyberspace. The following figure 1 is represented the classic cryptosystem

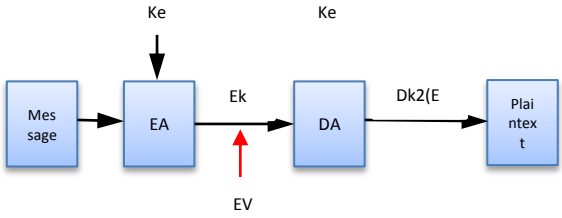


Figure 1. Model of Classic Cryptosystem

3.2. Unconditional Security

The present internet communication is done through cable and light. This communication system model is presented in Figure 2. Let us assume Alice and Bob as legitimate users in the system and Eve an eavesdropper. 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 the classical cryptosystem and their security depends on the complexity of computing. Still, latest hardware and advanced algorithms [9] have brought in extraordinary developments in the security 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 future.

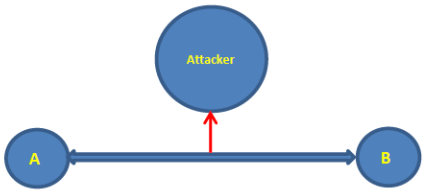


Figure 2 Classic communication model

Figure 2 Classic communication model

In the above example, sender (Aice) [10] is interested to share a common conference key with his/her Bob. This key would be used to encrypt/decrypt the messages they communicate. The QKD protocol used in this study, the real randomness of the key is assured by the essential properties of the quantum: uncertainty principle. Moreover, an attacker is definitely detected if it exists.

3.2.1 Sniffing Detection

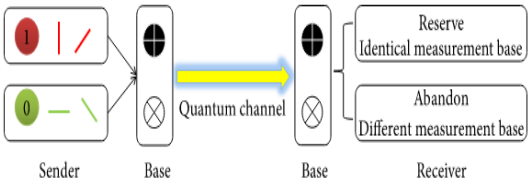


Figure 3 Illustrates the model of the famous QKD

In Figure 3 indications an exchange of data/message between Alice and Bob in public channel. To maintain secrecy, their message is encrypted. Even then, this does not assure protection from an attacker eavesdropping on the channel. Also, just based on the features like whether cable or optical fiber used, one cannot spot an eavesdropper. In the former medium, the listener can use a multi-meter/ oscilloscope to monitor while in the later the eavesdropper received data from any part of light signal. It is observed that the fiber loss is based on many environmental aspects like temperature and pressure, which make the loss caused by eavesdropping, not be perceived. In case of quantum communication, the eavesdropper will definitely get detected because of quantum no-cloning theory. When you look at Figure 4 it clearly explains that when an eavesdropper keeps an eye on the quantum channel, for 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 is observed that, for the quantum information of-bit, the probability of the eavesdropper being detected is. $1-(1/2)^n$.

3.3. Quantum Key Distribution (QKD)

There are many symmetric key cryptographic tools which are known to be quantum-safe. They all share Secret symmetric keys via an untrusted medium which is usually done with public key methods which are prone to quantum attacks. Here comes the need to secure and safely release symmetric Keys between distant parties, without depending on vulnerable Public key algorithms. Quantum Key Distribution (QKD) is one among the proposed solutions to the key distribution issues [11].

QKD offers assured security in accordance to the laws of physics also it is a safe method for secure key establishment against arbitrary attacks like quantum Attacks. This means, the attacker inspite of having unlimited computational resources such as unlimited classical and quantum computing resources is stopped by QKD which provides provable security. QKD is also tough to advanced cryptanalysis or in quantum computing. The following figure 4 spectacles the quantum key distribution.

