

Name : Divas Subedi
Course Number : PHYS 232L
Course Name : Phys III : Optics and Modern Physics
Title of the paper : Quantum Computing/Encryption
Date of submission : December 9th, 2019

Abstract

With the rise of data science, particle physics, intensive drug research and other problems with higher complexity, the computational power of current computer is turning into a bottleneck. There is a need for more powerful and time-efficient computers. Current computing power limits the possibility of simultaneous non-sequential calculations. In this paper, the working principle of classical computers and quantum computers will be discussed. This paper sheds light on how quantum computing is not just the implementation of higher computational speed and higher memory capacity but rather a paradigm shift in the problem-solving approach. This paper also touches on the currently working quantum computers: Sycamore and IBM-Q. Basics of encryption and the principle behind widely used RSA encryption are illustrated. The efficiency of Shor's algorithm to factorize a large number is discussed. The future implementation of quantum computation in simulation, encryption and computer security is discussed.

Contents

1	Introduction	3
2	A brief Overview of Standard Model	3
2.0.1	Properties of Fundamental Particles	4
2.0.2	Quantum Superposition	4
2.0.3	Quantum Entanglement	4
3	Computation	4
3.1	Classical Computers	4
3.1.1	Classical Bit	5
3.1.2	Classical Gates	5
3.2	Quantum Computers	6
3.2.1	Qubit	6
3.2.2	Spin as qubit	7
3.2.3	Bloch Sphere	7
3.2.4	Quantum gates	9
3.2.5	Pauli Matrices	10
3.2.6	Practical Implementation of Quantum Computers	10
3.2.7	IBM-Q programming	10
3.2.8	Limitations of Quantum Computers	12
4	Encryption	12
4.1	Symmetric Encryption	12
4.2	Asymmetric Encryption	13
4.2.1	RSA Encryption	13
4.3	Shor's Algorithm	14
4.4	No Cloning Theorem in Encryption	15
5	Conclusion	15

List of Figures

1	The Standard Model of Particle Physics	3
2	Classical Logic Gates	5
3	Representation qubit in vector space of two states with probability of (a) 50/50 and (b) $ \alpha ^2/ \beta ^2$	7
4	A Bloch Sphere representing a qubit	8
5	(a) Code for the Adder (b) Circuit for the Adder	11
6	Histogram of state of the particles detected	12

List of Tables

1	Axes and superposition	8
2	CNOT gate	9
3	Truth table for Adder	11

1 Introduction

In 1980's, Paul Benioff described the first quantum mechanical model of quantum computing. He showed that computers could operate under the laws of quantum mechanics by describing Turing machine in Schrödinger's equation form. He laid the foundation of quantum computing and since then, numerous physicists and engineers have been working on this project to accomplish this huge undertaking. The notion of quantum computing is intriguing but also complex. Since quantum computers work at a quantum level with non-intuitive laws of nature, it is difficult to predict what happens and also exciting to see the new possibilities.

2 A brief Overview of Standard Model

In simple terms, the Standard Model is a periodic table of the elements for particle physics. It is a theory of physics that basically explains all the fundamental particles and their interactions.¹ It encompasses two basic ideas of physics:

1. every matter in the universe is composed of fundamental particles;
2. the particles interact with each other by exchanging a mediator particle associated with the force.

Figure 1 shows the family members of the Standard Model.

