04/08/23

UNIT- 5

PHYSICS OF QUANTUM COMPUTING AND QUANTUM GATES

Classical Bit versus Quantum Bit

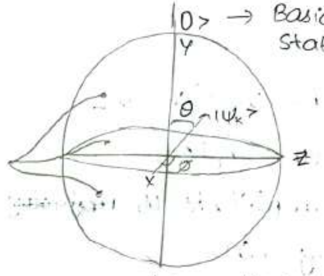
- A classical bit is represented by either '0' (or) '1', which means it possess only two states. This is used by large scale multipurpose computers and devices.
- Quantum bit (or) Q-Bit is the basic unit of the quantum information, Q-Bits are represented by '<u>Ket vectors</u>' as $|0\rangle$ & $|1\rangle$ also their exist large number of Q-Bits between $|0\rangle$ & $|1\rangle$

Difference between classical computing and quantum computing

Classical Computing	Quantum computing
* Information is stored in bits.	* Information is stored in Q-Bits.
* A classical computer has a memory made up of bits where each bit holds either '0' (or) '1'.	* A Q-Bit holds 1, 0 (or) super-position of these two.

* The device computers by manipulating these bits with the help of classical logic gates like AND gate, OR gate, NOR gate.	* The device computers by manipulating these quantum gates.
* In classical computers information is stored in bits which takes more space.	* Here the information is stored in Q-Bits. As Q-Bit can be in states are represented by $|0\rangle$, $|1\rangle$ but it can also be a superposition of these two states. $a|0\rangle + b|1\rangle$, where a, b are complex numbers.
* Classical Bits are slow	* Quantum Bits are fast (like CSE-C students)
* Its circuit behaviour is based on classical physics.	* Its circuit behaviour is based on quantum physics.

BLOCH SPHERE



5/8/23

- In Quantum computation, superposition of states is represented on "Bloch sphere". In Quantum mechanics, the block sphere is a geometrical representation of the pure state space of a two-level quantum mechanical system (Q-Bit).

: Assuming the space in the shape of sphere it also called Hilbert space.

- The north and south poles of the block sphere are corresponds to the standard basic vectors $|0\rangle$ & $|1\rangle$.
- If spin up represented by $|0\rangle$ then spin down is represented by $|1\rangle$
- The points on the surface of the sphere correspond to the pure state, the interior points corresponding to the mixed state (superposition states).

- Superposition states can be represented by -
  $a_1|0\rangle \; a_2|1\rangle$
- Mixed states can be written as -

$$|\psi_K\rangle = a_0|0\rangle \; a_1|1\rangle$$

where a_0 is the amplitude of measuring $|0\rangle$
a_1 is the amplitude of measuring $|1\rangle$

- The superposition state of a Q-Bit is represented as -

$$|\psi\rangle = e^{i\vartheta}\left[\cos\theta/_2|0\rangle + e^{i\phi}\sin\theta/_2|1\rangle\right] \rightarrow (1)$$

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \rightarrow (2)$$

where $a_0 = e^{i\vartheta}\cos\theta/_2$ - amplitude of measuring $|0\rangle$
$a_1 = e^{i\phi}\sin\theta/_2$ - amplitude of measuring $|1\rangle$

- The value of $e^{i\vartheta}$ is a overall phase factor which can be neglected

$$\Rightarrow |\psi\rangle = \cos\theta/_2|0\rangle + e^{i\phi}\sin\theta/_2|1\rangle \rightarrow (3)$$

where $0 \leq \theta \leq \pi$

- Thus any state $|\psi\rangle$ can be represented interms of $|0\rangle$ & $|1\rangle$ in the above eqn (3)

Quantum Gates

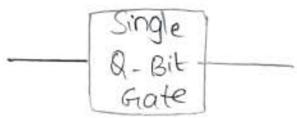
The quantum computing gates are represented by matrix i.e., $\sum_i |a_0\rangle\langle a_i|$

- Quantum gates are logic circuits which takes Q-Bits as input and delivers output.
- Quantum circuits are consist of gates and wires. The wires carries the information and gates manipulate that information.
- There are two types of logic gates
  1. Single Q-Bit logic gates
  2. Two Q-Bit logic gates

Single Q-Bit logic gates

These are the logic gates which takes one Q-Bit as the input and one Q-Bit as output.

