QUANTUM COMPUTING

Arpitha-IMT2018504
Neetha-IMT2018050
Nikitha-IMT2018051

“Quantum” is a term that comes from the study of Quantum Mechanics. It describes the physical properties of nature on an **atomic scale**. While Classical physics describes many aspects of nature at a macroscopic scale, it was found to be insufficient to explain the aspects of nature at small (atomic and subatomic) scales leading to the birth of Quantum mechanics.

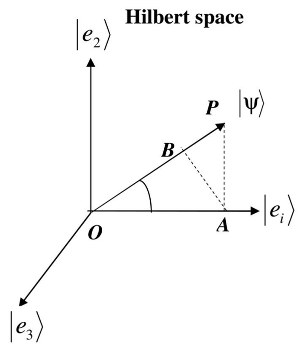
Nobel Laureate, Richard Feynman, observed in the early 1980s that certain quantum mechanical effects cannot be simulated efficiently on a classical computer. This observation led to speculation that perhaps computation, in general, could be done more efficiently if it made use of these quantum effects.
During a conference co-hosted by MIT and IBM in 1981, he challenged a group of computer scientists to develop a new breed of computing based on quantum physics. The field has evolved exponentially in the past 40 years and is known as Quantum computing today!

In summary, quantum mechanics provides four new phenomena: **quantization**, **entanglement**, the **principle of uncertainty**, and **wave-particle duality**. **Quantum computing** makes use of these quantum-mechanical phenomena to perform computation.

Quantum mechanics Foundations:

Before we dive into discussing Quantum computing, it is essential to look into the postulates/ foundations of Quantum mechanics on which they are built.
First Postulate: At a fixed time t_0, the state of a physical system is defined by specifying a wavefunction $\psi (x, y, z, t_0)$.
Second Postulate: Every measurable physical quantity A is described by an operator $\hat{A}$; this operator is called an observable. All observables are described by Hermitian linear operators.
(It is due to this that the eigenvalues of $\hat{A}$ are real. Observables should be represented as real numbers. Quantum transformations are also unitary making them reversible. Thus quantum gates must be reversible.)
Third Postulate: The only values that are obtained in a measurement of an observable “A” are the eigenvalues “a_n ” of the corresponding operator “ $\hat{A}$ ”. The measurement changes the state of the system to the eigenfunction of $\hat{A}$ with eigenvalue a_n .
Fourth Postulate: If a system is described by a normalized wavefunction ψ , then the average value of an observable corresponding to $\hat{A}$ is
$<a> = \int \psi^* \hat{A} \psi \, dt$

Hilbert space, Qubits and representation on Bloch sphere:



Classically, a bit is the smallest unit of information: capable of storing either a ***0 or a 1***. We can now imagine bits that obey the rules of quantum mechanics. These quantum bits, or ***qubits***, can then be used to process information in new and different ways. Mathematically, a qubit can be visualized as a ray in a Hilbert space.

Hilbert Space is a normed vector space, an inner product space, and a closed space which can be visualized as an infinite-dimensional sphere.

The Basis for a 2D Hilbert space can be denoted by {|0>, |1>} which has been fixed. The orthonormal basis |0> and |1> may correspond to the |↑> and |→> polarizations of a photon respectively could correspond to the spin-up and spin-down states of an electron. Unless otherwise specified, all measurements will be made with respect to the ***standard basis for quantum computation {|0>, |1>} where***

$|0>=\begin{bmatrix}1\\0\end{bmatrix}$ $\quad|1>=\begin{bmatrix}0\\1\end{bmatrix}$ (The $<|>$ being used refer to the bra and ket notation introduced by Dirac)

A qubit is can be represented as a ***state vector***: $|q>=\begin{bmatrix}a\\b\end{bmatrix}$ where a,b are complex numbers.