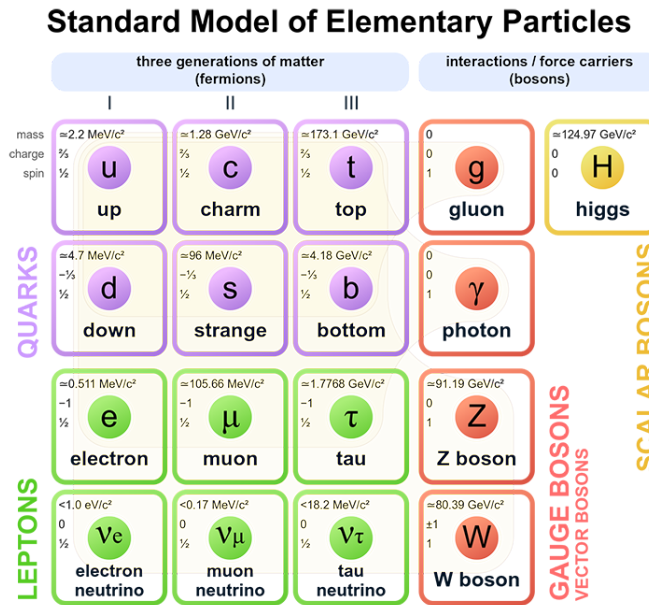


Figure 1: The Standard Model of Particle Physics

Source: Wiki-media

2.0.1 Properties of Fundamental Particles

The constituent particles in the model are distinguished in terms of their spin, mass, and the quantum numbers (charges) determining their interactions. It has been able to give a very comprehensive picture of all the fundamental constituents of matter. These properties of fundamental particles are what we use to represent information directly or in some manner. For example, the classical computer works with current and voltage which is eventually tied to the charge of particles. Spin is also one of the fundamental properties of the elementary particles. Spin is an intrinsic form of angular momentum carried by elementary particles, composite particles, and atomic nuclei.² It is being studied to be the basis for information in quantum computers.

2.0.2 Quantum Superposition

The properties of elementary particles are quantized. There is a discrete set of values that a physical property or observable of a particle can take. For example, the spin of an electron can be either $\frac{1}{2}$ or $-\frac{1}{2}$, the energy level of an electron in a hydrogen atom can be one of the principal quantum levels. However, the quantum state of the observable can also be a combination of those discrete values. Two or more quantum states can be added together or "superposed" to form another valid quantum state. Every quantum state can be represented as a weighted sum of two or more distinct states.³ When an observable is measured, the superposition collapses and the outcome is one of the discrete values. However, observation is not possible without interaction. It is analogous to a spinning coin in the dark, the only way to observe it is to smack a palm down on it, forcing it to be either heads or tails without knowing what was the orientation before. So, measuring particles forces the particle to take one of the quantum states.

2.0.3 Quantum Entanglement

Quantum Entanglement is the phenomena in which the fundamental property of two or more particle are not independent of each other. The combined state cannot be factored into the product of its constituents.⁴ For example, if a pair of electron is entangled, the spin of those electrons will be co-related. If the spin of one of the electrons is measured, the state of the other electron is also known with 100% certainty. The co-relation of their quantum state can not be explained by chance.

3 Computation

3.1 Classical Computers

Classical computer is the name given to the currently used binary computer. These computers undertake computation in binary level. The state of a binary digit in a circuit is fixed: either 0 or 1. The

3.1.1 Classical Bit

The name bit is a portmanteau of binary digit. It can be in either of two states: 0 or 1. There are various reasons why physicists and engineers decided 2 to be the base of the calculation. It was easier to encode in various different forms such as magnetization of disks, on and off state of the transistor, pits or land in optical devices. Generally classical computers use two different voltages: 0V and 5V as digital logic.⁵ Any two states can be represented as a binary. It can be a state of being charged or not, heads or tails of a coin, light polarized vertically or horizontally, or the spin of elementary particle. The necessary condition is that the two states should be **independent of each other**. In other words, if the states are represented as vectors, they should be orthogonal to each other in their vector space.

3.1.2 Classical Gates

In the lowest level, a classical computer uses logic gates, which are made out of CMOS transistors, to undertake simple computations. A combination of millions of gates can be used to make up an integrated circuit or microprocessor which can perform any classical calculation. Gates can also be used to make flip-flops and registers which makes up storage cells. There are 7 basic classical gates in total each with their own functionality: AND, OR, NAND, NOR, NOT, XOR, XNOR. All integrated circuits, microprocessors, SRAM are made using these gates. NAND and NOR are called universal gates as they can be used to replicate the output of every gate. Gates have one or two inputs and have one output. The truth table for NOT, OR, AND and XOR is given in figure 2. NAND, NOR, XNOR are just NOT combined with AND, OR and XOR combined respectively.

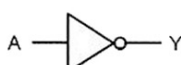
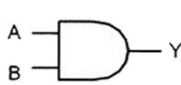
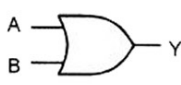
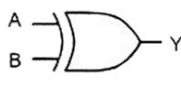
Logic function	Logic symbol	Truth table	Boolean expression															
Inverter (NOT gate)		<table><tr><th>A</th><th>Y</th></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table>	A	Y	0	1	1	0	$Y = \bar{A}$									
A	Y																	
0	1																	
1	0																	
2-input AND gate		<table><tr><th>A</th><th>B</th><th>Y</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	A	B	Y	0	0	0	0	1	0	1	0	0	1	1	1	$Y = A \cdot B$
A	B	Y																
0	0	0																
0	1	0																
1	0	0																
1	1	1																
2-input OR gate		<table><tr><th>A</th><th>B</th><th>Y</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table>	A	B	Y	0	0	0	0	1	1	1	0	1	1	1	1	$Y = A + B$
A	B	Y																
0	0	0																
0	1	1																
1	0	1																
1	1	1																
2-input EX-OR gate		<table><tr><th>A</th><th>B</th><th>Y</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table>	A	B	Y	0	0	0	0	1	1	1	0	1	1	1	0	$Y = A \oplus B$
A	B	Y																
0	0	0																
0	1	1																
1	0	1																
1	1	0																

