International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

A Survey Paper On Different Encoding Techniques Based On Quantum Computing

Abbasali Antelawala[1], Hatim Chathiwala[2], Nihal Kaul[3], Rishabh Shukla[4]

[1,2,3,4] *KJ College of Engineering and Management Research, Pune, India*

Abstract - *Quantum computing is the branch of science that studies theoretical computation systems (Quantum computers) that make direct use of mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from binary digital electronic computers based on transistors. Whereas commonly used digital computing requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1). Quantum computation uses Quantum bits, which can be in superposition of states. Quantum key distribution (QKD) uses Quantum mechanics to guarantee secure communication. It enables two parties (Alice and Bob) to produce a shared random secure secret key known only to them, which can then be used to encrypt and decrypt messages. Quantum communication involves encoding information in Quantum states, or qubits, as opposed to classical communications & use of bits. Usually, photons are used for these Quantum states. Quantum key distribution exploits certain properties like superposition and entanglement principles of these Quantum states to ensure its security. Thus, encoding techniques can be used to generate a shared secret key which can then be used to transmit message securely and can prevent eavesdroppers at bay.*

Key Words: **Quantum Computing, QKD (Quantum Key Distribution), Bloch sphere, Cryptographic Protocols, Quantum Cryptography, No-Cloning theorem**

1. INTRODUCTION

1.1 Quantum Computing

Quantum Computing is the branch of science which deals with the design and development of computers based on the principles of Quantum Mechanics. The subject of physics studies elementary objects and simple systems & the study becomes more interesting when things are larger & more complicated. Quantum Computation & information based on the principles of Quantum Mechanics will provide tools to ll up the gulf between the small & the relatively complex systems in Physics.

Quantum Mechanics arose in the early 1920's when classical physics could not explain everything ever after adding ad-hoc hypothesis. The rules of Quantum Mechanics were simple but overlooked counter intuitive. Quantum means very small i.e. it deals with the elementary particles (atoms) in space.

1.2 Quantum Computer

We know that a bit (a_0 or a_1) is the fundamental concept of classical computation& information. Also a classical computer is built from an electronic circuit containing wires & logic gates. Similarly, in Quantum Computer's we have Quantum Bits (also known as qubit) & Quantum Circuits which are analogous to bits & circuits in classical computer. A Quantum Bit or simply a Qubit can be mathematically defined as,

$$|\psi> = \alpha|0> + \beta|1>$$

Two possible states for a qubit are the states |0> and |1>. The notation |1> is known as the Dirac notation. Unlike a classical bit, a qubit can be infinite numbers of states, other than |0> and |1>. It can be in a state $|\psi> = \alpha|0> + \beta|1>$, where α and β are complex numbers such that $\alpha^2 + \beta^2 = 1$. The 0 and 1 are called the computational basis states & |ψ> is called a superposition. We can call $|\psi> = \alpha|0> + \beta|1>$ as a Quantum state. The Quantum bits are suspended using coefficients like α, β, γ, σ, etc to denote the magnitude of energy required to spin the atom to appropriate position. The coefficients are probabilistic nature it means that the coefficient may represent different values at different instance of time. The coefficients are related with Quantum spins.

1.3. Quantum Spin

Let's have a look at the structure of 1 - qubit (1 - qubit = 2 states)

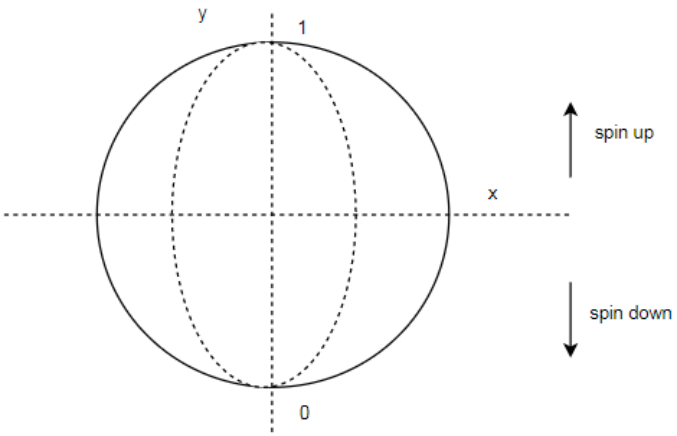


Figure 1 : 1-Qubit

In 1-qubit structure, the x-axis denotes horizontal polarization and y-axis denotes the vertical polarization. Spin up is the phenomena of spinning the position of the qubit upwards. Spin down is the phenomena of spinning the position of a qubit downwards. The spin up and Spin down is required to change the value if the qubit from 0 to 1 or 1 to 0. Therefore the qubits can be represented mathematically as

