Quantum Computing

Yusuf Shaik

Abstract- This research report will thoroughly explain quantum computing and the natural laws of physics behind it. It will go over the basics of bits, and quantum bits, then explain the laws of quantum physics that relate to quantum computing such as entanglement, superposition, and Heisenberg's uncertainty principle. Those laws will then be related to quantum computing and their importance will be signified. The laws will then be applied to quantum computing and theoretical applications of quantum computing will be explored. Although some laws make quantum computing seem impossible, there are ways around them that actually make it possible, and those laws will be explored. Only after the laws are examined and related to quantum physics, will the history be explained because it contains information that can only be properly understood after understanding the previous sections. This paper will discuss the history of quantum computing such as the contributions of Alan Turing and Richard Feynman. Finally, real applications such as the quantum computer by IBM will be explained, as well as possible future applications that could make an impact on the world.

I. INTRODUCTION

A. What is Quantum Computing?

Quantum computers are devices that rely on the principles of quantum physics rather than classical bits. They originated when Richard Feynman hypothesized that we would be able to use them to model more complex situations. Current computers (referred to as classical computers) rely on classical bits which can either be a 0 or a 1. However, principles of quantum mechanics such as entanglement, superposition, and spin, allow the use of quantum bits to perform much more processing intensive tasks. Quantum bits, or "qubits" can not only exist as a 0 or 1, they can exist at all states in-between as well (Computers that take advantage of this are referred to as quantum computers). When two qubits are "connected" or entangled, they inherit certain properties relative to each other. A state is any possible configuration of an item at a point in time. For example, a hole can be one state, while the filled in hole can be another state. Similarly, a 0 can represent one state, while a 1 represents another state. This is one of the fundamentals in beginning to understand quantum computing.

II. BITS

B. Bits and Qubits

To understand the mechanisms of quantum computing, one must first begin to understand how classical computers work. In the model of a classical computer, information is stored in the most fundamental building block of information, the bit. A bit can be either a 1 or a 0, and there is no state between changing from 0 to 1 or vice versa, only the 2 states themselves. With classical computing, since information can be stored as a 0 or a 1, we have 4 total possibilities with 2 bits of information: 01, 10, 00, and 11. However, in quantum computing we have qubits which can not only be 0 or 1, they can also be every value in-between. The in-between values are called a superposition state. A good comparison of bits to qubits is; a bit can be thought of as a 2D circle where one side is a 0, and the other side is a 1. The 2D circle can only have 1 face facing up at a time. Whereas a qubit can be imagined by a 3D sphere, where the north and south ends are 0 and 1 respectively. This 3D sphere has a multitude of spaces all over the sphere which allows the qubit to hold much more information than a classical bit [1]. This is useful because rather than encoding information into 2 bits, it now becomes possible to encode a lot more information because the bits can exist at any superposition of $|0\rangle$ or $|1\rangle$.

C. What Exactly Is A Qubit?

Qubits can be any elemental particle such as a photon with its polarization indicating whether it's a 1 or a 0, or even an electron with its charge indicating its bit value. Photons can be polarized at any angle, so from this we can realize the photon can exist in a superposition state where its polarization can be any value [2]. Similarly, we think of a qubit as an electron in a magnetic field, its spin can either align with the direction of the magnetic field, or be directly opposite

to it. The only way to change it, is to apply a certain force. Let's say a force of 1 unit is required to move the electron from an up spin to a down spin, if we apply half a unit of force, the electron now becomes in a state of superposition, and behaves as if it were in both states simultaneously [3].

D. Qubits and Quantum Computing

Why is this important? Well with qubits, in a quantum computer, any operation done on qubits, operates on the two separate bits at the same time. However, with classical bits, operations cannot occur on multiple bits simultaneously as they do with qubits. This grants quantum computers a huge advantage over classical computers for certain tasks [4]. These specific tasks are tasks that require multiple calculations at once. For example, if we were to use a classical computer to find a way out of a maze, it would try each possible solution until it found a correct way out of the maze [5]. However, if we were to use a quantum computer for the same task, the quantum computer would try all possible solutions at the same time, and find a solution much faster than the classical computer. Since each bit can be one of two values (zero or one), for n bits, there are 2^n possibilities that the bits could configure themselves into. Even when using qubits, there are actually 2^n possibilities as well. However, with qubits, due to superposition all those 2^n possibilities can exist at the same time. Thus, allowing for faster information processing [4]. Essentially, qubits are much faster at solving complex equations because they can run multiple calculations parallel to each other, unlike regular bits.