Figure 2: Classical Logic Gates

3.2 Quantum Computers

Quantum computers are new types of computer which is still in the neonatal phase. It is a non-classical computer that works with qubits instead of bits. Quantum computers perform calculations based on the probability of an object's state before it is measured - instead of just 1s or 0s - which could mean that they have the potential to process exponentially more data compared to classical computers. Various mathematical algorithm relies on having the capability of simultaneous calculations which cannot be done in classical computers. The mathematics behind quantum computing is done in a different dimension and different space which means there are different properties of operation that are not found in the mathematics of classical computers.

3.2.1 Qubit

Unlike classical bits, quantum states like spin or energy level of an electron do not have to take one certain value. It can be in a superposition. As mentioned earlier, different states can be represented as orthogonal or orthonormal vectors. Those orthonormal vectors are the basis of the vector space where all possible states can be defined. While in superposition, its state can be described as a linear combination of the basis vectors. For example, let the state of hydrogen electron being in ground-level be represented by $|0\rangle$ vector and state of being in an upper energy level be represented by $|1\rangle$ vector. Here the vectors are written in Dirac notation. The vectors $|0\rangle$ and $|1\rangle$ are orthonormal. At any moment, the energy level of the electron is in superposition and probabilistic. Therefore, it is written as a linear combination of basis vectors. If the probability of the electron occupying those energy level are equal, the superposition can be represented by a vector $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. The reason for dividing them by $\sqrt{2}$ is that vector representing superposition should be ℓ^2 normalized. The qubit could be represented as in figure 3(a). Similarly, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as shown in figure 3(b) has α^2 probability of being in state $|0\rangle$ and β^2 probability of being in $|1\rangle$ state where α and β are complex number. The probability of the electron being in an energy level is now given by the square of magnitude the co-efficient associated with it. In this way, the energy level of an electron can be used as a qubit. Another example would be the polarization of light or spin of an electron.

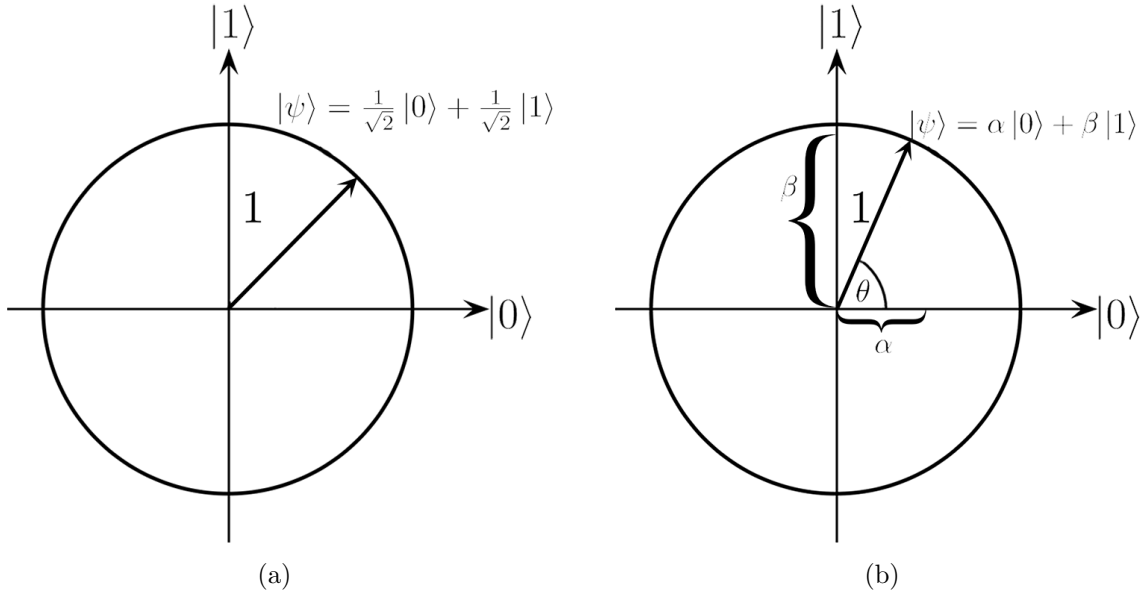


Figure 3: Representation qubit in vector space of two states with probability of (a) 50/50 and (b) $|\alpha|^2/|\beta|^2$