$\alpha|0> + \beta|1> \rightarrow$ Amount of energy required to spin the atom

Similarly, 2 qubits can be structured as: 2- Qubits will represent 4 states.

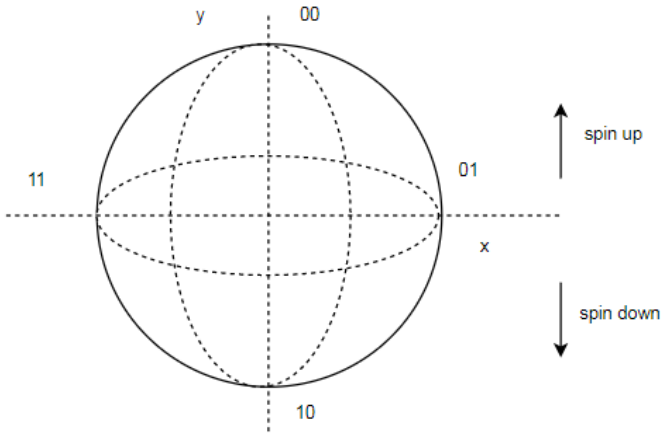


Figure 2 : 2-Qubit

Therefore to spin the atom to any of four state, we will require four coefficients determining the magnitude to change the state of the qubit. Therefore, the qubit can be represented as

$\alpha|00> + \beta|01> + \gamma|10> + \sigma|11>$ Amount of energy required to spin the atom

Similarly, we can imagine for 3-qubits, 4-qubits, ..., n-qubits, which will have 2^n states. Quantum bits can exist in superposition and entanglement.

1.3.1 Superposition principle

Superposition is the principle of Quantum mechanics and its states that a particular atom can exist in multiple states in space simultaneously.

1.3.2 Entanglement

Entanglement states the two or more qubits can exist in correlation with each other in space such that the change in one qubit will react in the state of its correlated qubit as well.

1.4 Quantum gates

Quantum logic gates are basic Quantum circuit which operates on single or multiple qubits. Quantum logic gates shows two analogous behavior to Quantum computers as the classical logic gates shows for digital computers. Logic gates are reversible and irreversible. But Quantum logic gates are reversible showing non-identical properties than classical logic gates.

1.4.1 Reversible and irreversible gates

Quantum logic gates operation is based in elementary unitary matrix operation which is reversible. The importance of reversible logic in Quantum computing is considered as a promising design paradigm. It is the ultra low power computation and is the emerging future technology because of the possibility of nearly energy free computation.

Quantum computing as a physical realization of reversible logic motivates to do further research in this domain. The gates in Quantum which are represented using the unitary matrix of matrices also have potential to implement the reversible logic. Classical logical reversible gates are ones which act on binary digits or bits.

Similarly, reversible gates are used in Quantum gates and act on qubit which is a unit of Quantum information. A circuit is called a reversible if and only if there is a one to one correspondence between its input and output. Here, the output can be uniquely determined from input and input can also be recovered from the output.

If a reversible function is shown by a truth table, then its output pattern must be the permutation of its input pattern. This phenomenon implies that the number of input and output of a reversible circuit are equal. Generally, with a input there exists 2^n reversible gates.

1.5 Commonly used Quantum gates

1. NOT gate

NOT gate is the simplest example of reversible logic gate. NOT gate represents 1-input / 1-output gate that simply inverts the bit value it gets. The truth table of NOT gate is shown below. In quantum computing a circuit may not have any physical wires connecting the gates together. Instead a circuit can be merely a visual specification of a sequence of gate operations with time increasing from left to right in the circuit diagram as successive gates are applied.