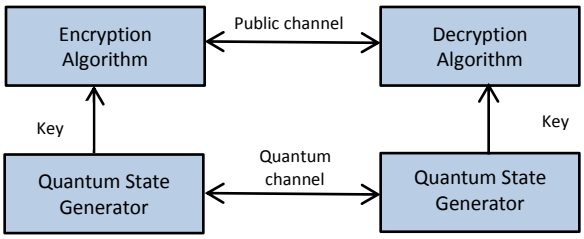


Figure 4. The Quantum Key Distribution (QKD)

Subsequently, a resource for secure distribution of secret keys is also offered by quantum key distribution that can be used with quantum Safe symmetric key algorithms like one–time pad encryption. Theoretically, QKD offers protection by encoding information in quantum states of light thereby following the fundamental laws in quantum Physics and quantum information theory.

3.3.1 The unique security properties of QKD

1. An anonymous quantum changes physically when measured as implied by the Heisenberg uncertainty principle. When it is applied for QKD, an eavesdropper studying the data stream will actually alter the values of certain Bits in a noticeable way.

2. As per the no cloning theorem it is physically not possible to create an exact copy of an unknown quantum state. This implies that there is no way for an adversary for copying a bit in the data stream just to quantify one of the copies hoping to hide their eavesdropping.

3. There is the presence of quantum entanglement properties placing basic restrictions on the data revealed to unofficial Third parties.

Fascinatingly, because of the quantum mechanics laws, it is highly difficult for an adversary to eavesdrop under cover on quantum key distribution. The information encoded in quantum states show real changes in the information that can be detected by the legitimate parties through various means. Just by having a look at the information getting transmitted will actually change the bits of information in the data stream and incorporate errors in such a manner that the sender and recipient can immediately recognize and measure .

Based on the amount of errors incorporated by the eavesdropper, enables the sender and receiver to confirm the presence of an eavesdropper but also the extent of information gained by the intruder using advanced technology and algorithms. This permits them to use well – analyzed, post – processing techniques to eliminate any data an eavesdropper might have obtained on the shared key.

The most vital feature of the quantum key distribution is, any attack should be done in real time. In contrast to the classical cryptographic schemes, there are no chances to protect the data for future decryption in QKD. This saves the meager chances of waging an attack against QKD; whereas the chances are high for conventional cryptography. QKD˝s composability is universally proven and it safely permits combination of the distributed Keys with other demonstrable secure schemes / Onetime pad encryption inspite of preserving quantifiable –and durable security.

3.3.2 Security of the QKD

In this subsection, for the sake of simulating real situations in the future Internet, firstly analyze the quantum key distribution protocol in noise-free channel. Further, search the quantum key distribution protocol in noisy channel. In order to study the security of QKD protocol, the encoding of quantum information and the measurement results under various measurement bases are specified in Table 1. Both the parties settle in advance that the horizontal and oblique downwards polarization represent “1” while the vertical and oblique upward polarization represents “0.”

Table 1. Measurement of QKD

Output	**Division**	
Bases	**XOR**	**XOR**
↔	1	0:50% ; 1:50%
↕	0	0:50%;1:50%
↗	0:50% ; 1:50%	0
↖	0:50%;1:50%	1

4. Proposed Methodology for Quantum Key Generation

1. Given security parameters *n, k, d, a random selection of* linear code *C* of length *n* rank *k* and minimum distance *d is done.* Such code is called a *[n,k,d]* code. An efficient decoding algorithm for *C* has to be known

2. Generate an $(n-k)\times n$ parity check matrix *H*.

3. Choose a random $(n-k)\times(n-k)$ invertible binary matrix *S* and a random $n \times n$ Permutation matrix *P*. The public key consists of the product $H_{pub} = SHP$, along with the number of correctable errors $t=\lfloor d-1/2 \rfloor$. The private key consists of (*S, P*) and the decoding algorithm of C.

