Systems Security Affectation with the Implementation of Quantum Computing

Advances in Quantum Computing

Norberto Novoa Torres[1], Juan Carlos Suarez Garcia[2], Erik Alexis Valderrama Guancha[3]
Faculty of Technology, Telematics Engineering
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia

***Abstract*—Current security systems use cryptographic robust tools that have been of great help in regulating information. During its time the implementation of these tools abolished the classic security systems, as by means of cryptanalysis they allowed decryption of information in a fast, automated, and simple mode from these systems. Considering this scenario, the same happens when quantum cryptographic systems are implemented, insomuch as the current security systems could be abolished, as tools exist that permit its encryption in a simple way, but with the risk of putting the data of worldwide organizations in danger. With the purpose of mitigating these risks, it is necessary to consider the upgrade of the available security systems, by security systems and quantic encryption, before a massive implementation of the quantum computer's use as an everyday tool. With this it does not mean that quantum computing would be a disadvantage, on the contrary, the advantages from this technology will mean that security information and data are almost invulnerable, which is a meaningful advance in the IT field. With security information professionals are obliged to recommend and perform an appropriate migration of new technologies to avoid existing exposition risks as data as well as transactions. If this were not the case, the same scenario presented in the classic security systems would occur.**

Keywords*—Quantum computing; encryption; cryptography; cryptanalysis; data security

I. Introduction

Encryption systems are drawn from the Vth century BC with the emergence of the Spartan Scythian, which consists of two bars of the same width in which people could only read messages. Then Caesar's encryption system appeared which is based on mono-alphabetic substitution. Another important encryption system is the Vigenere that implements the multi-alphabetic with character matrices. These systems are the ones we know today as classic encryption systems. During the Second World War, in the XX century, calculating machines were implemented with the purpose of deciphering the messages from these encrypted systems. Here the Turing machine is highlighted whose principle was based on rotors that automate the calculations to decrease the encryption time of the classic cipher methods, resulting in the obsolescence of these methods and the search for more complex encryption implementation methods. At this time, due to computation speed and the then current computers, new encryption methods were implemented, as the ones based on private password cryptography, in which is used the same password to cipher as well as decipher, are known as symmetric cryptography methods. Among them we could mention the DES algorithm that divides the messages into two similar parts and each interaction works alternately implementing an initial and final permutation. Other encryption methods are based on public password cryptography known as asymmetric key cryptography methods. These use a pair of passwords that belong to the same person, one is public and the other is private, for instance the Diffie-Helman and RSA algorithm. We can say that current cryptography is divided into two main types, symmetric key cryptography and asymmetric key cryptography. With the implementation of these current cryptographic systems, we can reflect about what happened to the classic encryption systems which were made obsolete due to emergence of current cipher methods. The classic methods could be decrypted in a much shorter time. Subsequently, we can see that the advance in quantum computing investigation will contribute to advancing current computing as we know it. This is based on the use of Qubits, a combination of ones and zeros, instead of bits as in the computers used currently., Also cipher algorithms would be on this principle, like the (QKD) quantum key distribution algorithm, Peter Shor, Groover and McEliece Algorithm. These quantum encrypted systems are more robust and capable of ciphering and deciphering information in such a way that they are almost impossible to break. From the perspective of the symmetric and asymmetric key encrypted systems used recently, their security is based on the use of complex mathematical problems which would take years to solve. However, with the implementation of quantum computers, these mathematical´ problems will change from being solved in years to minutes, as their processing speed will be much higher, and additionally will put in check security safeguarded information.

II. Methodology

A. Cryptography

Cryptography is the creation of techniques to encrypt data, having as its objective to obtain the confidentiality of the messages. If cryptography is the creation of mechanisms to cipher data, the cryptanalysis is the method to "break" these mechanisms and obtain the information. Once our data has passed a cryptographic process, we would say the information

is encrypted. Cryptography is a word that comes from Greek "Kryptos" that means hidden, whereby, it is understood as the study of science which by the treatment of information, protects itself from modifications and unauthorized use. Cryptography, besides being a discipline that studies the principles, methods and means to transform data to hide its meaning, guarantees its integrity, establishes its authenticity, and prevents its rejection. This has current mathematics bases that are: number theory, algorithmic complexity theory, information and statics theory. Cryptography must ensure that the sent information is authentic in a double sense: the sender is really who it says it is and that the content of the sent message, normally called the cryptogram, has not been modified during the transit. According to the Greek historian Polibio, the first cryptosystem was a substitution system based on the position of a letter in a table remarkably like Caesar's system used by the Romans, for example in military campaigns. Another documented cryptosystem that existed was the Scythian Spartan one which was based on a method of transcription using a cylinder as a key rolled to cypher and decipher.

Starting from the Second World War in the XX century, cryptography used tools like calculation machines to be more robust. The best known is the German Enigma machine, that used rotors considerably automatizing the calculations. This was necessary to perform the cipher and decipher operations from the messages that later were decoded by the mathematician Alan Turing. The classic methods use substitution and transposition methods over the characters in a message [1], these techniques having been proposed by Shannon to accomplish confusion and diffusion:

- Reverse Transposition: Consists in inversion of the message from the beginning to the end.
- Simple Transposition: This method divides the message symbol by symbol. If the total of symbols is odd for this group, one more symbol is added, getting two groups, the first one odd and the second one paired. They are united and the encrypted messaged is obtained.
- Double Transposition: The simple transposition is applied twice.
- Transposition by Groups: It is traded in a way the text characters are reordered in n character blocks, but they are reordered with a position number in the cryptogram, for example 321. meaning that character 3 is transmitted first, then the second, finally the first. This is repeated continuously by 3-character blocks. To decipher the message in this case the password would be 321.
- Transposition by Series: The message is ordered in such a way that the cryptogram is made by the sequence of the messages that has been considered to create it. In other words, simple functions are presented in a specific order to be able to cipher and decipher the message.