III. QUANTUM MECHANICS AND QUANTUM COMPUTING

E. Superposition

To delve deeper into the realm of quantum computing, we must first attempt to understand some basic quantum mechanics principles. We know that electrons and photons have a spin which is either up or down. However, the spin of the particle can be partly up and partly down at the same time. Similarly, qubits can be in multiple states at a time. This state, known as the superposition state, is a linear combination of the two binary states, and is mathematically indicated by a coefficient multiplied by each up or down spin as shown below:

$$|\Psi\rangle = \alpha|0\rangle + |\beta\rangle$$

(Equation 1)

Where $|\Psi\rangle$ is the linear combination of the 2 binary states, and alpha and beta are complex numbers. Although the qubit can actually be in multiple states at once, due to known laws of quantum mechanics, we cannot accurately measure the qubit in all those states. We can however, measure the probability that a qubit in superposition can be found in a certain state. Using the formulas indicated below, we can accurately depict the probability of finding the qubit in either state $|0\rangle$, or $|1\rangle$:

$|\alpha|^2$= Probability of finding the qubit in state $|0\rangle$

$|\beta|^2$= Probability of finding the qubit in state $|1\rangle$.

[6]

F. Heisenberg's Uncertainty Principle

Heisenberg's uncertainty principle states that you cannot measure a subatomic particles position and velocity at the same time without great uncertainty. The only way found to measure the velocity and position of a particle is to hit it with a photon, and then observe where the photon lands on the detecting device [7]. However, by hitting the subatomic particle with the photon, the velocity of the particle is now changed so the measurement of the velocity of the particle is now inaccurate. Similarly, Schrodinger's theory suggested that an object can exist in multiple states at once, and only by measuring it does it actually inhabit one state. The famous theory of Schrodinger's cat can be observed; if a cat is in a box and there exists a radioactive element that is decaying, and as soon as it decays the toxin will be released in the box, killing the cat [8]. According to Erwin Schrodinger, the cat is both alive, and dead at the same time. The only way to determine its state is to open the box and observe its state. Similarly, a qubit can exist in all possible states at once, and the only way to determine its state is to observe it. Before observing the qubit, it can exist as $|0\rangle$, $|1\rangle$, or any combination of the two: $|\Psi\rangle$ (superposition state). However by observing its state, it must now inhabit either the 0 or 1 state. So by attempting to measure the superposition of the qubit, it reverts back to its original 0 or 1 state, thereby losing all previous information. This seems complex to understand at first but its relation to quantum computing is of utmost importance. Due to this observer effect, quantum computers seem to be

impossible to create with our knowledge at the moment. This creates more questions; how is it possible to measure the information on a qubit without changing the information within it? The answer lies quantum entanglement [9].

G. *Quantum Spin*

What we need to realize about "quantum spin" is that particles are not actually spinning, they have an angular momentum and an orientation in space. We can measure "spin" of a particle by measuring it in a direction lol. If the direction of measurement is aligned with the direction of motion of a particle, we say it has an "up spin", if the direction of measurement is opposite to the direction of motion, we say it has a "down spin". The particle must now either be aligned with the direction of measurement or opposite of it after is measured [10]. However, this creates a new question: what if the measurement is taken at an angle compared to the direction of motion of the particle? A simple trigonometric function can be used to calculate the probability of finding the particle in each state. For example, if the measurement is taken at a 90 degree angle to the particles direction of motion, there is a 50% chance that it will be aligned in the direction of measurement, and 50% chance that it will be opposite to the direction of measurement. The trig function used is shown below with an example for a 90 degree angle:

$$p = \cos^2\left(\frac{x}{2}\right)$$

(Equation 2)

$$90^0 = \frac{\pi}{2}$$

$$p = \cos^2\left(\frac{(\pi/2)}{2}\right) = 0.5$$

$$0.5x100\%=50\%0.5x100\% = 50\%$$

[10]

- Therefore, there is a 50-50 chance that the particle will spin up, or spin down.
- Keep in mind that the angle must be in radians for this function to hold true.