Remark (Choos *S ,P*). S is not selected in a random manner but in a standard form forming SHP. Moreover, P assumed to be the identity matrix, as the binary Goppa code based Cryptosystem chooses a random permutation matrix, it becomes equivalent to using a uniformly random support vector. Permuting the elements of the support vector gives the same result as permuting the columns of the parity check matrix of a Goppa code. Assume this choice of S and P in the following.

a. Encryption for Quantum Key Generation

1) Given a public key $H_{pub} = SHP$ and the number of correctable errors *t*, and a message encoded as an error vector $e \in F^n{}_2$ of weight *t,* compute the syndrome of $E : c = H_{pub}\, e^T$.

b. Decryption for Quantum Key Generation

1) Given a ciphertext *c* and a private key, undo the multiplication by S: $S^{-1}\, c = HPe^T$.

2) Use the syndrome decoding algorithm to decode HPe^T to Pe^T .

3) Invert the permutation of the decoded error vector Pe^T to obtain the original error vector

$P^{-1}\, Pe^T = e^T$.

4) Typically, *e* will be decoded to the original message *m*.

This cryptosystem is exclusively great for important message transfers as it easily generates random error vector of any given weight. During the implementation of QKD for important transmissions, generating an error vector while encrypting the code. By applying a key-derivation function, a shared secret can be established from the error vector and sequence of key exchange is indicated the succeeding figure 5.

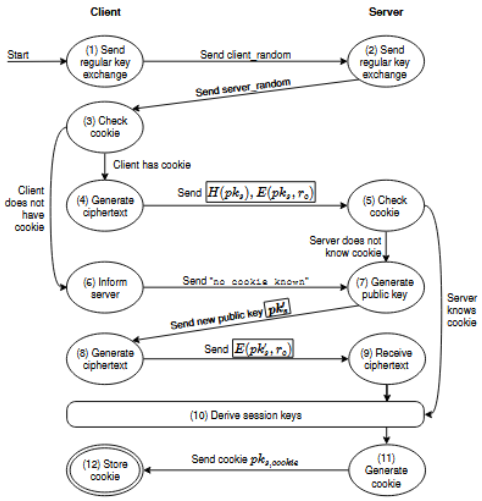


Figure 5. Quantum Key Exchange an authenticated channel

4.1. Procedure of Quantum Key Distribution

Quantum key distribution utilizes an genuine Communication network along with a quantum communication channel so that a secret key is generated. Whatever may be the protocol to implement QKD, they all need both a quantum channel (to send quantum States of light), and an authenticated classical. Optical fibers or free space/ satellite links are used by the quantum channel for sending photons (quantum states of light) between Alice and Bob, whilst the classical channel is a typical (authenticated) telephone line that Alice and Bob use to talk to each other. Strangely, both the channels can be public. It is essentially shown by the quantum channel regarding Alice and Bob and an eavesdropper listening in. Actually QKD protocols can broadcast the classical channel publicly with no compromise in security. Quantum Key Distribution process starts as Alice decides to share some Cryptographic keys to Bob. In order to create a quantum channel, both Alice and Bob require the specialized optical equipment and also an access to a classical channel to communicate with one another. For sending a photon stream sequentially, Alice uses a light source, where each and every photon can be 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‟‟. Basis is a view from which a photon is measured (Figure 6).