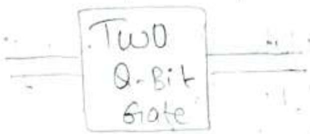
- They are four types
  (a) Pauli X - Gate - Quantum NOT Gate.
  (b) Pauli Y - Gate - Quantum Y - Gate
  (c) Pauli Z - Gate - Quantum Z - Gate
  (d) Hadmard Gate.



Two Q-Bit logic gates

These are the logic gates which takes two Q-Bits as input and gives two Q-Bits as output.

- They are two types:
  - i) CNOT Gate
  - ii) SWAP Gate



7/8/23 Representation of Quantum Gates in Matrix Form

The matrix representation of Quantum Gates are given by summation of input, output.

$$\sum_i |\text{input}\rangle\langle \text{output}|$$

Notation for computational basis

1. Single Q-Bit basis

Input	Output
$\|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\langle 0\| = [1 \; 0]$
$\|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\langle 1\| = [0 \; 1]$

2. Two-level Q-Bit basis

Input	Output
$\|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$	$\langle 00\| = [1\,0\,0\,0]$
$\|01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$	$\langle 01\| = [0\,1\,0\,0]$
$\|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$\langle 10\| = [0\,0\,1\,0]$
$\|11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$\langle 11\| = [0\,0\,0\,1]$

Single Q-Bit Logic Gates

1. Pauli X-Gate - Quantum NOT Gate

Quantum NOT Gate in matrix form

$$|0\rangle \text{---}\boxed{X}\text{---} \langle 1|$$

$$|1\rangle \text{---}\boxed{X}\text{---} \langle 0|$$

$$= |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix}[0 \; 1] + \begin{bmatrix} 0 \\ 1 \end{bmatrix}[1 \; 0]$$

$$= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

In Quantum NOT Gate if input is 'zero' then output is 'one' and if input is 'one' then output is 'zero'.

2. Pauli Y- Gate - Quantum Y-Gate

Pauli Y- Gate acts on a single Q-Bit.

- It equates to a rotation around the Y-axis of the bloch sphere by π radians...
- It maps from $|0\rangle$ to $i\langle 1|$ & $|1\rangle$ to $-i\langle 0|$

$|0\rangle$ —[Y]— $i\langle 1|$

$|1\rangle$ —[Y]— $-i\langle 0|$

Truth Table

input	output
$\lvert 0\rangle$	$i\langle 1\rvert$
$\lvert 1\rangle$	$-i\langle 0\rvert$

Matrix Representation of Y-Gate

$$Y = \sum_i |\text{input}\rangle\langle \text{output}|$$

$$= \sum_i |0\rangle i\langle 1| + |1\rangle(-i)\langle 0|$$

$$= \begin{bmatrix}1\\0\end{bmatrix} i \begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}(-i)\begin{bmatrix}1 & 0\end{bmatrix}$$

$$= \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & i\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}-i & 0\end{bmatrix}$$

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

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

3. Pauli Z- Gate - Quantum Z-Gate

It inverts sign of $|1\rangle$ to give $-\langle 1|$ and leaves $|0\rangle$ unalternate.

$|0\rangle$ —[Z]— $\langle 0|$

$|1\rangle$ —[Z]— $-1\langle 1|$

- For $|0\rangle$ input the output $\langle 0|$ and for $|1\rangle$ input the output is $-1\langle 1|$

Matrix Representation of Z-Gate

$$Z = \sum_i |\text{input}\rangle\langle \text{output}|$$

$$= |0\rangle\langle 0| + |1\rangle(-1)\langle 1|$$

$$= \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & -1\end{bmatrix}$$

$$= \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\0 & -1\end{bmatrix}$$

$$Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

4. Hardmard Gate in Matrix Form

- In Hardmarid Gate if the input is $|0\rangle$ and the output is $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and if the input is $|1\rangle$ and the output is $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$|0\rangle$ — $\boxed{\text{Hadmard}}$ — $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|1\rangle$ — $\boxed{\text{Hadmard}}$ — $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$\text{Hadmard Gate} = \sum_i |\text{input}\rangle\langle \text{output}|$$

$$= |0\rangle\langle \frac{|0\rangle |1\rangle}{\sqrt{2}}| + |1\rangle\langle \frac{|0\rangle - |1\rangle}{\sqrt{2}}|$$

$$= \frac{1}{\sqrt{2}}\left[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}\right]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} - \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right]$$