Modern cryptography is divided into two main tracks: key symmetric and key asymmetric cryptography. Symmetric cryptography, or secret key, are those algorithms that use only one cipher and decipher key. Therefore, its diffusion must be protected, as it is only for the authorized sender/receiver. For instance, the Data Encryption Standard algorithm or (DES) "Fig. 1" created in the 70s by IBM [2], uses the Feister framework (The data blocks are divided into two equal parts and in each interaction each one of its parts works alternatively) in blocks of 64 bits. Its initial key is 64 bits, then by each interaction it generates one of 56 bits, altogether it works with 16 interactions, implementing an initial and final permutation [3].

By contrast the asymmetric key cryptography (also known as public key one) is a system that implements a pair of keys. This pair of keys belongs to the same person. One is in the public domain, the other one is private. The MD5 algorithm "Message Digest Algorithm" is a coding algorithm related to a file. The one used to verify the file itself has not been modified "Fig. 2", it was designed by Ronald Rivest in 1991 [4]. It is based on a cryptographic reduction of 128 bits and is 5 parted: 1) Bits Addition: taking from an original text, this text is extended until it is consistent with the number 448 and module 512, to this is added a bit "1" then bit zero "0" to be extended 2) Length Message: a whole number of 64 bits is calculated which is the original text length before step 1 is made. These bits are linked to the result in step 1 having as a result a length that is multiple of 512. 3) Start a MD buffer: It is a 4-word buffer where each one has a length of 32 bits, and they are used to calculate a summary of the text. 4) Processing the text: XOR, AND, OR and NOT types of operations are made, also using a 64 elements table, made from a sine function, resulting in 4 words of 32 bits. 5) Exit: Finally, an exit text is produced where the 4 words come out from the least weight to the greatest.

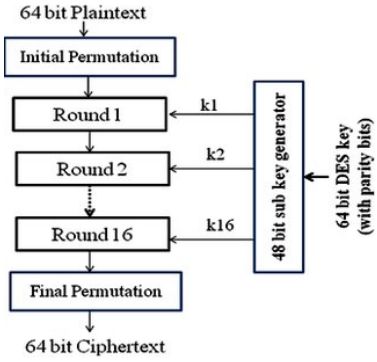

Fig. 1. DES Algorithm.

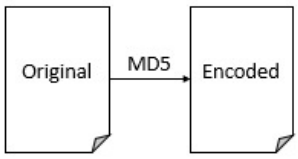

Fig. 2. MD5 Algorithm.

B. Quantum Cryptography

Although, traditional cryptography nowadays allows keeping a secure communication between two parts, the algorithmic proposals of Shor in 1994, which use the characteristics of a hypothetic quantum computer, could put in danger some of the most used cryptographic systems, such as the RSA. Quantum cryptography can reach secure communications using natural laws in a quantum scale, such as Heisenberg's Uncertainty Principle, of quantum overlaying and quantum interlinking. Quantum mechanics is a model to describe the behavior of subatomic particles [5]. With this it is proven that reality at a microscopic level behaves very differently to that at a macroscopic one. Classic physics, particularly Newton's Laws of Mechanics allow the performance of experiments that are verified at a macroscopic scale. For example, it is possible to track the journey of a cannon ball, or a basketball. However, quantum physics occurs at a level that is impossible to perceive with the five senses, like the polarization of a photon, or the spin of an electron.

Classic computers are physical systems, i.e., implications in terms of space, time and energy. Over time the demand for faster computers is higher. While computation devices keep miniaturizing, they get closer to the microscopic level, in which the laws of the quantum world rule. By the year 2020, computation will be carried on at an atomic level. With the arrival of quantum theory and some of its characteristics, like quantum overlaying and quantum interlinking, it was predicted that quantum computers, defined as "a type of computer that explodes the interactions of quantum mechanics", could develop some computing tasks exponentially faster than any conventional computer. These predictions go with the development of quantum algorithms, which from its theory, take advantage of quantum mechanics' features. To factor a number with 400 digits, a numerical achievement needed to break some security codes, it will take billions of years with even the fastest supercomputer. However, a quantum computer could complete the task in about one year.

C. Quantum Cryptographic Models

Quantum computing has created cryptographic models that work under the same paradigm, to achieve sharing information in two parts safely. Nevertheless, its construction and definition depend more on physics than on mathematics, because for this time the passwords are transmitted in photon shapes, not in bits as the current cryptography [6]. To understand these quantum cryptographic models, it is necessary to understand the following concepts:

- Superposition Principle: This principle consists in a quantum particle that is in a state of superposition. This means, it behaves as having different states at the same time [7], to change the state of the spin, the energy unit must be used, for example, laser, but what could happen if only half of the energy is provided? In this case theory says that the particle turns into a state of superposition.
- Heisenberg Uncertainty Principle: This principle establishes that in the subatomic world is not possible to know the values of two different magnitudes, from an elemental particle at the same time. Because the fact is that measuring the first one interferes with our capacity to measure the second one.
- The Shannon Bit: This consists in a bit only which can take one value at the same time, it can be 0 or 1. These bits have the ability to be copied.
- Qubit: This is that quantum unity which can take different values at the same time. It does mean 0 and 1 at the same time, so different from the Shannon bit.
- No-cloning Theorem: This theorem is the result from the quantum mechanics that bans the creation of identical copies from unknown and arbitrary quantum states.
- Quantum Entanglement: Starting from a group of particles that are entangled or connected in their existence, which even though they are separated by thousands of light years, a change of state of one of them affects the rest immediately.