Table -1: NOT gate: Truth Table

a	¬a
0	1
1	0

The representation of NOT gate is shown below:

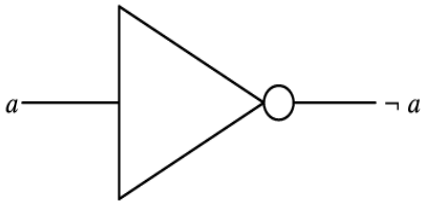


Figure 3 : NOT gate

2. CNOT gate

Alternative icon for a SWAP gate that is more common in quantum circuit diagrams. The reason for having a different icon for SWAP in quantum circuits compared to classical circuits is that many implementations of quantum circuits do not have physical wires as such. Hence, it could be misleading to depict a SWAP operation as a crossing of wires. Instead, a SWAP operation can be achieved as the result of a sequence of applied fields.

Table -2: CNOT gate: Truth Table

a	b	a'	b'
0	0	0	1
0	1	0	0
1	0	1	1
1	1	1	0

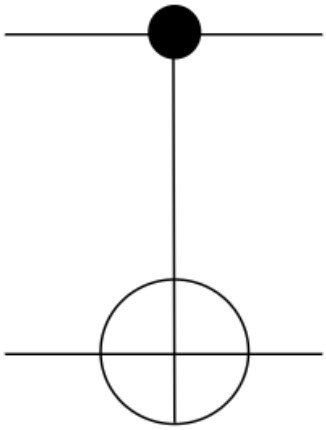


Figure 4: CNOT gate

The representation of CNOT is represented as: That is, the decision to negate or not negate the second bit is controlled by the value of the first bit. Hence, the name "Controlled-NOT". Note that, as shown, the SWAP gate can be obtained from a sequence of three CNOT gates.

3. Toffoli

The Toffoli gate is known to be universal for reversible Boolean logic, the argument for which is based on the fact that the Toffoli gate contains the NAND gate within it. A universal three-bit gate was identified by Toffoli in 1981, called the Controlled-Controlled-NOT.

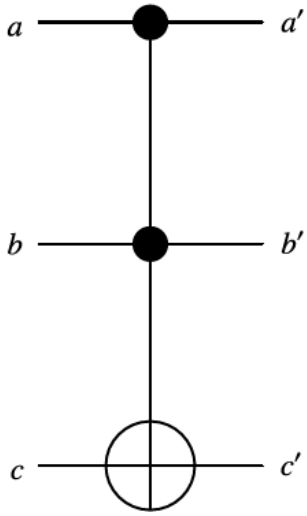


Figure 5: Toffoli gate

Table -3: Toffoli gate: Truth Table

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

4. Fredkin

Fredkin gate becomes very suitable for the reversible computing. It is a universal gate; so any logical or arithmetic operation can be conducted through the only use of Fredkin gates. The Fredkin gate is the reversible three-bit gate that swaps the last two bits if the first bit is 1. The truth table of Fredkin gate can be represented as:

Table -4: Fredkin gate: Truth Table

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

5. Hadamard gate

One of the most useful single qubit gates, in fact perhaps the most useful one, is the Hadamard gate, H. The Hadamard gate is defined by the matrix:

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

$$|0\rangle \quad -\boxed{H}- \quad \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \quad -\boxed{H}- \quad \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

1.6 No Cloning Theorem

The no cloning theorem is a result of quantum mechanics which forbids the creation of identical copies of an arbitrary unknown quantum state. It was stated by Wootters, Zurek, and Dieks in 1982, and has profound implications in quantum computing and related fields. The theorem follows from the fact that all quantum operations must be unitary linear transformation on the state. Suppose the state of a quantum system A is a qubit, which we wish to copy. The state can be written as

$$|\psi\rangle_A = a|0\rangle A + b|1\rangle A$$

The complex coefficients a and b are unknown to us. In order to make a copy, we take a system B with an identical Hilbert space and initial state |e>B (which must be independent of |ψ>A, of which we have no prior knowledge). The composite system is then described by the tensor product, and its state is |ψ> A |e> B.