Since the states $|0\rangle$ and $|1\rangle$ form an orthonormal basis, we can represent any 2D vector with a combination of these two states. This allows us to write the state of our qubit in the alternative form: $|q>=a|0>+b|1>$

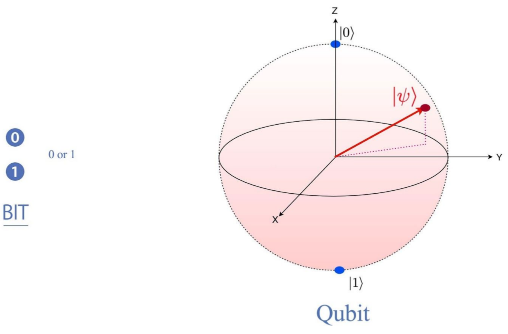
The statevector of the qubit tells us everything we could possibly know about this qubit. The first most basic conclusion about this particular example of a state vector is that it is not entirely $|0\rangle$ and not entirely $|1\rangle$. Instead, it is described by a linear combination of the two. In quantum mechanics, the linear combinations of two quantum states is called ***<u>SUPERPOSITION</u>***.

$|<q|0>|^2=a^2$ and $|<q|1>|^2=b^2$.

This means that the probability of finding q in |0> state = a^2 and in |1> = b^2 . Since it is normalised, the probabilities add up to 1 (which they should!) i.e **a^2+ b^2 = 1.**

As a result a qubit can also be represented in spherical coordinates with r=1:

$$|q>=cos\frac{\theta}{2}|0>+e^{i\phi}sin\frac{\theta}{2}|1>$$



Thus the easiest way to visualize the qubit is to picture it as a vector pointing along the surface of a sphere called ***BLOCH SPHERE***. When the qubit state is zero, it points towards the north pole and when the state becomes one, it points towards the south pole. The superposition state can lie anywhere along the equator of the sphere.

Classical vs Quantum

A Classical computer stores information in the form of 0s and 1s while a quantum computer encodes information in qubits. While a single bit has 2 possible states, a qubit can be in any state on the surface of the Bloch Sphere.

When we input a superposition state encoding all possible input values into the quantum computation, we get a superposition of all of the corresponding output values. Thus, in the time it takes for a classical computer to compute the output for a single input, a quantum computer can compute the values for all possible input states. This process is known as ***quantum parallelism***.

Further n in classical computations, the possible states of a system of n particles, whose individual states can be described by a vector in 2D, form a vector space of **2n** dimensions. However, in quantum, a system of n qubits has a state space of $\mathbf{2^n}$ dimensions.
This results in an ***exponential speedup of quantum computers over their classical counterparts.***

Entanglement:

Entanglement occurs naturally during the interaction between quantum systems as a result of the superposition principle. Superposition of inputs results in superposition of outputs (entangled state).The entangled state behaves in ways which cannot be explained simply by assuming that each of its constituents have a state of their own.

For example, in case of an entangled state of two photons, these two photons may be said to be in a definite state of sameness of polarization even though neither photon has a polarization of its own. Any property that we might try to attribute to these photons does not explain the strength of the correlation of their polarizations. Not just to determine if they had any polarization but if they had some property that could contribute to them separately. This famous result was discovered by John Bell in 1964.

Maximally entangled states:

As mentioned a n-qubit system has 2^n basis vectors.So the state space for two qubits has basis $\{|0> \otimes |0>, |0> \otimes |1>, |1> \otimes |0>, |1> \otimes |1>\}$, which can be written more compactly as $\{|00>, |01>, |10>, |11>\}$

Consider the state $|00> + |11>$. We cannot find a1 , a2 , b1 , b2 such that
$(a\ 1\ |0> +b1\ |1>) \otimes (a2\ |0> + b2\ |1>) = |00> + |11>$

States that cannot be decomposed in this way are called ***entangled states***. These states represent situations that have no classical counterpart.