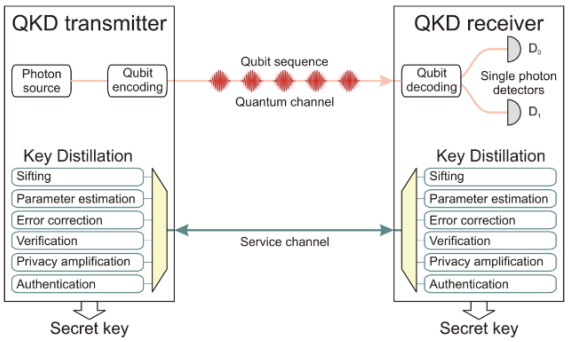


Figure 6. A Typical prepare/measurement of QKD

Bob is the recipient and it is essential for him to document the values for each photon he gets through the quantum channel. For this, he has to accept Alice, take measurements of each one, and has to choose one of the two possible „bases" and record the One he measured in. As previously discussed, these options are randomly made and do not need any details on the bases that Alice has chosen during transmission of every bit. Later, Alice and Bob communicate over the classical channel to find the better basis using which every individual bit was calculated at each end of the quantum channel. At times Alice and Bob may choose the same basis though randomly, and they receive the same photon value for these bits. When they calculate the photon using numerous bases, they discard this bit and ignore it in the final key. Once all the bits are sent and received, both the parties are able to speak openly on what basis they used to quantity every photon. This offers plenty of information to them for generating the Key from the received quantum states, even then cannot be sufficient for an adversary to reconstruct the key. Ultimately, an eavesdropper will not succeed in finding the transmitted key on a couple of grounds. Firstly, he cannot keep an eye the photon without changing them, hence getting found and having these Bits discarded by Alice and Bob. The second reason is, an indirect observation cannot be done by the adversary over the photon through the measurements of Alice and Bob either. Since Alice and Bob seldom reveal the final measurement result for each quantum state but only disclose which basis they used to measure it. By then, it becomes impossible for the eavesdropper to measure the Photons it has already been received by Bob. Hence, knowing that the basis Alice used is not useful. It is well-established Using Information theoretic proofs that the measurement Information is inadequate for an adversary to use to reconstruct the generated key.

4.1.1The introduced protocol works as follows:

a) A encrypts the data by |k1> and sends it to B

b) B encrypts his new data by |k2> and sends it to the third party.

c) B again concatenates his encrypted data with the data that has been received from A then encrypts all the data using the shared key |k3>. B sends it to A.

d) A decrypts the received data from B by the shared key |k3> and splits the concatenated data. Then A decrypts the data by |k1> to ensure that the data has not been altered. A sends B data (which was encrypted by |k2>) to the third party.

e) The third party decrypts the received data from A and B by |k2> to ensure that both data are identical and then informs both parties.

4.2. Mathematical Model of QKD

A data $|\psi>$(*qumbits*) is encrypted with the key that has been scaled with measurement operation. Before applying the gates, the following algorithm in (1) is used to prepare the tensor product,

$$|\psi_i> = |QB> \otimes |K_i>$$

Where the *Ki* is one of the three keys |k1>, |k2> and |k3> post the measurement process and QB is the Qubit data. The below given code is used to formulate the tensor product of A in step (a):

```
for i=1:4
        Tens_QA_KA(:,i)=kroon(M_op_K
A(:,i),Q_A(:,i);
end
```

Where the Q_A is A"s 4 *Qumbits* and M_op_KA is the measurement operator for A"s private key. Three gates (Pauli-Y gate, Hadamard gate, and Fredkin gate) are used sequentially in the proposed protocol. Pauli-Y gate is as indicated in (2):

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Pauli –Y gate is a revocable and unitary gate. It is employed in the encryption and decryption processes. The Hadamard matrix is represented as indicated in (3):

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

In case of the Hadmard matrix it is very crucial in quantum computing as it finds the shift from one basis to another basis. There are three inputs and outputs in Fredkin gate namely, the control input set at 0 and its respective output is always the same followed by the second output and the same as the input and at last the third output would be the same as the input. Besides, if the control bit set to one, then the output would be its reverse. The overall representation of Fredkin gate is as indicated in (4):

$|0,y,z\rangle \rightarrow |0,y,z\rangle and\ |1,z,y\rangle$

4.3. 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 was recently discovered Figure 7 shows a diagram of OTP. A scenario of this method is provided.