There are only two ways to manipulate the composite system. We could perform

an observation, which irreversibly collapses the system into some Eigen state of the observable, corrupting the information contained in the qubit. This is obviously not what we want. Alternatively, we could control the Hamiltonian of the system, and thus the time evolution operator U(Δt), which is linear. We must x a time interval Δt, again independent of |ψ> A. Then U(Δt) acts as a copier provided,

U(Δt) |ψ> A |e> B
= |ψ> A |ψ> B(a|0> A+b|1> A)(a|0> B+b |1>B)
= a_2 |0> A |0> B + ba |1> A |0> B + b_2 |1> A |1> B

For all ψ. This must then be true for all the basis states as well, so

U(Δt) |0> A |e> B = |0> A |0> B
U(Δt) |1> A |e> B = |1> A |1> B

Then the linearity of U(Δt) implies

U(Δt) |ψ> A |e> B
= |ψ> A |ψ> B(a|0> A + b |1> A) (a|0> B + b|1> B)
≠ a_2 |0> A |0> B + ba |1> A |0> + ba |1> A |0> B + b_2 |1> A |1> B

Thus, U(Δt) |ψ> A |e> B is not generally not equals to |ψ> A |ψ> B, as may be verified by plugging in a = b = 2 - $\frac{1}{2}$, so U(Δt) cannot act as a general copier. Q.E.D. In contrast, the no cloning theorem is a vital ingredient in quantum cryptography, as it forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key.

1.6 Bloch Sphere

Quantum mechanics is mathematically formulated in Hilbert space or projective Hilbert space. The space of pure states of a quantum system is given by the one-dimensional sub spaces of the corresponding Hilbert space (or the "points" of the projective Hilbert space). For a two-dimensional Hilbert space, this is simply the complex projective line. This is the Bloch sphere.

1.7 Bell states

Bell state is the concept in quantum information science and represents the simplest example of entanglement. An EPR (Einstein, Podonsky, Rosen.) pair is a pair of qubits that are in a bell state together i.e. entangled with each other.

1.8 Heisenberg's uncertainty principle

In quantum mechanics, the uncertainty principle, also known as Heisenberg's uncertainty principle or Heisenberg's indeterminacy principle, is any of a variety of mathematical inequalities asserting a fundamental limit to the precision with which certain pairs of physical properties of a particle, known as complementary variables, such as position x and momentum p, can be known, it states that the more precisely the position of some particle is determined, the less precisely its momentum can be known, and vice versa.

2. Data encoding protocols in quantum encoding

2.1 BB84

The first ever cryptographic protocol in Quantum computation is BB84. This protocol was invented and developed by Charles Bennett and Gills Brassard in 1984. The protocol is secure and provably relying on the Quantum property that information gain is only possible if the 2 states, one is trying to distinguish are not orthogonal. The concept behind this point is no cloning theorem. BB84 protocol is

used for secure communication from source to destination in Quantum computers. BB84 scheme, suppose that the source 'A' wishes to send a private key to 'B'. 'A' begins with a 2 string of bits 'a' and 'b', each of n bits long. Then these Strings are encoded of n qubits.

$$|\psi> = \bigotimes n_i = 1 \ |\psi a_i b_i>$$

a_i and b_i are i^{th} bit of a and b respectively. a_i and b_i together gives us an index of four qubits states

$$|\psi 00> = |0>$$
$$|\psi 10> = |1>$$
$$|\psi 01> = |+> = \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$$
$$|\psi 01> = |-> = \frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>$$

The Important part is to take in guidance is that the b_i is what decides in which basis a_i is encoded. Therefore, the qubits are now not in mutually orthogonal states. Thus it is now impossible to determine all of them with certainly without knowing b.

2.1.1 Working of BB84

The Benetton Brossard quantum cryptographic key generation protocol or BB84 protocol: Assume Alice and Bob, as they would like to send encrypted messages between each other so that their messages can securely be made private. To do this they need a cryptographic key that is only known to them and which they'll use to encrypt their messages. Unfortunately they know that somewhere out there are nemesis, Eve may try to intercept their messages and foil their secret plans. Alice assures Bob however that they need not to worry about Eve. She will teach Bob about BB84 protocol and it will allow them to come up with a secret key they can both use and trust. Eve wont perceive any message. To communicate through fundamentally different communication channels, a classical channel and a quantum channel. The classical channel allows them to decide individual bits of information back and forth just as they would if they were using say the internet as the bits travel across the classical channel; it is possible for Eve to intercept them. Eve can observe the bits and then send copies of them on to their regular destination. When communicating over the classical channel, Alice and Bob have no way to detect Eves intrusion on their privacy. The quantum channel behaves quite differently. Instead of transferring bits, the quantum channel transfers qubits. The qubits represents bits and can be generated by either of two processes, as process A and process B. The BB84 protocol takes advantage of some special properties of qubits. First, a qubit cannot be copied. And second, it is not possible to determine whether the qubit was produced by process A or process B.