3.2.2 Spin as qubit

As stated earlier, the spin of an elementary particle is quantized. The spin of an electron can take one of two possible values or can be in a superposition of those quantum states. The SI unit of spin is the same as the classical angular momentum. Generally, it is represented by just a dimensionless spin quantum number by dividing the spin angular momentum by the reduced Planck constant \hbar . There is also a magnetic moment associated with an electron due to its spin. The Stern-Gerlach experiment showed that the intrinsic magnetic moment of particles is quantized and takes one of two values. So the spin can be either spin-up ($|\uparrow\rangle$), spin-down ($|\downarrow\rangle$) or superposition of two ($|\psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$). Hence, the spin can be used as a qubit.

3.2.3 Bloch Sphere

In figure 3, α and β have only the real part, but they can be complex. Here, the vector $|\psi\rangle \in \mathbb{C}^2$. To represent the entirety of the qubit, a four-dimensional figure is needed since each complex number is represented by a 2-dimensional complex plane. However, the constraint that $\alpha^2 + \beta^2 = 1$ makes it feasible to represent the vector in a 3-dimensional sphere. Each

complex number can be written in their Euler form $\alpha = r_\alpha e^{i\phi_\alpha}$ and $\beta = r_\beta e^{i\phi_\beta}$.⁶

$$|\psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$$

$$|\psi\rangle = r_\alpha e^{i\phi_\alpha} |\uparrow\rangle + r_\beta e^{i\phi_\beta} |\downarrow\rangle$$

$$|\psi\rangle = e^{i\phi_\alpha} (r_\alpha |\uparrow\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} |\downarrow\rangle)$$

The global phase $e^{i\phi_\alpha}$ is irrelevant as it doesn't affect any measurement

$$|\psi\rangle = r_\alpha |\uparrow\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} |\downarrow\rangle$$

Now since $r_\alpha^2 + r_\beta^2 = 1$, they can be written as $r_\alpha = \cos\left(\frac{\theta}{2}\right)$ and $r_\beta = \sin\left(\frac{\theta}{2}\right)$

Also taking the relative phase as $\phi = \phi_\beta - \phi_\alpha$

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |\uparrow\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi} |\downarrow\rangle$$

Now, this can be represented in a spherical co-ordinate system. This unit sphere is now called Bloch Sphere. Figure 4 shows a Bloch sphere. In the figure, it seems like $|1\rangle$ is antipodal to $|0\rangle$. However, they are still orthogonal in this space. Now, positive z-axis is $|\uparrow\rangle$ and negative z-axis is $|\downarrow\rangle$. X-axis is $\frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\rangle$, Y-axis is $\frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{i}{\sqrt{2}} |\downarrow\rangle$

Axis	$ \psi\rangle$
+X	$\frac{1}{\sqrt{2}} \uparrow\rangle + \frac{1}{\sqrt{2}} \downarrow\rangle$
-X	$\frac{1}{\sqrt{2}} \uparrow\rangle - \frac{1}{\sqrt{2}} \downarrow\rangle$
+Y	$\frac{1}{\sqrt{2}} \uparrow\rangle + \frac{i}{\sqrt{2}} \downarrow\rangle$
-Y	$\frac{1}{\sqrt{2}} \uparrow\rangle - \frac{i}{\sqrt{2}} \downarrow\rangle$