Although the example only shows the equation for 90 degrees ($\frac{\pi}{2}$ rad), the function can be used to measure the probability at any angle. As seen in the example above, the probability actually measures the outcome, so therefore the "outcome" spin will now end up being different than the "input" spin. By using this trigonometric equation, we can see that measuring a particle in any direction, can actually change its direction of motion. This follows Heisenberg's uncertainty principle that states that a particles motion cannot be measured without altering its orientation and vice versa [11].

H. *Quantum Entanglement*

The law of conservation of momentum states that the total momentum of the universe must remain constant. If we consider two particles created from energy, and we know that the law of conservation of momentum must hold true, it follows that the spin of each of these particles must be opposite so that the momentum of the universe remains constant. So, if a particles direction of motion is aligned with the direction of measurement A, the other created particle measured in direction A must be opposite to the direction of measurement. This holds true for particles that are measured at angles as well. From this, we can conclude that the particles don't actually have an inherent property of "spin" itself, in reality, they are "connected" in a sense such that whichever spin particle A has, particle B must have a spin in the opposite direction. Distance is not a factor here because the particles are actually "entangled" together, they're not transmitting information across space. Therefore, the "information" is actually passed faster than the speed of light. When two particles are connected in this manner, it is referred to as quantum entanglement [11].

IV. APPLYING QUANTUM MECHANICS TO COMPUTING

I. *Measuring Information in Qubits*

In classical computing when we have 2 classical bits, we have four possibilities: 01, 10, 11, and 00, and all you need to determine the information encoded in the two bits, are the values of the first and second bit. In quantum computing however, we must recall that measuring a quantum particle actually changes it, so we can't actually measure the value of a qubit in superposition without it reverting back to a 0 or a 1. We need to realize that for quantum particles such as electrons we actually have four possible states with two particles. The major difference is, the up-down spin, and down-up spin are not the natural states in quantum computing unlike classical computing.

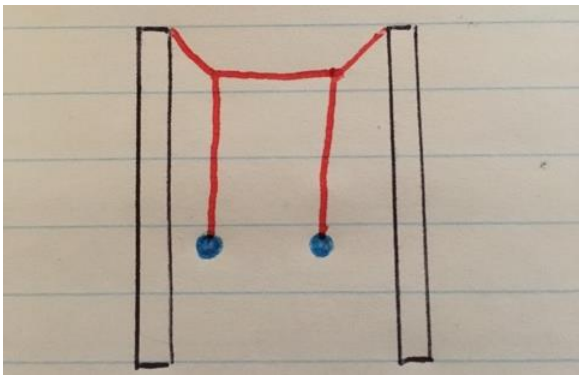
Due to entanglement, we have the following as our four states:

$$|\uparrow\uparrow\rangle, |\downarrow\downarrow\rangle, [\frac{1}{\sqrt{2}}]^*|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle, \text{ and } [\frac{1}{\sqrt{2}}]^*|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle$$

With upward facing arrows. Indicating spin up, and downward facing arrows indicating spin down. The first and second options are simple, the two upward facing arrows indicate that both electrons have spins in the same upward direction, and the two downward facing arrows indicate that both electrons have spins in the same downward direction. The second two possibilities are a bit more complex. In the superposition state, each electron does not have a direction of its own. They have opposite spins from each other and the spin of one electron is dependent on the spin of the other; this is known as entanglement. Without being measured, they exist in a state of superposition, and only when the particle is measured, can we find out the spin of the other electron. How does this explain the last two complex states? Well since the particles are entangled, the motion of one is dependent on the motion of the other. So, in the state of superposition, if a particle's spin is up-down, and the spin of one particle changes, the spin of the other particle must change to the opposite direction. This is shown as the third possible and fourth possible states from above:

$$[[\frac{1}{\sqrt{2}}]^*|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle \text{ and } [\frac{1}{\sqrt{2}}]^*|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle$$

A much simpler way to understand this topic is by modelling it with Newtonian physics. An astounding example was presented by Doctor Andrea Morello, professor of electrical engineering and telecommunications. His example put into perspective a special double pendulum. A string hung from the top of two vertical rods, has two strings hanging from it, each with its own wooden ball (Diagram Below).