There are four states of two qubits which lead to this maximal value of $2\sqrt{2}$ and are known as the maximally entangled two-qubit states or Bell states.

$$\frac{|00>+|11>}{\sqrt{2}}, \quad \frac{|00>-|11>}{\sqrt{2}}, \quad \frac{|01>+|10>}{\sqrt{2}}, \quad \frac{|01>-|10>}{\sqrt{2}}$$

EPR Paradox

When an EPR particle(entangled particle) is measured, its state becomes certain at that instant and at that exact same moment, the other EPR particle's state also becomes certain. For this to happen there should be some communication from the measured particle to the other particle at a speed greater than the speed of light. This is in direct violation of Einstein's theory of relativity, which states that nothing can go faster than the speed of light. So here we can either accept that nothing can go faster than the speed of light and accept that quantum mechanics is false or we accept quantum mechanics but disregard theory of relativity.

Quantum Gates:

A quantum gate is any rudimentary quantum circuit which changes the state of a qubit. They are reversible. ***Hadamard gates (H-gate):*** It is a single qubit operation which maps the basis state $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and basis state $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$, thus creating an equal superposition of the two basis states. Its matrix representation is .

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

The rows of the matrix are orthogonal. ⇒ H is a unitary matrix.

Pauli X-gate**:** It is a single qubit operation gate similar to the classical NOT logic gate. It maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.

Pauli Y-gate**:** It is a single qubit operation gate which maps $|0\rangle$ to $-i|1\rangle$ and $|1\rangle$ to $i|0\rangle$.

Pauli Z-gate**:** It is a single qubit operation gate which maps $|1\rangle$ to $-|1\rangle$ and leaves $|0\rangle$ unchanged.

Phase gate (S-gate)**:** Single qubit operation defined by

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

T-gate: Single qubit operation defined by $T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{-i\pi}{4}\right) \end{pmatrix}$

***CNOT gate*:** Two qubit operation with the first qubit as the control qubit and the second qubit as the target. When the control qubit is in state |1□, it performs a Pauli X-gate on the target qubit; when the control qubit is in state |0□, it leaves the target qubit unchanged.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Domains:

Quantum Cryptography

A majority of the classical cryptographic algorithms are based on problems that have no known poly-time algorithm, making them perfect candidates to use in encryption.
The RSA protocol, for instance, is based on the mathematical complexity of factoring large numbers. The largest number that can be factored classically is of 768 bits. Even that required 2 years using hundreds of computers! Typical RSA is 1024 or 4096 bits long.

However, Shor's algorithm proved that with quantum gates, it is possible to perform factorization of large integers, in polynomial time!

Shor's Algorithm:

Given an integer N this algorithm must return the factors of N.
It consists of two parts:

1. A reduction of factoring problem to that of a period finding problem(Classical)
2. An algorithm to find the period (Quantum)

<u>Classical part:</u>
Pick a pseudo-random number g < N
Compute gcd(g,N) using the Euclidean algorithm to find if they share a common factor.

1. If gcd(g,N) != 1,then we can directly output factors as a=gcd(g,N) and b= $\frac{N}{a}$
2. If not, we have to transform this g into a no. that is more likely to share factors with N.

When gcd(g,N)=1, $g^p mod\ N = 1$.
$Implies,\ g^p - 1 = m.N$ for some integer m, p.
If we find p, then $g^{p/2} + 1\ and\ g^{p/2} - 1$ share factors with N and hence we can use the Euclidean algorithm to find the factors and break the encryption.

Problems that we encounter while finding p and the need for quantum computing:

1. The power p might be an odd no., p/2 will not be an integer and hence $g^{p/2}$ isn't a whole number which is not useful.
2. One of the numbers $g^{p/2} + 1$, $g^{p/2} - 1$ could themselves be a multiple of N, then the other no. will become a factor of m. These will not be useful.
3. Finding p for large values of g, N could take exponentially long time.

Quantum part: Shor's algorithm is probabilistic like most of the quantum algorithms. It gives the correct answer with high probability, and the probability of failure (here, the problems 1 and 2) can be decreased by repeating the algorithm.

We can notice that $f(x) = g^x \bmod N$ is a periodic function. We need to find the period of this function.

$$|x\rangle \longrightarrow \boxed{g^x} \longrightarrow |x, g^x\rangle \longrightarrow \boxed{Rem} \longrightarrow |x, r\rangle$$

Here, r is the value of f(x) obtained and the box refers to a quantum computer.