D. Quantum Key Distribution (QKD)

The algorithm of Quantum Key Distribution (QKD) is a revolutionary encrypted technology that takes advantage of quantum mechanics' laws to reach a secure key interchange in the information theory. QKD allows the two parts of the encryption process "to increase" a secret shared key without adding any limits in the power of computing processing and is one of a kind in its capacity to detect the presence of any third party's participation during the keys' interchange. Due to the fundamental laws of quantum mechanics, any interception from a third party during the key interchange will introduce traceable errors. If the errors are under a defined limit, a secure unconditional key can be distilled. When a QKD is used with a symmetric cryptographic algorithm like the One-Time Pad [8], the result is an unconditionally cryptographic secure system. The beginning of the quantum keys distribution (QKD) dates to Stephen Weisner, who developed the idea of quantum codification of concerted in the last decade of 1960. He described two applications of quantum codification: a fraud proof creation money bills method (quantum money), also a method for the creation of multiple messages in such a way that one reading of the messages destroys the others (quantum multiplexing). The Wiesner quantum multiplexing uses polarized photons in concerted bases like quantum bits (qubits) to pass the information. Thus, if the receiver measures the photons in the correct polarization base, it will get a high probability of a correct result. However, if the receiver measures the photons on the incorrect base, it will obtain a random result and it will destroy all the information on the original base. The encrypted process is the following, to destroy a key, the dispenser part, Alice, creates a random bit in a random base, sending a photon this being 1 or 0 in a horizontal or vertical way. The photon created by Alice is received by Bob, who does not know the base Alice used. Bob measures the photon polarization, as he chooses randomly any of the two bases. Alice and Bob then discuss through a public channel on the one they decide to measure, and they discard the bits Bob did not measure using the same base that Alice did to create the photons.

This process permits a secure channel to the key distribution, as any person that listens to the channel must guess in which base it measures. If Alice and Bob choose the same base, but the spy chooses a different base, there is a 50% possibility that Bob will measure a different bit value from the one Alice sent. Therefore, Alice and Bob have the possibility to detect an interceptor through a public comparison and discard a certain number of bits for the ones who chose the same base.

E. Peter Shor Algorithm

The Peter Shor Algorithm allows decompounding prime factors in any N number, hence its potential implementation in a quantum computational device brings as a consequence that cryptographic systems based on a factorization process like the public key system RSA will be broken easily [9]. While the processes related to the key public algorithms are executed in super polynomial times by the mode exp[c(In N) 1/3 (In) 2/3], to the Shor quantum algorithm, with the necessary time to execute this same polynomial task and by the mode O(Log(N) 3). The great strength of calculation the Shor algorithm has regarding the implemented algorithms in conventional computer consists in the fact of doing quantum effects like interference, enhancing and allowing an information process in a parallel mode, which is competingly translated in a processing reduction of time. This algorithm underlies its power to determine the period of an adequate function. Although its study presents a high level of complexity, it can be interesting to analyze the new approach of quantum mechanics that offers a solution to the problem of factorization.

F. Groover Algorithm

The Groover Algorithm is used to search in a non-ordered sequence of data. It was invented by the North American scientist of Indian origin, Loc Kumar Grover in 1996 [10]. This algorithm avoids reconstructing a previous organization of the search. The algorithm is strictly probabilistic whose answer has an error percentage and so must be small enough. To explain how it works let us suppose we have a non-structured data base with N elements, and they are numbered from 0 to N-., These elements are not in order. Normally, we will test element by element, until we have the one, we are looking for. Using the Grover Algorithm, *we only need attempts*. The Groover algorithm has registrations: n qubits in the first and 1 qubit in the second. The first step is to create a superposition of all 2n states from the computing base. This is made by initializing the first register in the state and applying the operator Hn, where H is from the Hadamard door [11]. Then, we set a function f that recognizes the solution as f:{0,….,N-1}→ {0,1}, f(k) = 1 if K is the searched element, on the contrary f = 0. The function f "Fig. 3" also is recognized as an oracle and it can be defined as:

This algorithm has an operator sequence of Groover (G) iteration and the states of the first register correspond to the first iteration.

G. McEliece Encryption

The McEliece cryptosystem is an asymmetric encryption algorithm developed in 1978 by Robert McEliece. It was the first of these schemes to use randomization with the encryption process. The algorithm has never earned much acceptance among the cryptographic community, but it is an application of the quantum post-cryptographic, as it is immune to attacks using the Shor algorithm and, more generally, the measure of the coset states using the Fourier sampling.