Table 1: Axes and superposition

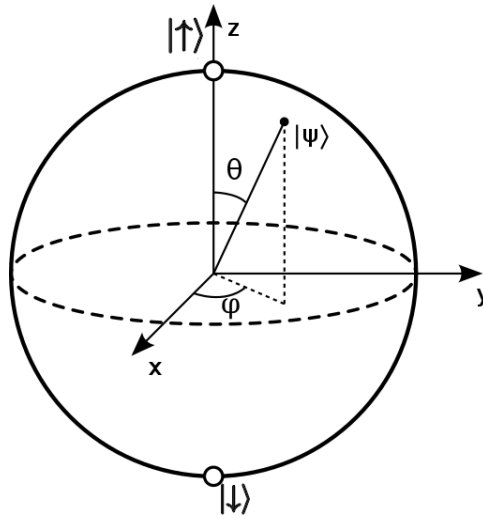


Figure 4: A Bloch Sphere representing a qubit

Source: Wikimedia

3.2.4 Quantum gates

Much like classical computer needs logical gates, quantum gates are need for quantum operations on a qubit. There are various Quantum gates. The quantum gates are implemented using matrices. The vectors $|\uparrow\rangle$ and $|\downarrow\rangle$ can be written as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ respectively as set of orthonormal vectors in \mathbb{R}^2 . Quantum gates performs an operation on a qubit which can be written as matrices. The matrices representing quantum logic are square matrix which means that the number of output is same as input. The matrices are unitary matrices (matrices whose conjugate transpose is also its inverse matrix). Few important gates are CNOT, X(bit flip) , Z(phase flip), Hadamard transformation. The X gate is similar to classical NOT gate. $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. When $|\psi\rangle = |\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$,

$$X |\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

If the quantum state is in superposition $|\psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$.

$$X |\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta |\uparrow\rangle + \alpha |\downarrow\rangle$$

So, the matrix rotates the Bloch sphere by π radians about the X-axis. H gate is another important gate which is represented by matrix $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. It rotates π radians about $\hat{x} + \hat{z}$ axis. It creates a superposition in which probability of each state is equal.

If there are more than one qubit, the state of two qubit is given by their tensor product. If $|\psi_1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ and $|\psi_2\rangle = \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$

$$|\psi_1\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} \alpha \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \\ \beta \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{bmatrix} = \alpha\gamma |\uparrow\uparrow\rangle + \alpha\delta |\uparrow\downarrow\rangle + \beta\gamma |\downarrow\uparrow\rangle + \beta\delta |\downarrow\downarrow\rangle$$

If $|\psi_1\psi_2\rangle = \eta |\uparrow\uparrow\rangle + \lambda |\downarrow\downarrow\rangle$, it is impossible to factorize. This state is called bell state also called maximally quantum entangled state.

One of the important two-qubit gates is CNOT. CNOT is similar to classical XOR, CNOT (cX) is conditional not — it flips the bit according to the control bit. If the control bit is $|\downarrow\rangle$, then it flips the bit or else leaves as it is.

Control _{in}	Target _{in}	Control _{out}	Target _{out}
$ \uparrow\rangle$	$ \uparrow\rangle$	$ \uparrow\rangle$	$ \uparrow\rangle$
$ \uparrow\rangle$	$ \downarrow\rangle$	$ \uparrow\rangle$	$ \downarrow\rangle$
$ \downarrow\rangle$	$ \uparrow\rangle$	$ \downarrow\rangle$	$ \downarrow\rangle$
$ \downarrow\rangle$	$ \downarrow\rangle$	$ \downarrow\rangle$	$ \uparrow\rangle$

Table 2: CNOT gate

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

If the Target_{out} bit is examined, its output is same as $\text{Target}_{in} \text{ XOR } \text{Control}_{in}$. Combinations of quantum gates can be used to mimic all the classical operations and create newer non-classical operations.

3.2.5 Pauli Matrices

Pauli Matrices are matrices associated with quantum gates that rotates the Bloch sphere by π radians about different axes. There are 3 such matrices as there are three axes of rotation. They are Unitary and Hermitian (those matrix whose conjugate transpose is itself). Those three matrices are:

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

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

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

3.2.6 Practical Implementation of Quantum Computers

Even though quantum computing is still in its infancy, there are a lot of proposed theories backed by mathematics and physics on what a sophisticated computer can do ranging from factorizing large prime number, creating truly randomized numbers, simulating DNA, complex protein molecules. With the rise of data science and machine learning which require huge amount of computational power, classical computers might turn into a bottleneck. It is predicted that If a sophisticated enough quantum computer was built, it would boost the development in machine learning.