To compute the period of a function f, we evaluate the function at all points simultaneously (Quantum computer allows us to do this). We are left with a superposition of all states that lead to remainder r. And these states,by the definition of period, differ by p. But we cannot access this information directly. Because measurement of quantum information will give one of those values destroying the others.

Therefore we must transform this superposition into a state that will return p or 1/p(frequency). The best tool is Fourier Transform. The quantum fourier transform can be applied to this superposition which will destructively interfere leaving us a single state $\frac{1}{p}$ i.e the frequency. (Intuition: Fourier transform of an impulse train with period T: is a constant $\frac{1}{T}$.

$$|x\rangle + |x+p\rangle + |x+2p\rangle + \ldots\ldots \longrightarrow \boxed{QFT} \longrightarrow \left|\tfrac{1}{p}\right\rangle$$

From here we can retrieve p and hence factor the integer N.

Thus with the advent of quantum computing, classical cryptography methods are under risk and can be compromised. It is therefore essential to come up with new and better methods that are unbreakable even for quantum systems. This has led to the development of the field of Quantum Cryptography.
Quantum protocols make use of some of the quantum mechanics principles such as Uncertainty principle, Monogamy of entanglement, No cloning theorem to provide intrinsic security.

Quantum Key Distribution(QKD):

Quantum key distribution protocols follow directly from the No Cloning Theorem and State Collapse on measurement.
Say, Alice and Bob, want to communicate a secret message over an insecure channel (such as the internet). They need to encrypt messages. For that, Alice and Bob have to agree on a secret key allowing them to communicate using symmetric-key cryptography.

If Alice and Bob use a classical communication channel to share their key, it is impossible to tell if Eve (any 3rd party) has made a copy of this key for herself. However, in a quantum communication channel, Alice and Bob will get to know if Eve intercepted Bob's message before it gets to Alice. Here is how-

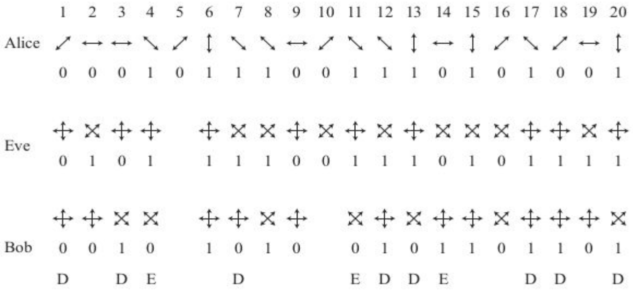
Steps:

Alice chooses a string of random bits, say 1000101011010100
and a random choice of basis for each bit, say ZZXZXXXZXZXXXXXX
Alice keeps these two pieces of information private to herself.

Alice encodes each bit using the corresponding basis string. Each qubit is in one of the states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$, chosen at random. In this case, the string of qubits would look like this:
$|-\rangle|0\rangle|+\rangle|0\rangle|1\rangle|0\rangle|1\rangle|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|0\rangle|+\rangle$ This is the message she sends to Bob.

Bob then measures each qubit he received from Alice. For measurement, he again uses a random set of bases. for example, he might use the bases:
XZZZXZXZXZXZZZXZ
And Bob keeps the measurement results private.

Bob and Alice then publicly share which basis they used for each qubit.
Alice: ZZXZXXXZXZXXXXXX Bob: XZZZXZXZXZXZZZXZ
If Bob measured a qubit on the same basis Alice prepared it in, they use the corresponding qubit to form part of their shared secret key. Otherwise, they discard the information for that bit.
Finally, Bob and Alice share a random sample of their keys, and if the samples match, they can be sure (to a small margin of error) that their transmission is successful. They have now agreed on a secret key.
Now how can they know if Eve intercepted the message?