The algorithm is based on the strength of decoding a general linear code [12]. To a decryption of the private key, a correction code of errors is selected as it is known that a decoding efficient algorithm can correct the errors. The original algorithm uses binary Goppa codes (codes subfield of geometrics, Goppa codes from a gender-0 curve over finite fields of characteristics. These codes are easy to decrypt due to an efficient algorithm on account of Patterson. The public key drifts from the private key to encrypt a selected code as a general linear code "Fig. 4". The McEliece cryptosystem has some advantages, for example, with RSA the cipher and decipher are faster. For some time, it was thought McEliece could not be used to generate signatures. However, a signature scheme can be built over the Neiderreiter base scheme, the double alternative of the McEliece scheme. One of the main disadvantages of McEliece is that both private and public keys are large matrices. To a standard parameter's selection, the public key is 512 kilobits. Because of this, the algorithm is used too little during practice. An exceptional case that uses McEliece for encryption is the Freenet application. McEliece is about three algorithms: a probabilistic key generation algorithm that produces a public and private key, a probabilities algorithm, and a deterministic decryption algorithm.

H. Quantum Cryptography vs. Classic Cryptography

As it is seen during this paper, one can analyze how the techniques, modes, and methods to make a cryptographic system securer have evolved, from simple steps or movements with the alphabet to complex mathematical calculations, for instance, one technique is the use of substitutions. This consists in replacing by parts the message to transmit with other words or symbols keys that later can be decrypted by the receiver if this one has the same key combination. Another one is by making a transposition in the message in which one will not be replaced by other alphabet, but they change them in position or geometrical mode order, for example to write the message backwards and at the end by making mathematical calculations with prime numbers, modulation of a number, whole factorization and discrete logarithms, among others.

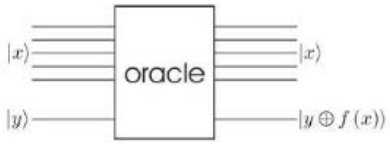

Fig. 3. Oracle of the Function.

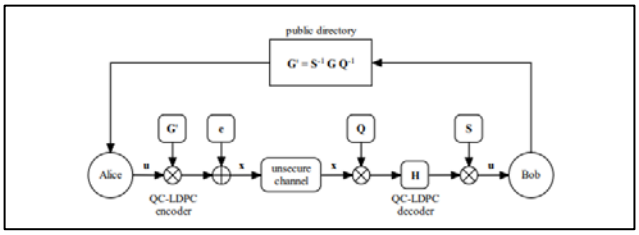

Fig. 4. McEliece Encryption.

These techniques have solved the problem of transmitting messages in a secure mode through time, in most telecommunications such as cellphones, the internet, fixed telephony, satellites, the use of cryptography exists. Similarly, in the financial field when the use of cryptography was adopted by banks, this necessitated the change in use of cards with magnetic stripes to the use of EMV chip cards, with the calculation capacity, and the holders' reliability, improving the quality and security of transactions. Large financial companies like Visa, Mastercard, American Express adopt this technology and create their own security standards [13].

Due to cryptography our data has managed to travel in different networks safely, however, there are also those who want hidden information and with the use of cryptographic engineering have managed to decipher algorithms that were believed impossible to break. Every time the complexity of a cryptographic algorithm increases, more processing memory is needed. A common electronic device such as the cellphone does not have the capacity to process a complex algorithm. The human mind can create new algorithms to hide information, whereas the machine is still inferior in its processes. There are mathematical algorithms which the traditional machine can take years to process and solve, such as the Riemann Hypothesis where all non-trivial zeros of the Riemann zeta function have a real part of 1/2. These complex mathematical processes are processed in large supercomputers that are not available for anyone as they use a lot of space, consume a lot of energy, and are expensive. Thus, it is impossible for a device as small as a cellphone to encrypt a message that is totally safe for several years. It should be noted that existing algorithms are still being improved to make them more secure. But it cannot be forgotten that there are always the same bases and principles to hiding a message, making it vulnerable, because, just as the digital age advances rapidly, breaking security systems also advances. This is classical cryptography, which is accustomed to employing the same bases, the same tools, and the same laws of physics.

The birth of quantum cryptography occurred when several physicists, including Albert Einstein, discovered that there were different and unexpected behaviors when one enters the subatomic world of matter [14], called quantum physics, where many of the physical laws known nowadays do not apply. Normally an algorithm returns something that can be true or false if its execution were correct or not if the light bulb were on or off. When we talk about quantum physics, creating an algorithm at that level is expecting different simultaneous responses which are impossible to be observed at that moment. If one wants to know a precise answer statistical predictions should be used. In classical cryptography if the encryption algorithm is known, a spy can at some point in the execution of the algorithm, find the hidden message. While in quantum cryptography it is impossible to stop at an execution point and find the hidden message since the spy would find a message that is no longer part of quantum physics. That means it would no longer be part of the quantum algorithm, therefore the message is modified making it impossible to reach the receiver. Consequently, this is a point in favor in quantum cryptography because if the receiver at no time receives the hidden message, it is because the channel has been intercepted, while in classical cryptography the intruder can even listen to the channel without the sender or receiver suspecting it.