(Diagram 1)

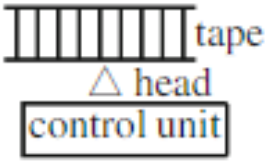
If the first wooden ball is pushed, it swings back and forth, eventually slowing down, while the second ball begins to move. After a while, the second ball slows down and the first one speeds up again. This process would continue on forever in a perfect pendulum. The switching from one swinging ball to the other is indicated in the third and fourth states shown above [12]. Thus, the way to measure the spin of an entangled particle, is by measuring its partner, and knowing that the partner has the opposite spin of whatever the original particle had. Quantumly entangled particles actually hold information in both of them, and the only way to retrieve understandable information from a quantamly entangled particle *A*, is to also retrieve the information from its quantamly entangled partner *B*. If only particle *A* is measured, or only particle *B* is measured, the information read from them is random [13]. The reason for this is that in quantamly entangled particles, the information is not in the particle itself, it is rather hidden within the correlation between the two particles [14]. Therefore, in quantum computers we can measure the correlation between two entangled particles, and get the information stored within them.

V. HISTORY

J. Model of a Quantum Computer

Alan Turing, known as one of the founders of modern computing, created the Turing model for a computer which required only a pen and paper. Pictured below, the model consisted of three components, a tape, a head, and a control unit. The tape was of infinite length in each direction, and it was split up into compartments called cells. In each cell, only a symbol could be written inside of it. Since the tape has an infinite length, it therefore had infinite states. The closest

similarity to today's computers is storage (where each cell having a symbol in it or not having a symbol in it indicates a 0 or 1). The head can read each cell on the tape, or write information on the cell. The control unit has finite memory, stores the current state of the machine, and computes the instructions by changing its state and the state of the head. This is closest to a CPU in today's computers [15].



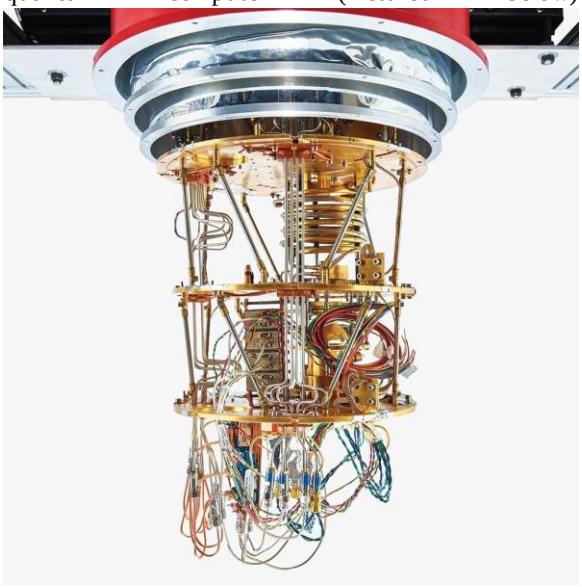
(Diagram 2 [15])

After years of progression with the classical computer, scientists began using them to model certain systems in a lab because in reality, computers evolved to do these calculations much faster than humans. Eventually, a physicist named Richard Feynman asked the question: "Can a classical, universal computer simulate any physical system? And in particular, what about quantum systems?" [16]. As we know, particles in quantum superposition can exist in multiple states at once. We also know that in different states, they'll have different information, and there is a way to calculate the probability that we find a particle at a certain state. The last thing to keep in mind is that with multiple electrons, we'll have to keep track of not only 2 probabilities, we will have to keep track of 2^n probabilities where the exponent n is the number of electrons used. This becomes extremely difficult to do with more electrons because for only 50 electrons, we would have to keep track of $1x10^{15}$ probabilities. This would be impossible for a classical computer, so Feynman came up with the idea that; instead of using classical computing to model quantum physics, we should use quantum computing [16].