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Alice	⤢	↔	↔	⤡	⤢	↕	⤡	⤡	↔	⤢	⤡	⤡	↕	↔	↕	⤢	⤡	⤢	↔	↕
	0	0	0	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	1
Eve	+	×	+	+		+	×	×	+	×	+	×	+	×	×	×	+	+	×	+
	0	1	0	1		1	1	1	0	0	1	1	1	0	1	0	1	1	1	1
	+	+	×	×		+	+	×	+		×	+	×	+	+	×	+	+	+	×
Bob	0	0	1	0		1	0	1	0		0	1	0	1	1	0	1	1	0	1
	D		D	E			D				E	D	D	E			D	D		D

Eve intercepts the message as it passes through her channel. She tries to measure the qubits in a random selection of bases, in the same way Bob would later on.

Now for a given qubit, If Eve's random choice of basis (Z) is not the same as Alice's (X) - this will change the qubit state from $|+\rangle$, to a random state in the Z-basis, with 50% probability of $|0\rangle$ or $|1\rangle$ as, $|+>=\frac{1}{\sqrt{2}}*(|1>+|0>)$

For Alice and Bob to use a qubit's result, they must both have chosen the same basis, say X. With Eve in the middle 3 cases can occur:

1. If Eve chooses X too, she will successfully intercept this bit without introducing any error. There is a $\frac{1}{2}$ chance of this happening.

2. If Eve chooses Z, i.e. a different basis to Alice and Bob: There is still a $\frac{1}{2}$ chance Bob will measure the value Alice was trying to send. In this case, the interception also goes undetected.

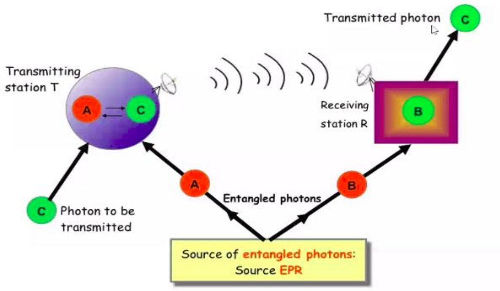
   There is a $\frac{1}{2}$ chance Bob will not measure the value Alice was trying to send, and this will introduce an error into their keys.

Thus the probability that in 1 bit, the error/ Eve's interception goes undetected = $\frac{3}{4}$

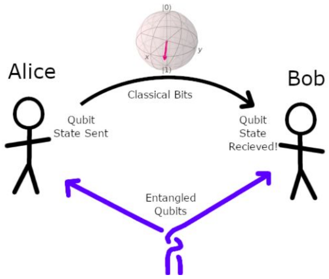
However if Bob and Alice compare 50 bits, the probability that Eve's interception is undetected = $\frac{3}{4}^{50}$ = 0.00006% !! So they can almost always be sure that they have been intercepted. Then they discard the transaction and start a new session.

Thus QKD protocol provides a Quantum secure way to share the key instead of RSA.

Quantum Communication



a. Quantum Teleportation:*CAN WE CHUCK COMMUNICATION??*



Quantum teleportation is a process by which the state of qubit ($|\psi\rangle$) can be transmitted from one location to another, using two bits of classical communication and a Bell pair. (maximally entangled pair)

Quantum no-cloning theorem stipulates that quantum states cannot be copied. The explanation being, while it does seem that entanglement between two particles helps transfer a qubit instantaneously across space, this interaction must begin locally. The two electrons must be entangled in close proximity before one of them is transported to another site. To complete the teleport,we need a digital message to interpret the qubit at the receiving end. Two bits of data created by measuring the first particle must be transmitted by a classical channel that is limited by the speed of light. When we measure a particle for this digital message, we destroy its quantum information at the initial position.

Thus, the protocol destroys the quantum state of a qubit in one location(Alice) and recreates it on a qubit at a distant location (Bob), giving rise to the term Teleportation!