Process A → |10> **Process B → |10>**

There exists a very special machine for observing qubits that were produces by process A. Call it machine A. When a qubit represents 0, is fed into machine A. The machine will output a 0. When a qubit representing a bit 1 is fed into machine A, the machine will output 1. In both cases, the qubit will also be destroyed in the process. On the other hand, if machine A is fed a qubit produced by process B , its output will be random. Half the time is 0, half the time 1 and the qubit will still be destroyed. Likewise a special machine exists, for observing qubits produced by process B, call it machine B. When given a qubit produced by process B, machine B will output the correct bit. But when fed by a qubit produces by process A, machine B's output will be random. Just as with machine A, the qubit will be destroyed. So when Bob receives a qubit over the quantum channel, he won't know which machine to use to observe it. He will decide via a coin toss (random), half the time feeding the qubit to the machine A, half the time feeding it to machine B. The protocol begins with Alice sending Bob a very large number of qubits over the quantum channel. Bob records all of the outputs he receives, as he feed the qubits randomly to his qubit measuring machines. Since he will choose the correct machine half the time on average 50% of his measurement will be correct of the remaining qubits for which he used the wrong machine, he will still end up with the correct bit, half the time just by chance. This means, that 75% of Bob's measurements will agree with the corresponding values used by Alice. However, if Eve intercepts, the qubits, before they reach Bob, she will also have to make random guesses as to which machine is the correct one for measuring each qubit. Half the time she will use the machine A, and use the process A to generate a new cubit to pass on to the channel . The other half of the time, she will use machine B to observe the qubit and process B to generate a substitute to pass on the channel. Thus, with Eve attempting to listen on the quantum channel, half of the substitute qubits she send to Bob will have been generated correctly and half of them will have been generated incorrectly and are therefore simply random qubits. This means, only 75% of the qubits that reach Bob will represent the same bits that Alice intended. Now when Bob finally receives the qubits he will still be making random guesses as to how they should be measured. Half of the qubits will jibe with those that Alice sent and we know Bob will get 75% of those correct. The other half will have been generated incorrectly by Eve and are thus completely random. Bob will only get the correct bit from those half the time just by chance alone. This gives Bob a new accuracy of only 62.5% on average. Bob however does not know this yet. So Alice and Bob have to communicate some information between each other to work out what kind of accuracy Bob is getting. Once Bob has finished measuring all the qubits he received, he will open the classical channel and send Alice a string of bits that indicate to her which machine he used to measure each of her qubits. Once she receives that message from Bob, She will cross reference her personal records and send a stream of bits telling him which of his qubits he should have ended up measuring correctly. Now Bob can throw away the bits which he used the wrong machine. Alice can do the

same. They need to verify however that this is indeed the case since that they have a very large sequence of bits they can afford to sacrifice a random subset of them in order to determine whether Eve was listening over the classical channel, they choose the subset of bits and compare them if they are satisfied that the communication was secure, they can use the remaining bits to form a secret cryptographic key. If they observe an accuracy of 100%, they can be reasonably con dent that their shared bits are secure and they can begin using them to crypt further communication. If they observer an accuracy rate slightly below 100%, they will know that Eve intercepted some or all of their qubits and the communication is not yet secured. Thus, by using this protocol, Alice and Bob can determine their secrecy and can communicate privately.