3.2.7 IBM-Q programming

Quantum Supremacy is a milestone which marks a quantum computing surpassing the fastest classical computer in at least one problem. This has not been achieved but different tech business has been tried to achieve it. IBM-Q is the 16-bit quantum computer that is available for everyone to use for free. IBM-Q also supports Qiskit. Qiskit is an open-source framework for quantum computing. It provides tools for creating and manipulating quantum programs and running them on prototype quantum devices and simulators. In order to test the simulation, quantum adder circuit was designed which could add three qubits. The code for the program is given in figure 5. Table 3 shows the expected output in traditional binary form. In the table, the output is 00 for 1 instance, 01 for 3 instances, 10 for 3 instances, and 11 for 1 instance. In the implementation of the adder circuit, all of the input qubits start

from $|0\rangle$. Hadamard transformation is applied to all input qubits so the input to adder is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Here, for each qubit the possibility of being $|0\rangle$ or $|1\rangle$ is equal, so there is no biasness. 4096 qubits are passed through the circuit and carry and sum qubit are measured. From the table, it can be expected that 1 out of 8 qubit set would yield $|00\rangle$, and 3 out of 8 will yield $|01\rangle$, 3 out of 8 will yield $|10\rangle$ and remaining eighth will yield $|11\rangle$. The figure 6 shows the prediction is true.

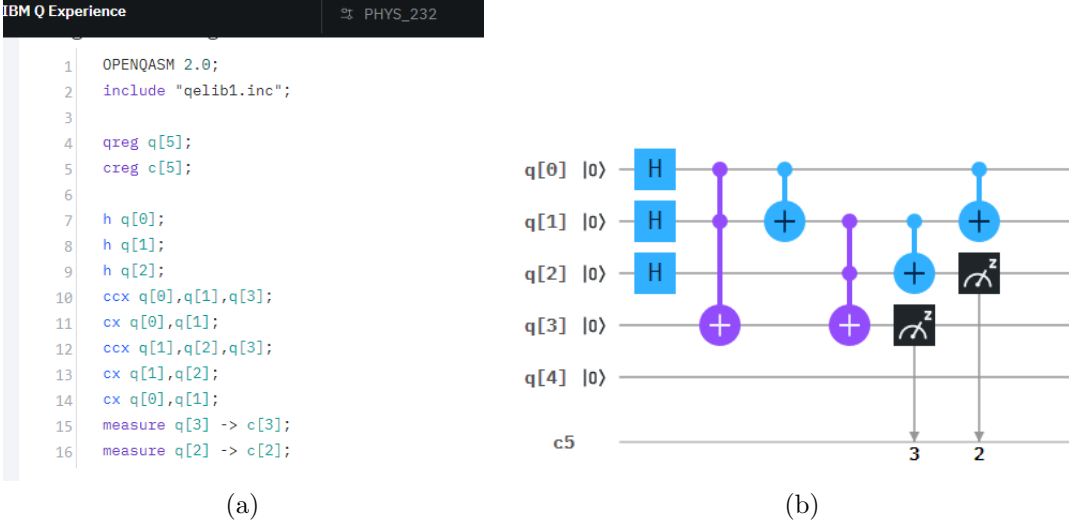


Figure 5: (a) Code for the Adder (b) Circuit for the Adder

Table 3: Truth table for Adder

Input1(q[0])	Input2(q[1])	Input3(q[2])	Carry(q[2])	Sum(q[3])
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