Protocol:

Step 1:

The process begins with the creation of 2 entangled states: When the H-gate is applied to first qubit, it creates superposition and we get the state: $|0+>=\frac{1}{\sqrt{2}}*(|00>+|01>)$

Then CNOT gate is applied. The CNOT gate entangles both qubits, i.e. it flips the target if the control is $|1\rangle$.
ψ $0 = CNOT\frac{1}{\sqrt{2}} * (|00 > +|01 >) = \frac{1}{\sqrt{2}} * (|00 > +|11 >)$

The first qubit is sent to Alice and the second qubit to Bob. Alice has a qubit whose state she doesn't know. φ = a|0> + b|1> . She wants to send the state of the qubit to Bob through classical channels.

Step 2:
The starting state is the quantum state :
φ ⊗ ψ 0
$= \frac{1}{\sqrt{2}} * ((a|0 > \otimes(|00 > +|11 >) + (b|1 > \otimes(|00 > +|11 >)) = \frac{1}{\sqrt{2}} * (a|000 > +a|011 > +b|100 > +b|111 >)$

of which Alice controls the first two bits and Bob controls the last one. Alice applies a ***Cnot*** gate to the first qubit q1 , controlled by |φ⟩ (the qubit she is trying to send Bob). Then Alice applies a ***Hadamard*** gate to $|φ\rangle$. The identity gate I is present on the third bit as Bob has that qubit.

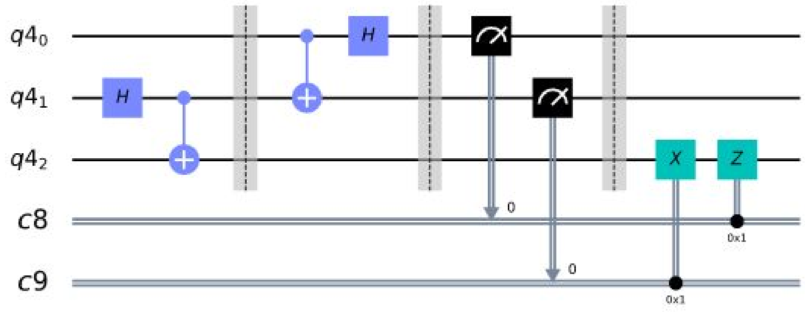
(H ⊗ I ⊗ I)(Cnot ⊗ I)(φ ⊗ ψ 0) $= \frac{1}{2} * (|00 > (a|0 > +b|1 >) + |01 > (a|1 > +b|0 >) + |10 > (a|0 > -b|1 >) + |11 > (a|1 > -b|0 >))$

Next, Alice applies a measurement to both qubits that she owns, $q1$ and |φ⟩, and stores this result in two classical bits. Now she may measure |00>, |01>, |10>, or |11> with equal probability. Depending on the result of the measurement, the quantum state of Bob's qubit is projected to a|0> + b|1>, a|1> + b|0>, a|0> − b|1>, or a|1> − b|0> respectively as q1 and q2 were entangled in the beginning.

When she measures the state, however, Alice irretrievably loses the state of $|φ\rangle$ as stated above. This in line with the **No cloning** theorem.She then sends these two bits to Bob.

Step 3: Bob, who already has the qubit $q2$, then applies the following gates depending on the state of the classical bits:

Classical bits received	State of q2 at B	Gate to retrieve $a|0 > +b|1 >$
00	$a|0 > +b|1 >$	I
01	$a|1 > +b|0 >$	X
10	$a|0 > -b|1 >$	Z
11	$a|1 > -b|0 >$	Y



Circuit:

Superdense coding:

Superdense coding is a procedure that allows someone to send two classical bits to another party using just a single qubit of communication. The superdense coding protocol can be thought of as a flipped version of the teleportation protocol. It demonstrates the exponential growth of quantum state spaces with the number of particles.

Protocol:

Step 1:
The process begins with the creation of 2 entangled states:
When the H-gate is applied to first qubit, it creates superposition and we get the state:

$$|0+>=\frac{1}{\sqrt{2}}*(|00>+|01>)$$

Then CNOT gate is applied. The CNOT gate entangles both qubits and results in a maximally entangled Bell state.

$$CNOT\frac{1}{\sqrt{2}}*(|00>+|01>)=\frac{1}{\sqrt{2}}*(|00>+|11>)$$

The first qubit is sent to Alice and the second qubit to Bob.