2.2 SARG04

Another protocol after BB84 is the SARG04 protocol. Advanced version with more reliability an robustness , the SARG04 protocol comes into the quantum cryptography family. This protocol was built when researchers noticed by suing 4 states of BB84 with a different information encoding which would be more robust. SARG04 robustness can be seen against the photon splitting attack when attenuated laser pulses are used instead of single photon sources. The protocol SARG04 has some insecurities with the implementation of single photon. Let us start with some examples: Alice and Bob where Alice is source and Bob is the receiver Alice sends private key to Bob, now Alice starts with 2 strings a and b of n bits. Alice encodes those 2 strings with the n qubits. Now after receiving the string Bob proceeds to generate a string of bits b' of same length as b. Now here the thing comes that Bob announces publicly that he has received the transmission of Alice For each transmitted qubit the sender chooses one Hadamard basis state. These two states are announced by Alice that is Hadamard state and computational basis state. Now the 2 states which are announced are noted by Alice whether they are computational basis state or Hadamard state. If either one is chose or identified then that piece of information make up the secret bit. This secret bit is used by Alice to communicate with Bob. For example, Alice transmits |ψ00> state and announces the states |ψ00> and |ψ01> . Now, we can check for both computational basis as well as the Hadamard basis. Outcome is clearly with the state having been |ψ00> and it would be consistent as well if the outcome would been |ψ01>

By using the possibilities of Hadamard basis for the state if it would be the |ψ01> transmitted by Alice. The probabilities would be either |ψ01> or |ψ11> each with 50% probabilities as measured with Hadamard gate. Now if the outcome is |ψ01> then again this state is consistent with either of state in the starting. Now, if the outcome is |ψ11> ,it cannot be possibly observed from a qubit in state of |ψ01>. So if Bob measures using Hadamard basis and observed the state |ψ01> then he can be aware that of which state he was sent and what the secret bit can be to communicate with Alice. Now for the remaining say k bits Bob measurement was conclusive. The sender chooses some $\frac{k}{2}$ bit randomly and announces the choices on the public channel. Similarly, Bob also does it and both of them runs a check to see if more than a certain number of them agree. If yes then they are further proceeded to use privacy amplification and information reconciliation to create number of shared secret key. In BB84, Alice or the sender never announces the basis of his/her bits and therefore the eavesdrop or the hacker hast to store more copies of qubit in order to determine the basis of the state. The beneficial use of SARG04 is in situations where information is started by a poisonous source producing weak pulses. The term poisonous source producing weak pulses mean the number of photon < 1 and are received by an imperfect detector. The security test performed by Kiyoshi Tamaki and Hoi-Kwong lo were successfully in proving securities for one and 2 pulses using SARG04. SARG04 is more robust than BB84 against incoherent PNS attack The better performance between SARG04 and BB84 was observed. By using single photon implementations SARG04 and BB84 were considered equal according to the theory. But experiments showed that this was proves wrong and was inferior.

2.2 E91

The E91 algorithm uses entangled pairs of photons. These can be created by Alice or by Bob or by some other party. The photons are distributed so that Alice and Bob each end up with one photon from each pair. The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated , it means that that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. This necessitates that the two distant parties have exact directionality synchronization. However, it is impossible for Alice to predict if she and Bob will get vertical polarization or horizontal polarization. Second, any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect. Similarly to BB84, the protocol involves a private measurement protocol before detecting the presence of Eve. They keep their series of basis states private until measurements are completed. Two groups of photons are made, the first consisting of the photons measured using the same basis that of Alice and Bob while the second contains all other photons. To detect eavesdropping, they can compute the test statistic S using the correlation coefficients between Alices bases and Bobs similar to that shown in the Bell test experiments. Maximally entangled photons would result in ||S||= 2 2 . If this were not the case, then Alice and Bob can conclude Eve has introduced local realism to the system, violating Bells Theorem. If the protocol is successful, the first group can be used to generate keys since those photons are completely anti-aligned between Alice and Bob.

3. Data encryption

Data Encryption is a field which is emerging day-by-day. Main aim of this field is to protect digital data confidentiality. In this, we convert data from one form to another so that privacy can be maintained. Encrypted text is called as Cipher text. This kind of data is not easy to understand as the data is encrypted by using a pattern which can only be decrypted by the key. We can get the original data if we know the key or have the password. There are mainly two methods of encryption :

1. **Symmetric Encryption:** This method of encryption is also called as private-key cryptography. In this method the key used is secure. Sender uses the key to encrypt messages and receiver uses the key to decrypt the messages.