Regarding this speed, whereas in classical cryptography when it makes the algorithm more complex the processing time is slower. In quantum physics an algorithm of considerable complexity can be processed in less time. This means that with the use of the quantum physics it can be implemented without any problem ciphered algorithms of high complexity, allowing an increase of the security in communications, including finance, the results are shown in Table I. However, this science is new in practice and the attempts to reach quantum behaviors are highly expensive, as they involve subatomic particles where the matter overheats and its refrigeration is not at all easy. This is a negative point because there still does not exist sufficient portable hardware for computer systems to take advantage of the benefits of quantum mechanics. Even so, at present all the potential that could be had if a quantum computer were created is being studied by means of theories and the creation of new quantum algorithms that can even easily break the existing cryptographic algorithms. This is the case of the Shor Algorithm which is implemented in a quantum computer that can break down into prime factors any number no matter its length. Or ((log N)3), which could leave obsolete a lot of public key cryptographies like the RSA. An advantage that quantum physics has is entanglement, consisting of, a particle influencing another particle despite how far we find it from the other one. This can yield an advantage for secure communication because while a sender has in its power a particle that influences another particle that the receiver has, it be able to communicate only by taking advantage of this property. Now imagine that it were not only a particle but the whole message, then it would only be required to interlink the messages. Thus, the two points can communicate by means of a quantum channel. This is different from classical cryptography where the sender and receiver must share a key or password that allows enciphering and deciphering of the message. Here below, is shown a comparison between these two types of cryptographies, noting that the quantum is superior.

TABLE I. COMPARISON OF QUANTUM CRYPTOGRAPHY AND CLASSICAL

	Classical	**Quantum**
Speed	As more complex, slower	Fast, no matter the complexity
Security	Only for a while until deciphering is done	When the message is intercepted immediately it loses the information.
Implementation	For more complex calculations it requires more power of processing.	The hardware of quantum technology is in the development process
Future	Insecure	Decrypts most of the implementations of classical cryptography.
Channel	There must exist a physical connection between the parts	It is not necessary to have a physical connection if it takes advantage of quantum interlinking
Keys	The sender and receiver must have the key to encipher and decipher the message.	With the use of quantum interlinking the use of keys would not be necessary.

I. Types of Security Systems Would be Affected

Future general use of quantum computers would take away the latent risk of the current public key infrastructure systems and private key. The majority of world-wide transactions are based on the systems of current cryptography to protect their security, the super powered quantum computers making use of the encrypted and decrypted quantum algorithms mentioned in the present article, which are based in quantum bits or qubits. These will allow the speed of processing from encryption and decryption of the best systems of security used today to change from being decrypted in thousands of years to only fractions of a second.

Quantum computing is really closer than we imagine. The companies and organizations that handle critical data like banks, governmental agencies and the field of medicine development that do not start considering this scenario, could be exposing data and information highly vulnerable as their methods of encryption could be decrypted easily when facing quantum computing.

If information security professionals do not implement measures right now and understand that the advance in the construction of operable quantum computers is developing in great steps there potentially will be a threat for the current methods of encryption and they will be faced by an exhibition of data and catastrophic leaked information.

The systems of asymmetric encryption would be the most vulnerable as they are based in cryptography of public key, the one that is based on extraordinarily complex mathematical algorithms [15]. However, this prospect would remain delayed if they used quantum computers.

Because of this it may be too late to guarantee that when quantum computation is implemented the processes of encryption in the different organizations are protected because it would take too long for the computation of trail algorithms and quantum encryption to integrate to the organizations satisfactorily. Although there are tasks that security professionals can implement so they are not totally exposed, these are based on encryption agility and the capacity to implement and adapt algorithms of quantum encryption once available.

J. Encrypted Simulation

A quantum computer will break the encrypted RSA of 2048 bits in eight hours. If now a quantum machine of 20 million cubits were implemented it could do it in a record time [16]. The systems of encryption like the RSA never have been unfailing. As mentioned, its security is based in the massive quantity of time that a conventional computer would need to do it. The current methods of encryption are designed specifically for encrypted processes that were so slow that they seemed practically unbreakable.

Several computer scientists have tried to calculate the resources that a quantum computer would need to discover how long it would take to build a machine of this type. However, this calculation must be reviewed due to the work of the Google researcher in Santa Barbara (USA) Craig Gidney and the researcher of the Royal Institute of Technology KTH in Stockholm (Sweden) Martin Ekerå. Both have found a more efficient way for quantum computers to perform encryption code calculations, which reduces the resources needed by a magnitude of several orders.

Their findings suggest that these machines are much closer to being made for real than we had suspected. The effect will be uncomfortable for governments, military and security organizations, banks and anyone who needs to store data for longer periods than 25 years from now, because as is indicated in the algorithm of Peter Shor, big numbers are factorized, and there is the crucial element of the process to decrypt the codes based in mathematic algorithms.

These algorithms are based on the process of multiplication, that is easy to perform in one direction, but much more difficult in the reverse sense. For example, multiply two numbers result very simple: 593 x 829 = 491.597. The difficult part is to begin with the number 491.597 and calculate which two numbers have been multiplied to produce it.

As the numbers increase, the issue gets more complicated. In fact, computer scientists consider it practically impossible for a conventional computer to calculate the numbers with more than 2048 bits, which is the base of the most used mode of the enciphered RSA.

Shor showed that a quantum computer powerful enough could do it with ease, something that surprised the cyber security industry. Since then, the power of the quantum machines has not done anything but increase. In 2012, some physicists used a quantum computer of four cubits to calculate the factor 143. In 2014, they used a similar device to calculate the factor 56,153.

So, anyone could think that, at this pace, quantum computers are about to surpass the best conventional computers.

For Gidney and Ekerå have just shown that a quantum computer could do the calculation with only 20 million cubits. In fact, they claim that it would take only eight hours in completing the calculation. As a result, the estimate of the worst case of how many cubits needed to factorize the RSA of 2048 bits has reduced by almost two orders of magnitude. Its method focuses on a more efficient mode to make a mathematical process called modulate exponentiation “Fig. 5”. It consists in finding the reminder when a number elevates to a true level and afterwards divides it by another number. This process is the most expensive operation of the computing level of the algorithm of Shor. However, Gidney and Ekerå have found several forms to optimize it, which significantly reduce the necessary resources to execute the algorithm.