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

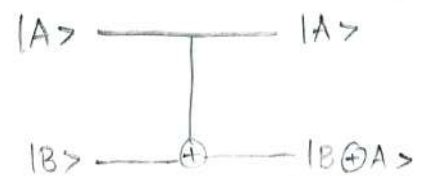
8/8/23

Two-level Q-Bit Gates in matrix form

Input	Output
$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$	$\langle 00| = [1\ 0\ 0\ 0]$
$|01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$	$\langle 01| = [0\ 1\ 0\ 0]$
$|10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$	$\langle 10| = [0\ 0\ 1\ 0]$
$|11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$	$\langle 11| = [0\ 0\ 0\ 1]$

Controlled NOT Gate - CNOT Gate

- CNOT Gate has two input Q-Bits knows as controlled Q-Bit and target Q-Bit.
- The circuit representation of CNOT Gate is shown in the below diagram



- The top line represents the 'controlled Q-Bit' while the bottom line represents 'target Q-Bit'.
- The action of the CNOT Gate is as follows -
  - → If the controlled Q-Bit is set to '0' then the target Q-Bit is left alone.
  - → If the controlled Q-Bit is set to '1' then the target Q-Bit is flipped.

Truth Table of CNOT Gate

Input	Output
$\|00\rangle$	$\langle 00\|$
$\|01\rangle$	$\langle 01\|$
$\|10\rangle$	$\langle 11\|$
$\|11\rangle$	$\langle 10\|$

Matrix representation of the CNOT Gate

$$\text{CNOT} = \sum_i |\text{input}\rangle\langle\text{output}|$$

$$= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

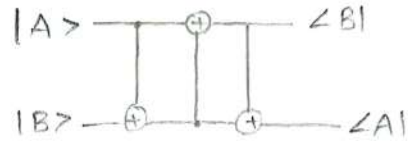
$$= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}[1000] + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}[0100] + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}[0001] + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}[0010]$$

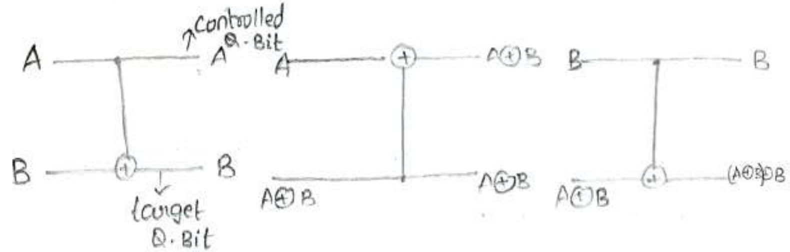
$$= \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$

$$= \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

SWAP Gate in matrix form

SWAP Gate swaps the states of the two Q-bits, it is prepared by using 3 CNOT Gates, the sequence of the SWAP Gate is represented below





Truth Table

Input	Output
$\|00\rangle$	$\langle 00\|$
$\|01\rangle$	$\langle 10\|$
$\|10\rangle$	$\langle 01\|$
$\|11\rangle$	$\langle 11\|$

Matrix representation of SWAP Gate

$$M_{SWAP} = \sum_i |input\rangle\langle output|$$

$$= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

$$= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}[1000] + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}[0010] + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}[0100] + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}[0001]$$

$$= \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$

$$M_{SWAP} = \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$$

Advantages of Quantum Computation over Classical Computation.

* Classical computers gradually approaching their limits, the Quantum computers promises to deliver a new level of computational power.
* It is a new theory of computation that incorporates the strategy effects of Quantum mechanics.
* Encode the more information.
* Easily crack secrete codes.
* Fast in searching database.
* Hard computational problems becomes trackable.
* It supports Artificial Intelligence.

Quantum Teleportation

Teleportation is a process which involves scanning of objects, dematerialization and transmitted to another location which results the object rematerialization i.e., back to original state.

Teleportation - (Telecommunication + Transportation)

This concept was first given by "Charles Bennet" and his co-workers / team from IBM. They confirmed that ~~transport~~ Quantum Teleportation was possible, but only if the original object being teleportated was destroyed.