2. **Asymmetric Encryption:** This method of encryption is also called as public-key cryptography. In this method there are two keys. First key is used to encrypt messages, which can be owned by multiple users as it is public. Second key is private, used to decrypt the messages owned by receiver only.

There are different types of encryption techniques such as :

1. **DES (Data Encryption Standard):** DES is a symmetric data encryption technique. DES has an effective key length of 56 bits. It is an outdated technique been replaced by modern encryption techniques.

2. **Triple DES:** Triple DES was designed to replace the original DES (Data Encryption Standard) which hackers eventually learned to defeat with ease. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits. This technique is rarely used in industries nowadays.

3. **RSA algorithm:** RSA is a public-key encryption algorithm. It is standard for encrypting data sent over the internet. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. Attackers take quite time and processing power to break this, so it is widely used.

4. **Blowfish:** Blowfish is a another technique to replace DES. In this, the messages are split up into 64 bits data and then each block is encrypted separately. This technique is famous for its speed and its effectiveness.

5. **Twofish:** Twofish is the successor of blow sh. In this key can be of 256 bits in length and as it uses symmetric encryption method, only one key is needed. Twofish is considered as the fastest encryption algorithm. Blowfish and Twofish are freely available.

6. **AES (Advanced encryption standard):** AES is an Advanced encryption technique. It is very efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes in industries.

Cyber-attacks are evolving day-by-day. To put a check on this we need to use more advanced version of security for our data. One of the emerging method is Quantum Key Distribution, which shares keys embedded in photons which is passed through fiber optic cable. So in this paper we introduce Quantum Encryption technique which uses the concepts of physics and to break, it will take attackers a lot of efforts. It is true that nothing is 100% secure, but we can choose a method that can provide better security now and in future as well.

4. Quantum Key Distribution

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. QKD is used to generate a shared secret key and not to transfer data. The key is known only to the sender and receiver which is then used to encrypt and decrypt messages. The ability of QKD is that the presence of any eavesdropper trying to intercept the channel can be detected. By using the principles of superposition and entanglement the system to detect eavesdroppers can be implemented. The network consists of a certain threshold. If the eavesdropping level is below a certain threshold, a key can be produced otherwise key will not be produced and communication will be aborted. The efficiency of the QKD system relies on the foundations of Quantum Mechanics. It depends on the mathematical functions. Once the key is produced it can be wrapped around with algorithms to encrypt or decrypt a message, which can be transmitted over a standard communication channel. Most commonly used algorithm associated with the QKD is the one-time pad. It can also be used with encryption using symmetric key algorithms like the Advanced Encryption Standard(AES).

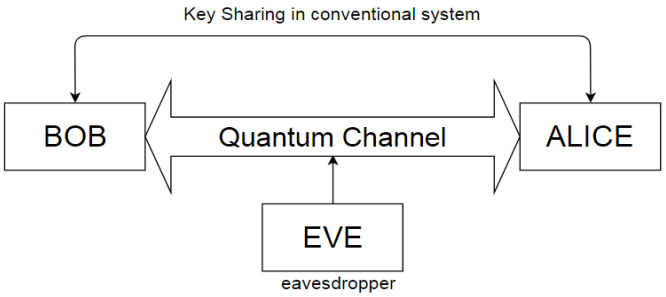
5. Existing System

Today's network systems are susceptible to various security threats and vulnerabilities. Also, today's network systems cannot detect the presence of intruders in the network. Today's existing systems also does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols and procedures. This need to be fixed through proper design and setting up of advanced infrastructure. Also if we introduce more and more cryptographic techniques and add various levels of security, then the information processing leads to delay. The security of cryptographic technique is limited by the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems on increasing the

computing power can render a cryptographic technique vulnerable. These drawbacks in classical systems can be overcome by quantum systems.