VI. APPLICATIONS

K. What Is Going On At The Moment?

Currently, IBM has successfully developed a 16 bit quantum computer (Pictured below)



(Picture 3 [17])

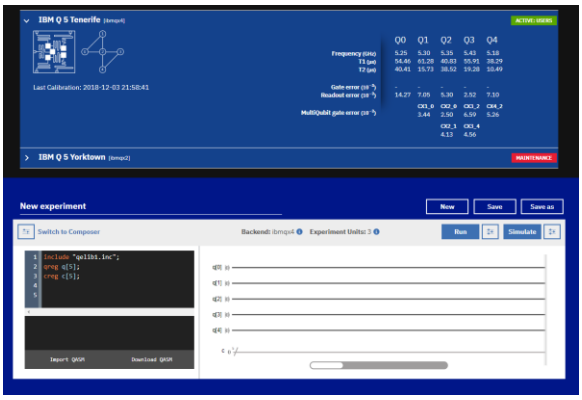
The quantum computer uses superconductors as qubits, which are cooled to below 1 Kelvin. Just like how current computers work by either sending an electric pulse through a wire to represent a 1 or 0, quantum computers use superconductors. Since electric current can flow through superconductors with no resistance at low temperatures, quantum algorithms can flow through undisturbed. In this case the qubit (pictured below) is a one inch long object made from synthetic material that allows for microwave photons to send the junction point of the "Y" shape into superposition. If microwave photons are sent into the "Y" junction of 2 qubits at the same frequency, those qubits can become entangled. Since the junction is now in superposition, it obeys laws of quantum mechanics and is therefore susceptible to interference as well[17].

(Picture 4 [17])

These machines must be kept at extremely low temperatures (around 0.01 Kelvin) in order to work because at the quantum state, the smallest bit of destructive interference could cause the quantum computer to proceed in an unwanted manner. Similarly, scientists can use constructive interference to "edge" the computer in the way they want [18]. However, since we know that qubits allow for a computer to apply an operation to different variables simultaneously 2^n times, we can realize that a qubit and a classical bit will not vary at all if we only have a single qubit or classical bit. Thus, we can realize that we need more than one qubit to complete complex tasks. This quantum computer built by IBM has 50 qubits, which allows for the computer to solve a problem trying 1,000,000,000,000,000 options at once. That means, if there is a maze with 1,000,000,000,000,000 possible outcomes, the quantum computer would be able to find the correct pathway out of the maze in the same time that it takes for a classical computer to attempt one pathway.

The most interesting thing about this quantum computer that IBM is developing, is that it is actually available to the public via the cloud. Any person can access this computer and IBM actually encourages it because they believe that the only way to generate ideas on how quantum computers would be effective, is if the public has access to it and they find new ways to work with it. The quantum computer can be used in one of two ways, either the user uses the composer (picture 5) which works with gates, or the user uses the quantum assembly language to code (picture 5).

(Picture 5 [19])



(Picture 6 [20])

L. Future Possibilities?

At the moment, quantum computers are in their infancy stage. They are similar to when computers were originally created, and people didn't have much of a clue as to how amazing they could actually become. Previously, they were used for calculations, now, they're used for browsing the internet, streaming videos, communicating, typing, navigating, shopping, and much more. The point is, when they were first created, none of these ideas were around, but people eventually came up with ideas like Microsoft office, games, and eventually the internet. Similarly, Quantum computers are being created for the idea that they can run an operation on a lot of data at once. However, the issue is that quantum computing could most likely be used for so much more, just like how classical computers were. Scientists in the field believe that quantum computers could be extremely helpful in modelling chemical equations, thus aiding the pharmaceutical industry to produce more efficient medicine [18]. A scary part of this is prime

factorization. Currently, websites that accept credit card purchases use prime factorization to encrypt the information behind a credit card [21]. Basically, they take two large prime values, and multiply them together, and this final value is the key used to hide the card information. The final value is what the public can access, and the two prime factors that multiply to the large prime number are known only by the company you are buying from. Attempting to decode this number. I.e. find the two primes would take an absurd amount of time with classical computers because they have to try every value one at a time. However, quantum computers can run each operation parallel to each other, and would therefore take much less time. With quantum computers. Factoring prime numbers would not be an issue, and therefore it renders online credit card security useless. Similar to how the internet changed the world and the way we consume information, I believe that within a few years, quantum computing will also conquer feats that we have not even dreamed of yet.