Quantum Teleportation

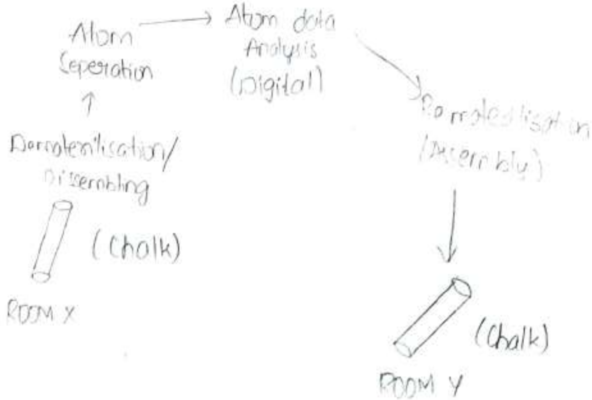
- It is a process by which quantum information (i.e., the exact state of an atom or photon), by which quantum information can be transmitted.
- Quantum teleportation is making of an object (or) person disintegrate at one place by a perfect replica appears somewhere else.
- Quantum teleportation involves entangling two things like photons (or) ions. so their states are dependent on one another and each can be effected by the measurement of the others state.

Steps involved in the Quantum Teleportation

- Scanning the object completely at the source side.
- Deassembling the scanned data and sending it to the destination.
- Assembling the object from the data, which was sent to destination.

9/8/23

- For example - In Quantum Teleportation an object send the image chalk piece from room X to room Y, the following process is the required steps.



Classification of Teleportation

Basically there are two types of teleportation.

1. Classical Teleportation
2. Quantum Teleportation

Classical Teleportation

In Classical Teleportation the exact replica of the source object is obtained at the destination, where as in Quantum Teleportation the exact copy of the source object at the destination and the source object is destroyed.

Quantum Entanglement

- The two particles of the system are said to be entangled, if any change in one particle brings a change in the other particle irrespective of the distance between two particles.
- In entangled state both particles remains the part of the same quantum system. So whatever you do to the one of the particle its effects another particle in a predictable way.
- Quantum entaglement transforms information around <u>three trillion m/s</u> (or) <u>four orders of magnitude faster than light</u>.

Heisenberg Uncertainity Principle

This principle states that one cannot measure accurately and simultaneously the position and the momentum of a quantum particles.

- The measurement of one value changes the other particle value accordingly.
- This law makes it impossible to measure the exact quantum state of any object with certainity.
- In order to teleport a photon without violating heisenberg uncertainity principle, a phenomena is used known as entaglement.

Advantages of Quantum Teleportation

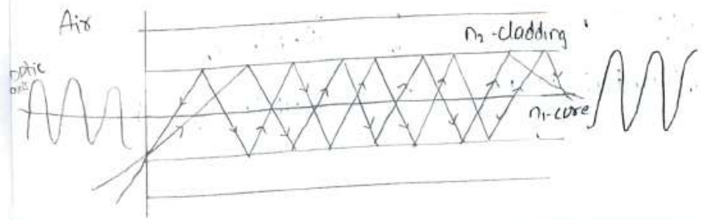
- Transmission of data at higher rates.
- Secure data transmission.
- Transportation becomes much easier.
- Reduced cost of transportation.

Dispersion

- During the transmission of information through optical cables several effects results in spreading of pulse width. This spreading of pulse width at the receiving end is called **dispersion**, which is considered as fibre loss.
- Spreading of output pulse may result in overlapping of adjacent pulses at the receiving end of the fibre.
- As a result of this transmission rate of signal is gradually decreases.
- Dispersion is divided into two types:
  1. Inter model dispersion
  2. Intra model dispersion

Intermodel Dispersion

→ In multimode step index optical fibre each mode enters the fibre at different angles and travels at different parts. Thus the ray arise at the different time at fibre output as shown in the diagram.



Intramodel Dispersion

- Based on the refractive index of the core material and also due to material properties dispersion takes place.

10/8/23

BB84 Protocol

In 1984 the first protocol for quantum cryptography was proposed by Charles. H. Bennit and Giller. Brassard. Therefore the name BB84 is given.

- This concept is purely dependence on Quantum mechanics, this protocol used pulse of "polarized light" where each pulse (light ray) contains a ~~sig~~ single photon.