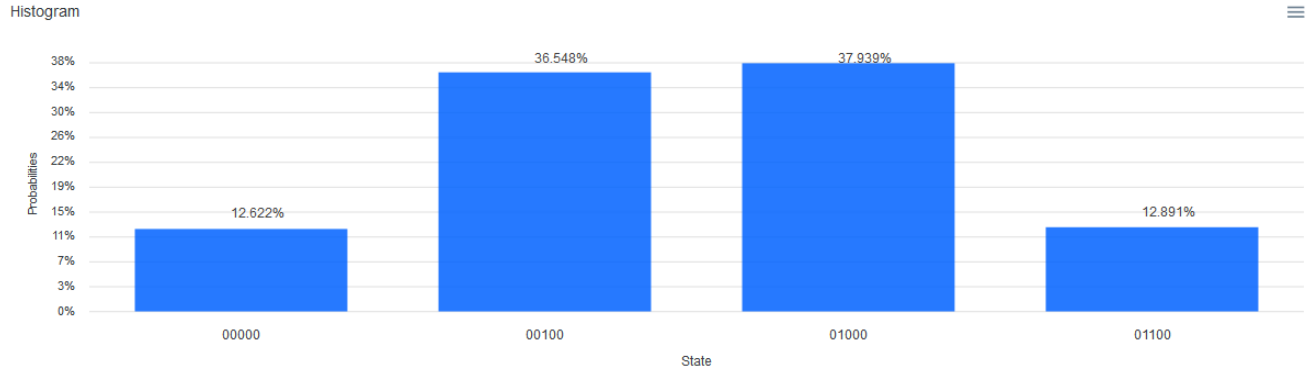


Figure 6: Histogram of state of the particles detected

3.2.8 Limitations of Quantum Computers

Quantum Computing has a lot of potentials but implementing it is very difficult. Building quantum computing is like building the perfect computer out of the all imperfect part.⁷ A quantum computer is very sensitive to perturbation and noise due to the environment. The quantum computer needs to be in a very low-temperature setting which requires a expensive Dilution refrigerator. The fault tolerance of quantum computing is slim. There are chances that a qubit carrier is lost or information carried is lost.⁸ Decoherence is a problem as well. If the quantum gates are not faster than the decoherence time, information is lost. The technology is still very frail. The current stage of quantum computing is analogous to the vacuum tube stage of classical computers.

4 Encryption

Encryption is a process of scrambling the data in such a manner that it is incomprehensible to anyone without the proper key and method of unscrambling it. A simple example of the encryption of a message might be shifting every letter to the next letter. "HELLO" would be "JFFMP" and the intended receiver should the key that is shifting the letter to the previous one. In networks, messages and information are encrypted before sending so that any eavesdropper might not replicate, change or misuse the data. There are various ways of encrypting a piece of information. In computing and network, a piece of information would generally mean any type of data in its binary form or its decimal equivalent. Classical encryption can broadly be classified into two categories: Symmetric and Asymmetric.

4.1 Symmetric Encryption

As the name suggests, the process of encrypting a piece of information and decrypting the cipher is symmetric. The same key is used for encrypting and decrypting. For example, if a system involves three people: Alice, Bob and Charlie, each pair need to have their unique key. Alice and Bob share a key that is unknown to Charlie. Alice and Bob each have a shared key with Charlie unknown to the other. If Dave joins the system, now Dave needs to

have a shared key with everyone. So, the number of keys keep on increasing. For a system with n members or nodes, there needs to be $\binom{n}{2}$ keys. Now, if Charlie knows key shared by Alice and Bob, he can view the data, he can change it and send it as Alice or Bob. Breaking into encryption is not simple, the algorithm to implement the encryption is really advanced. Symmetric encryption is relatively faster compared to the asymmetric encryption. But, they are not entirely reliable.

4.2 Asymmetric Encryption

As the name suggests, the process of encrypting a piece of information and decrypting the cipher is asymmetric. Different keys used for encryption and decryption. This means every individual needs to have two keys: private and public. The private key is supposed to be kept secret by the individual and the public key is shared with everyone in the system. For a system of n nodes, the required amount of key is $2 \cdot n$. The specialty of the asymmetric encryption is that they come in pairs and data encrypted by one key can be decrypted if and only if decrypted by its pair. A message encrypted by the public key can be decrypted by its private key only and vice-versa. Not even a private key can decrypt its own encryption. Now, if Alice wants to send Bob a message, she uses Bob's public key to encrypt the message and sends it. She can be sure that no one except Bob can read the message as only Bob has the private key. Another example of its implementation: Evan wants to send a message to the entire group and wants to be sure that the message is unaltered, he can encrypt the message using his private key. Everyone with his public key would be able to decrypt it and can be certain that Evan sent it. An encrypted message can be further encrypted using a different key. For example, if Alice wanted to send a message to Bob and Bob wants to be entirely certain that it was Alice who sent the message, Alice can first encrypt the message using Bob's public key so no one except Bob can access it. After the first encryption, she can further encrypt the encrypted message using her private key. So, now Bob is entirely sure the message was from Alice and the communication is secure. This forms the basis of the digital signature that is used to verify the authenticity of digital documents.

4.2.1 RSA Encryption

RSA (Rivest–Shamir–Adleman) is an example of an asymmetric encryption algorithm. The algorithm is pretty straight forward to use. This algorithm relies on the fact that factoring a large number if the number only has two prime factors, is a very complex computational work. Since it is asymmetric encryption, a pair of key is generated. This is done by the following process:

1. Choose 2 random prime number p and q
To make the calculation simple, $p = 11$ and $q = 13$
2. Now, $n = p * q$. This is the max range of data that can be encrypted
 $n = 17 * 23 = 391$
3. Calculate the totient: $\phi(n) = (p - 1) * (q - 1)$
 $\phi(391) = 16 * 22 = 352$

4. Choose e that is co-prime of $\phi(n)$
Let $e = 13$
5. Now calculate d such that $de \bmod \phi(n) \equiv 1$
 $d = 1381$. Since $1381 * 13 = 17953$ and $17953 \bmod 352 = 1$
6. The keys are generated. One of them is $(n, e) = (391, 13)$ and the other is $(n, d) = (391, 1381)$.