Step 2:

For Alice to send 2 classical bits of information to Bob using her qubit she needs to apply a set of quantum gates to her qubit. The gates depend on the 2 bits of information she wants to send.

Value to be encoded (2 bits)	Gate applied (only on q1, the other is always Identity gate I)	Resulting state ψ

00 encoded as 0	$\psi 0 = (I \otimes I)\psi\ 0$	$\frac{1}{\sqrt{2}}(\|00>+\|11>)$
01 encoded as 1	$\psi 1 = (X \otimes I)\psi\ 0$	$\frac{1}{\sqrt{2}}(\|10>+\|01>)$
11 encoded as 2	$\psi 2 = (Y \otimes I)\psi\ 0$	$\frac{1}{\sqrt{2}}(-\|10>+\|01>)$
10 encoded as 3	$\psi 3 = (Z \otimes I)\psi\ 0$	$\frac{1}{\sqrt{2}}(\|00>-\|11>)$

Step 3:

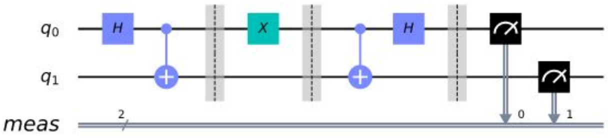
Alice then sends her qubit to Bob. Bob applies a control- NOT to the two qubits of the entangled pair as now he has both the qubits. Through this Bob can now measure the second qubit without disturbing the quantum state. If the measurement returns |0> then the encoded value was either 0 or 3 if the measurement returns |1> then the encoded value was either 1 or 2. Bob then applies H to the first bit.

The possibilities are below:

Entangled pair with B	After CNOT gate	First Bit	After H(First bit)	Second bit
$\psi\ 0$	$\frac{1}{\sqrt{2}}(\|00>+\|01>)$	$\frac{1}{\sqrt{2}}(\|0>+\|1>)$	$\|0>$	$\|0>$
$\psi\ 1$	$\frac{1}{\sqrt{2}}(\|11>+\|01>)$	$\frac{1}{\sqrt{2}}(\|1>+\|0>)$	$\|0>$	$\|1>$
$\psi\ 2$	$\frac{1}{\sqrt{2}}(-\|11>+01>)$	$\frac{1}{\sqrt{2}}(-\|1>+0>)$	$\|1>$	$\|1>$
$\psi\ 3$	$\frac{1}{\sqrt{2}}(\|00>-\|01>)$	$\frac{1}{\sqrt{2}}(\|0>-\|1>)$	$\|1>$	$\|0>$

Thus now Bob can measure both bits and decode the 2 classical bits of information sent by Alice.

Circuit:



Difficulties Faced:

A lot of operations now are limited by the no. of qubits that can be used. The reason is decoherence. While we can arrive at our results by observing the changes in our qubits. But qubits are extremely delicate. The state of the qubit may end up getting affected due to factors that we cannot observe, even observation might cause our wave function to collapse.

Fault tolerance is being able to control the "uncontrollable cascade of errors caused by the interaction of quantum-bits, as these concepts can be directly mapped to quantum information."

Until we are able to maintain coherence and achieve fault tolerance, the performance of quantum computers will be severely limited due to their high sensitivity to environmental disturbances.

New developments in the field, future possibilities:

Quantum computers are not a replacement for classical computers. They are not universally faster. They are helpful for special types of calculations where we can exploit the availability of all the quantum superposition states at the same time, places where computational parallelism is required. Every operation might in fact become slower, but the no. of operations required to arrive at the result is going to be exponentially smaller.

Resources:
https://www.nature.com/articles/s41534-018-0085-z
https://www.youtube.com/watch?v=QXJ96Kyt6TA
https://www.youtube.com/watch?v=lvTqbM5Dq4Q