6. Proposed System

Our proposed system is based on Quantum Key Distribution mechanism. The QKD system is useful in sharing a secret key between two parties(namely Alice and Bob) securely. Quantum key distribution requires a transmission medium on which quantum carriers are transmitted from Alice to Bob. In theory, any particle obeying the laws of quantum mechanics can be used. The quantum carriers are photons, the elementary particle of light; while the channel may be an optical fiber (e.g., for telecommunication networks) or the open air (e.g., for satellite communications). In the quantum carriers, Alice encodes random pieces of information that will make up the key. These pieces of information may be, for instance, random bits or Gaussian-distributed random numbers. During the transmission between Alice and Bob, Eve might listen to the quantum channel and therefore spy on potential secret key bits. This does not pose a fundamental problem to the legitimate parties, as the eavesdropping is detectable by way of transmission errors. Also, the secret key distillation techniques allow Alice and Bob to recover from such errors and create a secret key out of the bits that are unknown to Eve. After the transmission, Alice and Bob can compare a fraction of the exchanged key to see if there are any transmission errors caused by eavesdropping.



7. CONCLUSIONS

QKD relies on a property of physics to secure the transmission of information. Highly secure communications are possible by using the QKD channel to transmit symmetric keys. Symmetric keys have much higher and proven quantum and classical attack resilience. Furthermore, the fact that the existing cryptographic techniques are not provably secure makes QKD a safer option even without the existence of quantum computation. There is no reason other than trust in the academic community to suspect that classical public key protocols have not already been broken and that highly secretive decoding of internet traffic is currently being performed. Thus, controlling the implementation flaws, QKD systems are proven to be secured based on scientific principles.

REFERENCES

[1] Qiankai Yao,Bin Zhang,Yanwei Luo,Hui Huang: A Single Quantum Cannot be ClonedNature,

[2] Dieks D.: Communication by EPR devices.Physics Letters A, vol. 92(6), pp. 271-272(1982)

[3] Buzek, V. and Hillery, M.: Quantum cloning. Physics World 14 (11) , pp. 25-29 (2001)

[4] Baichuan Huang, Yan Huang, Jiaming Kong, Xin Huang: Model Checking Quantum Key Distribution Protocols, Department of Computer Science, University of Liverpool, 8th International Conference on Information Technology in Medicine and Education (2016)

[5] Anand Sharma, VibhaOjha, Prof. S.K.Lenka:Security of Entanglement Based Version of BB84 protocol for Quantum Cryptography, Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference (2010)

[6] Sapna Saxena and Bhanu Kapoor: An E cient Parallel Algorithm for Secured Data Communications using RSA Public Key Cryptography Method, Advance Computing Conference (IACC), 2014 IEEE International (2014)

[7] Abhishek Parakh: New Protocol for Quantum Public Key Cryptography, University of Nebraska, Omaha Advanced Networks and Telecommuncations Systems (ANTS), 2015 IEEE International Conference (2015)

[8] Joo Yeon Cho and Helmut Griesser: Secure Deployment of Quantum Key Distribution in Optical Communication Systems (2017)

[9] M. Deepthi and G. Murali: Robust Quantum Key Distribution Based On Two Level QRNA Technique To Generate Encrypted Key, Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference (2016)

[10] Anton Pljonkin and Konstantin Rumyantsev: Single-photon Synchronization Mode of Quantum Key Distribution System, Southern Federal University Taganrog, Russia, Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference (2016)

[11] Javier Sanchez, Ronny Correa, Hernando Buenano, Susana Arias and Hector Gomez: Encryption Techniques: A Theoretical Overview and Future Proposals, Universidad Tecnica de Ambato, Ecuador, eDemocracy eGovernment (ICEDEG), 2016 Third International Conference, (2016)

[12] Horace P. Yuen: Security of Quantum Key Distribution, Northwestern University, Evanston, IL 60208, USA, IEEE (2016)

[13] Lizal Iswady Ahmad Ghazali, Ahmad Fauzi Abas: Security Proof of Improved- SARG04 Protocol Using the Same Four Qubit States, Photonics (ICP), 2010 International Conference (2010)

[14] Huang Hong-Mei: Quantum secure direct communication protocol based on cluster entangled state, University of Armed Police Force Engineering Xian, China, P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference (2015)

BIOGRAPHIES

Abbasali Antelawala
B.E. Computer Engineer
KJCOEMR Pune.

Hatim Chathiwala
B.E. Computer Engineer
KJCOEMR Pune.

Rishabh Shukla
B.E. Computer Engineer
KJCOEMR Pune.