For any ordinary citizen, this finding does not entail a lot of risks. Most people use encryption of 2048 bits, or similar, for tasks like sending details of credit cards through the internet. If these transactions were registered today and be decrypted in 25 years, the damage would be minimal. Nevertheless, for governments, the situation would result in more trouble. Today’s messages sent between embassies or the army could be important in the next 20 years and would be better kept secret. If these messages were still sent through an enciphered RSA of 2048 bits, or something similar, these organizations would have to begin to worry a lot.

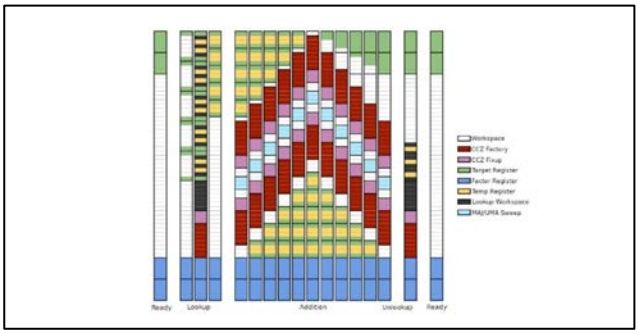

Fig. 5. Calculation Simulator of Encryption.

K. How to Find the Security in the Cloud

Different internet platforms offer cloud services where the user does not require installing any type of software in their computer, rather only using a browser web that can access different services of the cloud, as it is with emails, music, editing of photos and videos, online office, online films, social networks etc. Each service in the cloud has implemented its security based on the protocols of SSL (Secure Sockets Layer) and TLS (Transport Layer Security) These are cryptographic systems for computer networks that guarantee transmitted information in the network is not intercepted by an unauthorized third party [17]. The SSL protocol works using an SSL certificate inside the server, so when a customer requires access to it, it is done by means of a public key of the server making a safe connection by means of symmetrical cryptography. This validation is made by the browser web again without needing software installed. As long as, the quantum computing was not entirely developed this method of security joined with HTTP, meant, generating secure HTTPS versions "Fig. 6" that would keep being secure and used a lot in based cloud-based services.

Nonetheless, big companies that offer cloud services have already known the impact that the implementation of quantum computing can have, as too many cryptographic protocols will stop being secure. Because of this, companies like IBM, that have developed quantum computers with some qubits, had the idea of letting people access the quantum computer though the cloud [18]. As we mentioned before, it is too complex for homes or small businesses to have a quantum computer because extreme cooling is needed and due to any interference quantum properties might be lost. Thus, IBM opened the "IBM Quantum Computing" platform in which the community can register, program and generate quantum algorithms that are directly executed in a 16 qubits quantum computer. This is with the aim that programmers, scientists, including physicists, make their investigations tests using quantum computing and validate the efficiency and the answer speed. The mode to program on this platform is by the terms of quantum rational ports, as the logic port of Hadamard, phase displacement, the SAWP gate, CNOT, and Controlled-U, amongst others "Fig. 7". These logic gates are moved as pieces inside a virtual circuit over each qubit line as is shown in the following chart.

Besides, there is a platform that lets one create quantum algorithms and execute them in its computer. IBM is developing a service in the cloud of quantum cryptography to let several companies requiring to increase their internet security to do so. They could do so by connecting to these services from the year 2020. Of course, access to these services is awfully expensive but it guarantees that the security of the information will be safer, despite quantum computation being implemented.

Also, Microsoft with its cloud platform, "Azure", is offering quantum services that provide free a group of tools for quantum programming called Q# (Q-Sharp) of open source and available in GitHub. It has a package of quantum solutions precompiled ready to be used in the projects inside Azure, also including simulators to test the algorithms before executing them in the quantum real machine. Equally, it is expected the giant Google will open a platform to the public to access its quantum servers as they have been recognized to reach quantum supremacy by executing an algorithm of random numbers in just 200 seconds. A normal computer would take nearly 10,000 years [19]. Amazon, another of the big technology companies, also opened a platform in the cloud called "Braket", which offers quantum computation as a cloud service [20]. This allows the creation of a community in which they only develop quantum algorithms to be tested afterwards by the Amazon simulator, AWS. They offer an environment of work which is, *Jupyter*, entirely managed. All these tools of Amazon allow the investigation and identification of applications of quantum computation that can be feasible for the companies' customers.

As has been observed, the big technology companies are opening their doors using the cloud so that those interested in the subject can collaborate in the development of quantum computation. The cloud acts as a bridge between the programmers, scientists, physicists, amongst others and the quantum computer [21]. Then, a company that provides services on the internet, like on-line music, can start up the investigation of how to improve its security using these platforms of quantum processing, generating new algorithms or improving the cryptography they are using. The problem in using these platforms from third parties is that we continue depending on their quantum computers. By their hardware they can take advantage of this technology by implementing methods of collection in their services. However, it is not a problem for those that really wish to increase their security in the cloud, like in the case of the banking agencies and virtual shops who could develop software that connects to these quantum services to prevent fraud in electronic transactions.

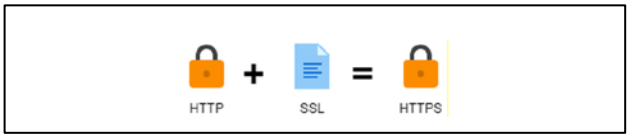

Fig. 6. Https Protocol.