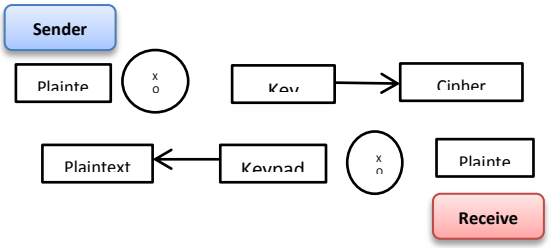
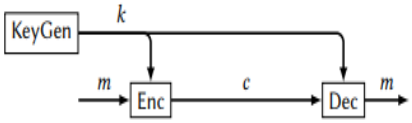


Figure 7 The One Time Pad (OTP)

OTP is used when two parties wish to communications have to share a key called pad. This pad is a randomly generated key and the length of the key should be equal to the message so it can be sent. OTP is for a sender and receiver to initially share a key *k* that was chosen according to a key-generation process to call *Key Generation*. When the sender wishes to securely send a message *m* to the receiver, she encrypts it using the encryption algorithm *Encryption* and the key *k*. The result of encryption is a ciphertext *c*, which is sent to the receiver. The receiver can then use the decryption algorithm *Decryption* with the same key *k* to recover the plaintext *m*.



OTP uses keys, plaintexts, and cipher texts which are all *λ-bit* strings (i.e., elements of $\{0,1\}^{\lambda}$). The choice of λ (length of plaintexts, ciphertext, and keys) is a public parameter of the scheme, meaning that it does not need to be kept secret. The specific KeyGen, Enc, and Dec algorithms for OTP are given below:

KeyGen: $k \leftarrow (0,1)^{\lambda}$ Eny(k,m,€$(0,1)^{\lambda}$) returnk⊗m Dey(k,c, ,€$(0,1)^{\lambda}$) returnk⊗c

Recall that *"$k \leftarrow \{0,1\}^{\lambda}$ "* means to sample k uniformly from the set of *λ-bit* strings. The definition of one-time pad mandates that the key should be chosen in exactly this way.

Example of Encrypting the following 20-bit plaintext m under the 20-bit key *k* using OTP results in the ciphertext *c* below:

1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 0 0 1 1 *(m)*
⊗0 0 0 1 1 0 0 1 1 1 0 0 0 0 1 1 1 1 0 1 *(k)*
---
1 1 1 1 0 1 1 0 0 1 1 1 1 1 0 1 1 1 1 0 *(c=Eny(k,m))*

Decrypting the following ciphertext *c* using the key *k* results in the plaintext *m* below:

0 0 0 0 1 0 0 1 0 1 1 1 1 0 0 1 0 0 0 0 *(c)*
⊗1 0 0 1 0 0 1 1 1 0 1 0 1 1 1 0 0 0 1 0 *(k)*
---
1 0 0 1 1 0 1 0 1 1 0 1 0 1 1 1 0 0 1 0*(m=Dey(k,c))*

4.3.1. Security in OTP

Suppose you encrypt a plaintext m and an eavesdropper eventually sees the resulting ciphertext."*The eavesdropper doesn't learn about m"* The quite precise about what exactly the eavesdropper sees in this situation-in fact, the eavesdropper gets an output of the following algorithm:

View $(m€(0,1)^{\lambda})$
$k \leftarrow (0,1)^{\lambda}$
$c:=k \oplus m$
return *c*

This algorithm describes how the sender computes the values using secret values (choosing a key k in a specific way, and using the one-time-pad encryption procedure). It also describes that the eavesdropper sees only the ciphertext (but not the key). This is a randomized algorithm, which you can see from the random choice of k. Even after fixing the input m, the output is not fixed. Instead of thinking of view (m) as a fixed value, will think of it as a probability distribution. So more precisely, can say that an eavesdropper sees a sample from the distribution view (m).

4.4 Proposed Algorithm for QKD by using OTP

This work recommends novel secret key sharing schemes between the sender and receiver to encrypt quantum information and pass it through an effective quantum channel. The proposed scenario is described below.

4.4.1 Classical Channel Steps

1. Sender (Alice), needs to communicate with receiver (Bob), and hence releases a request message with its public key PU_A and ID_A to a third party, (assuming it as a trust authority). The encryption of the requested message takes place with the help of the sender private key PR_A and the third party public key PU_T . This is then sent to trusted third party between Alice and Bob via a traditional channel as indicated in equations (1), (2), and (3).