Given that, p and q are huge number, even if public key and the entire algorithm is known to someone, it is almost impossible to figure out the private key. Now, if the message to be sent is , following process is followed for encryption and decryption:

1. $c = m^e \bmod n$
For example $m = 42$, $c = 42^{13} \bmod 391 = 145$. 145 is the cipher message
2. $m = c^d \bmod n$
 $m = 145^{1381} \bmod 391 = 42$

In real-life applications, p and q are huge numbers. They use 512-bit numbers for p and q meaning each number is over at least $2^{400} = 10^{120}$. The computation with numbers with hundreds of digit is very difficult and even the fastest of classical computer might take years to break one pair of asymmetric keys.[?]

4.3 Shor's Algorithm

Shor's Algorithm was developed by Peter Shor in Bell's Lab. The algorithm is an approach to factorize a large number into its prime factor. It consists of five stages – one of which requires a Quantum Computer. This algorithm takes advantage of modular periodicity and quantum Fourier transform.^{9 10} It consists of the following steps:

1. To factorize N , choose a random integer $m < N$, such that they are co-prime
Let the number to be factorized $N = 21$, and the random chosen number $m = 2$
2. Use quantum computer to determine the unknown period P of the function using QFT
 $f_{m,N}(x) = m^x \bmod N$
Using simple calculation in this case, P is found to be 6.
3. If P is odd, repeat from Step 1, else proceed
4. If $m^{P/2} + 1 = 0 \bmod N$ then, go to Step 1
If $m^{P/2} + 1 \neq 0 \bmod N$ then, goto step 5
 $2^3 + 1 = 9 \neq 0 \bmod 21$
5. Compute $d = GCD(m^{P/2} - 1, N)$
 $GCD(7, 21) = 7$
6. Answer is d .

4.4 No Cloning Theorem in Encryption

Quantum measurements are destructive, in the sense that they alter the state of the system measured. When an observable of a system is measured, the superposition it was in previously collapses. Therefore, it is impossible to measure and copy a qubit. This property can be advantageous in computer networking and data security. BB84 is a quantum cryptography protocol that uses the fact that When the photons passing through the filter are aligned at the same angle or orthogonal to the angle of the filter, the photons exhibit the deterministic behavior, but when it is at an angle, it shows probabilistic behavior. BB84 is used to share an encryption key through a secured quantum channel. Due to no-cloning theorem, if the quantum information sent was observed the keys are not consistent which will make the communication invalid and the session ends.¹¹

5 Conclusion

The theoretical potential of the quantum computer is huge. The mathematical algorithm based on quantum computation shows promising possibilities. The unique ability to work in quantum level of nature makes it very powerful. For the time being, classical technology can manage any task thrown at a quantum computer. Even if quantum computers were to come to complete fruition, it would not be for general purpose for years to come. Not everybody is convinced that quantum computers are worth the effort. Some mathematicians believe there are obstacles that are practically impossible to overcome, putting quantum computing forever out of reach.

References

- ¹ The standard model of particle physics | symmetry magazine.
<https://www.symmetrymagazine.org/standard-model/>.
- ² Eugen Merzbacher. *Quantum Mechanics (3rd ed.)*. 1998.
- ³ PAM. Dirac. *The Principle of Quantum Mechanics (3rd Edition)*. 1947.
- ⁴ N. Bohr. Can quantum-mechanical description of physical reality be considered complete. 48:696–702.
- ⁵ Ting-Chung Wang. Case-based instruction of ”how computer works” courses for high school students. In *2015 International Conference on Learning and Teaching in Computing and Engineering*, pages 207–208.
- ⁶ Ian Glendenning. The bloch sphere. QIA Meeting, TechGate, European Centre for Parallel Computing at Vienna.
- ⁷ The limits of quantum computers, nature. <https://www.scientificamerican.com/article/the-limits-of-quantum-computers/>.
- ⁸ Rodney Van Meter, Thaddeus D. Ladd, Austin G. Fowler, and Yoshihisa Yamamoto. Distributed quantum computation architecture using semiconductor nanophotonics. 08(1):295–323.
- ⁹ Erik Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O’Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and John M. Martinis. Computing prime factors with a josephson phase qubit quantum processor. 8(10):719–723.
- ¹⁰ P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.
- ¹¹ Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. 85(2):441–444.