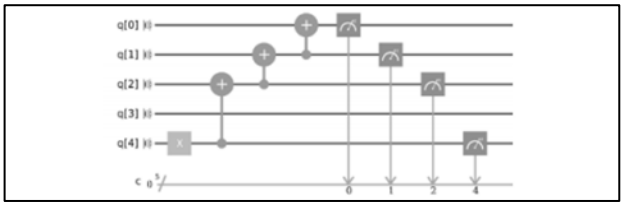

Fig. 7. Quantum Logic Gates.

That said, one of the important properties of quantum physics is quantum teleportation which takes advantage of quantum interlacing to send information from place to place. In 1997 the experiment to transport information was conducted on separate quantum particles to less than a meter. They did it and realized that this could be duplicated, even though the quantum particles were more widely separated. In 2012 a team of physicists from the Austrian Academy of the Sciences of the University of Vienna in Austria carried out quantum teleportation to 143 kilometers successfully [22]. From these developments they have made longer distance teleportation from space and underwater to 1,200 kilometers, quantum chips interlaced sending information instantly without existing physical or electronic connection between both circuits. It is said, that if in a future a network or quantum cloud existed these servers could send information without needing a physical connection between them. Theoretically speaking it would be enough only to take advantage of quantum interlacing; this would suppose an exceedingly high security in the quantum communications as an interceptor or hacker does not have a channel that intercepts. The problem with this is that it only happens between quantum servers and not in compound networks. However, if the technology continues advancing so quickly in maybe 50 years or more there could be more quantum computers forming a new cloud between them [23].

III. Discussions

Information security is an essential subject in telecommunications. If security did not exist its use would be extremely limited as we could not create online stores, there would be systems of information with session start, and we could not make bank transactions, amongst other things. Therefore, security always will be involved in a continuous study where security methods are increasingly difficult to break and the information is kept safe. For this reason, different algorithms have been created to allow a secure information transmission mode; algorithms like the AES, GIVE and MD5 have taken enough strength and are practically every electronic device like cellphones, computers, credit cards, TVs, cameras of surveillance cameras, etc. [24]. The mathematics that these algorithms use is modular mathematics, factorization of prime numbers, combinations, permutations etc., thus allowing a greater complexity for a third party or attacker trying to break the method of encryption. This has been possible due to the computing power that has been evolving through time. Cryptology has taken advantage of the computational power increasing the quantity of bits to be used to encipher a message. Even so, the same computational systems are unable to break systems of security in a short time but can take many years processing and trying to discover the keys that allow decoding of the information.

Then, why is a piece of information not completely secure is because its channel of communication can be easily intercepted or because it does not use big enough keys to encrypt the information. Therefore, it is necessary to consider that its channel should be the most private possible. Attackers sometimes use social engineering so that the people who are sending or receiving confidential information are unaware and show the key that allows decoding of this information., It may be by just showing fake advertising in web pages, fake buttons or application of information. Also, the intruder through these techniques can insert malware which allows control of the computer or simply collection of information. Thus, when it requires greater security requires greater computational using more power space and more hardware. This does not mean that it is a negative benefit to improve computational power with the aim of improving information security. On the contrary, it is a positive by improving the methods of encryption making us feel safer sharing information or making bank transactions. Yet this is not entirely sufficient. The current computational power is based in binary systems, with all the calculations, processing and digital life based in the binary system which when it creates a supercomputer is able to process much faster mathematical complexes calculations than a conventional computer. We can say that a system of encryption is in danger of being decoded in a shorter time. Current supercomputers like the Summit of IBM instrumented with artificial intelligence have a power of 200 petaflops [25], this means, that they can do 200 floating comma operations per second and could be able to decode some algorithms of cryptography.

Now, quantum physics has taught us that it can be used to create quantum computers where we take advantage of the main characteristics of these physical states, which means if a conventional computer based in binary systems (1 or 0), the quantum computer can take the 1 and 0 at the same time, being a lot more powerful, faster that a supercomputer and without occupying a lot of space. If a supercomputer based in the binary system can break some cryptographic systems, the quantum computer also will do it in less time. An example of this is the publication by Google where its quantum computer was able to execute an algorithm that generates random numbers in 200 seconds when a conventional supercomputer can take 10.000 years. Even up to now some studies as well as prototypes of quantum computers have been made [26]. The scope of these computers is quite wide, having important uses in medicine, astronomy, chemistry, physics and of course in computing especially in the field of cryptography, where it has designed quantum algorithms that allow a research of information in non-orderly data (called the algorithm of Grover). This means data does not even require to be organized in intelligible form for informational research. Another algorithm called the Algorithm of Shor performs factorization of numbers using quantum physics. This is important in security since many of the current cryptographic algorithms are based in breaking down a number to prime factors. It means with the implementation of quantum computation all the current systems of security would be in danger, as a quantum computer with sufficient capacity of Qubits, [the basic unit of the quantum computer as the bit is for the conventional computer], can easily break these algorithms.