Working

- To provide a secure communication sender can choose between 4 non-orthogonal states, receiver has two basis with polarized photons

The horizontal vertical bases ✛

- Vertical polarized ↕ Qubit = 0
- Horizontal polarized ↔ Qubit = 1

The diagonal bases ✕

- Diagonal 45° polarization ⤢ Qubit = 0
- Anti-Diagonal 135° or -45° ⤡ Qubit = 1

Two bases with polarized photos

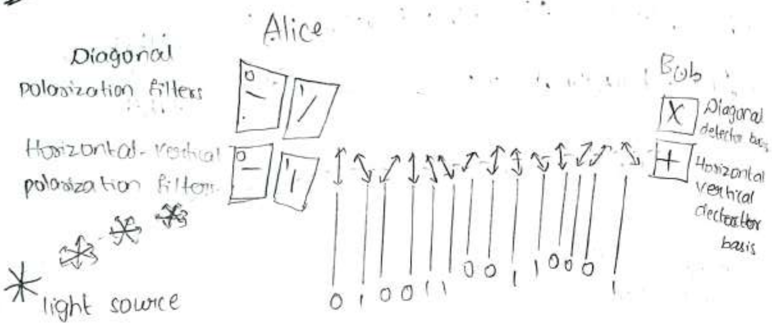
Type of polarization \ Value	0	1
Rectilinear +	|	—
Diagonal X	/	\

The process of BB84 protocol

The sender (Alice) choose randomly both the basis and polarization of each photon and sends corresponding polarization state to the receiver.

- Independently and randomly for each photon, receiver chooses one of the two basis, he either measures in the same basis as Alice and gets a perfectly corelated result or the exact opposite, he measures in the different basis than Alice and gets an uncorelated results.
- Sometimes it happens that receiver does not register anything because of the error in the detection (or) in the transmission.

11/8/23



- Receiver obtains a string of all received bits, also called 'raw key'
- For each bit receiver announces through the public channel which basis was used and which photon was registered. and he does not reveal which result he obtained.
- After comparing the selected bases, sender and receiver keep only the bits corresponding to the same bases because both are randomly choosen the bases they get corelated results with equal probability therefore 50% of raw key is discarted, this shorted key is called 'shifted key'
- Sender and receiver choose at random some of the remainings bits which they discart later to check the error rate. There are two main reasons why the error rate can differs from the expected value which gives technical imperfections in the setup and their arrangements. only receiver has this key
- To ensure a secret key, sender & receiver must correct the errors. With the help of this procedure they reduce eve's knowledge of the key. The remaining string of the is the secret key.

Now, the actual process of securely encrypting a message can began

- "Note that the secret key is truly random neither sender nor receiver can decide which key results, because they choose randomly between the bases"

Example : The following example is given to illustrate the process of BB84 protocol
In this case $|\leftrightarrow\rangle$ and $|\nwarrow\!\searrow\rangle$ for '1' and $|\updownarrow\rangle$ and $|\swarrow\!\nearrow\rangle$ for '0' (code)

Transmitting end	Transmitted bits	0	0	1	0	1	0	1	0	1
	Transmission basis	×	+	×	+	×	+	+	×	+
	Transmitted information	↗	↕	↘	↕	↘	↕	↔	↗	↔
Receiving end	Measuring basis	+	+	+	+	×	×	×	×	+
	Received results	↔	↕	↔	↕	↘	↔	↗	↗	↔
	Received bit	1	0	1	0	1	1	0	0	1
	Bases match	NO	YES	NO	YES	YES	NO	NO	YES	YES
	Derived key	-	0	-	0	1	-	-	0	1

NO-CLONING THEOREM

The theorem states that "It is impossible to make copy of an unknown quantum state".

- It was first proven in 1982 by Zurek and Wooters. In Quantum key distribution, this means that eve cannot make a copy of sender of photon and send it to receiver. Suppose if we want to clone an unknown quantum state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- We use some operators Vcopy as shown in the following diagram

$$V_{copy}|\psi\rangle_1|0\rangle_2 = |\psi\rangle_1|\psi\rangle_2$$

- The left hand side of the above equation is

$$V_{copy}|\psi\rangle_1|0\rangle_2 = V_{copy}(\alpha|0\rangle + \beta|1\rangle)_1|0\rangle_2$$
$$= V_{copy}(\alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|0\rangle_2)$$

- Note that the result is an entangled state
- Therefore equation of left side is not equal to equation on right side unless $\alpha = 1$ & $\beta = 0$ (or) viceversa, only $|0\rangle$ (or) $|1\rangle$ states can be copied but not a general quantum state

with superposition. An alternative viewpoint is that the matrix corresponding to V_{copy} is not unitary and therefore cannot be implemented. Therefore it is impossible to make a copy of unknown quantum state.