VII. CONCLUSION

Essentially, quantum computers work by sending microwave photons into a qubit, which sends the qubit into a superposition state. Microwave photons can also entangle two qubits. The qubit can then exist as 1, 0, and every value in-between. The entangled information between two qubits is read within the correlation between the two qubits. While it seems as though quantum computers are making a big step in the right direction, there is still a long way to go until they become as normal as classical computers. With the expensive materials that are needed to make quantum computers such as superconductors and the system that keeps them at almost absolute zero, it would not be practical for each household to have one. Furthermore, it would not be useful to most people because the people that have used quantum computers don't use it for everyday tasks, they use it for research purposes such as modelling chemical formulas. Therefore, although quantum computers allow for an absurd amount of processing power, it will not be practical to use them for everyday tasks.

Bibliography

[1] A. Beall and M. Reynolds, “What are quantum computers and how do they work? WIRED explains | WIRED UK,” 2018. [Online]. Available: https://www.wired.co.uk/article/quantum-computing-explained. [Accessed: 01-Dec-2018].

[2] “(2) Polarization of light, linear and circular | Light waves | Physics | Khan Academy - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=HH58VmUbOKM. [Accessed: 01-Dec-2018].

[3] M. Rouse, “What is qubit? - Definition from WhatIs.com.” [Online]. Available: https://whatis.techtarget.com/definition/qubit. [Accessed: 01-Dec-2018].

[4] S. Bone and M. Castro, “Weblet Importer.” [Online]. Available: https://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/. [Accessed: 04-Dec-2018].

[5] M. A. Bashuk, “Solving a maze with a quantum computer,” 2003.

[6] D. McMahon, *Quantum Computing Explained*. A John Wiley & Sons, 2008.

[7] A. Wilkins, “Quantum computers could overturn Heisenberg’s uncertainty principle.” [Online]. Available: https://io9.gizmodo.com/5602933/quantum-computers-could-overturn-heisenbergs-uncertainty-principle. [Accessed: 04-Dec-2018].

[8] J. Brean, “Canadian researchers take a step toward a quantum computer | National Post,” 2013. [Online]. Available: https://nationalpost.com/news/canada/canadian-researchers-take-a-sneak-peek-at-schrodingers-cat-and-a-step-toward-a-quantum-computer. [Accessed: 01-Dec-2018].

[9] K. Bonsor and J. Strickland, “Qubits and Defining the Quantum Computer | HowStuffWorks,” 2000. [Online]. Available: https://computer.howstuffworks.com/quantum-computer1.htm. [Accessed: 04-Dec-2018].

[10] *Quantum Entanglement & Spooky Action at a Distance - YouTube*. .

[11] A. Morello, *(2) How Does a Quantum Computer Work? - YouTube*. .

[12] A. Morello, *(2) What is Quantum Mechanical Spin? - YouTube*. .

[13] D. Smith, “Quantum Entanglement and Quantum Computing | Caltech.” [Online]. Available: http://www.caltech.edu/news/quantum-entanglement-and-quantum-computing-39090. [Accessed: 04-Dec-2018].

[14] J. Preskill, “Quantum entanglement and quantum computing.” .

[15] S. Akama, *Elements of Quantum Computing*. Cham: Springer International Publishing, 2015.

[16] J. John Fernandez, “Quantum computation and quantum information.” [Online]. Available: https://medium.com/quantum1net/richard-feynman-and-the-birth-of-quantum-computing-6fe4a0f5fcc7. [Accessed: 01-Dec-2018].

[17] C. Iozzio, “Photos inside a quantum computer | Popular Science,” 2018. [Online]. Available: https://www.popsci.com/quantum-computer-photos. [Accessed: 03-Dec-2018].

[18] T. Gershon, “(2) Quantum Computing Expert Explains One Concept in 5 Levels of Difficulty | WIRED - YouTube.” [Online]. Available: https://www.youtube.com/watch?v=OWJCfOvochA&feature=youtu.be. [Accessed: 01-Dec-2018].

[19] “IBM Qasm Editor.” [Online]. Available: https://quantumexperience.ng.bluemix.net/qx/qasm.

[20] “IBM Q Composer.” [Online]. Available: https://quantumexperience.ng.bluemix.net/qx/editor.

[21] E. Frenkel, “Online credit card security: The RSA algorithm, prime numbers, and Pierre Fermat.,” 2013. [Online]. Available: https://slate.com/technology/2013/06/online-credit-card-security-the-rsa-algorithm-prime-numbers-and-pierre-fermat.html. [Accessed: 04-Dec-2018].