Thus, they have produced diverse studies in quantum cryptography. In addition, protocols that allow one to perform a safe communication like the protocol EPR taking advantage of interlaced quantum between pairs of photons. This means that when two photons are interwoven, and a photon changes the state or makes some perturbation immediately the other photon takes on the same behavior. This property is now particularly useful to send information and in a safe mode, since with a small perturbation that comes from no controlled

external entities one can modify the original information warning the receptor that the message has been intercepted and is not intelligible at the moment of decoding. If we take advantage of this property of quantum physics in quantum computers, it will improve security significantly since the intruder could not try to read the message because it would be modified without intention and immediately raise an alarm indicating an intervention in the communication. However, the same was thought when they created the first systems of cryptography like the enciphered Caesar. There it was believed for decoding it was necessary to use black magic or ask the help of some witchcraft. Also, with the enigma machine that was used by the Nazis it was thought that it was an impossible system to decode until Alan Turing managed to do it due to his knowledge of mathematics and logic; then also it can succeed in finding the way to intercept the messages in the quantum computers not immediately but when these quantum theories of the physics and quantum mechanics are near to be in the use a lot of people who can study and understand them. Therefore, the competition between them which is apt to create the best unbreakable encrypted algorithm for the coder and the attacker who wants to decode it in the shortest time will continue existing even with the arrival of quantum computation.

For quantum computation use to be near all of us, as well as the current computation, a lot is missing for implementation since the existing quantum computers suffer from different problems. Firstly, the quantum computer requires quite a lot of refrigeration that can be costly as the particles being in a quantum state generate quite a lot of heat. Secondly, the current quantum computers still do not have the necessary power to completely replace the current ones. The first quantum computers would be used especially by scientists in matters of biology, astronomy, chemistry, amongst other. There does exist the possibility of accessing a quantum computer via the cloud for academic use, thanks to platforms launched by IBM, Amazon, and Microsoft. They can design quantum algorithms with new programming languages and test their functionality. It is here where the community that devotes to the cryptology can investigate and develop new methods of computer security that in the future can be applied in networks of quantum computers which require to communicate in a secure mode. Meanwhile the cloud can generate something as well as “quantum services” that are to the order of those that require quantum computational power for some internal process of some company. For example, a programmer of a security company can develop an algorithm that strengthens the system of security that is internally in the company. A banking entity can improve its security of transactions connecting its system of security to one of these quantum services. A software app for text mailing like WhatsApp or Telegram can make use of these quantum services to improve its security in sending messages. Software of streaming like Netflix or HBO can avoid theft or copies from original series. Software of VPN can improve its efficiency taking advantage of these quantum services to improve the privacy and security in those companies that use VPN for safe connections in the web. So, with this successively different software, banking and governmental companies can take advantage of this new technology.

Taking advantage of this new technology depends on the freedom to access the cloud of a quantum computer. Since its use can in future carry additional cost, for example, as well as Microsoft Azure, different services that are by payment, will also carry quantum services, and is not too surprising since their price is necessary to keep a cutting-edge technology progressing obtaining a favorable result for the customers. It is true that, if very few know their potential, demand for consumption of these services will be low. Therefore, it is important that academies of computer security even universities or schools begin to explore the world of quantum computation. The programming of quantum computers that already exists varies like the Q# of Microsoft, Quipper, the Quantum Composer of IBM, amongst others; as professionals exist in the subject they can develop the new cryptographic algorithms that improve technological security in the world. Since a company can apply, into its systems of small security, a process to connect into a quantum service, they will see the success that it has by observing that the system is more reliable and faster. It will be popular; it will attract a lot of more customers and its income will be much higher; from this moment other companies will be attracted by this technology and surely incorporate it in their services. It is here where a new need opens to purchase the knowledge of programmers, scientists and physicists in the quantum subject. Therefore, it is important to begin to learn to use this technology that is for the future.

Another field that will importantly be affected by quantum cryptography are the cryptocurrencies [27]. Although it is known that cryptocurrencies save a unique hash that is not able to be copied and their system of transactions have security, therefore it has a value. When we dominate the quantum cryptography the majority of cryptocurrencies will no longer be safe and therefore it its use would go down use since it is a totally digital coin. However crypto coins could also see benefit if they inject quantum cryptographic algorithms into their systems of security algorithms quantum, as is done already by Bitcoin, Ethereum. Or possibly develop a new cryptocurrencies based in quantum computation, that in my opinion would make cryptocurrencies safer and their use would increase. This subject of security where money is at stake is important for banking agencies which would have to be concerned not only because their technological systems would become vulnerable but also because if the quantum cryptocurrencies arrived first before of the agencies increased their security, the use of banks would lessen.

IV. Conclusions

This new technology like any other, has to be controlled. They cannot have all their potential immediately belonging to all community as it could be used for hacking different systems. The first step is to allow important sectors, like banking, and government programs to use this technology with all its potential, as they improve its system against attacks and afterwards put at the disposal of the public a small part of the power that quantum computation would have as we know that the systems of current security can be very vulnerable.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the faculty of technology of the Universidad Distrital Francisco Jose de Caldas. From Bogotá, Colombia.

REFERENCES

[1] Domínguez Espinoza, Edgar Uriel. Pacheco Gómez Leonardo. Classic cryptography algorithms. apr 10th 2007. National Autonomous University of Mexico. [Quoted apr 23rd 2019]. Available at: https://docplayer.es/21024045-Universidad-nacional-autonoma-de-mexico-facultad-de-ingenieria-criptografia-algortimos-de-criptografia-clasica.html.

[2] Héctor Corrales Sánchez, Carlos Cilleruelo Rodríguez, Alejandro Cuevas Notario. Cryptography and Encryption Methods. Madrid. apr 24th 2014. University of Alcalá. [Quoted apr 25th 2019]. Available at: http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf.

[3] B. Bhat, A. W. Ali and A. Gupta, "DES and AES performance evaluation,"International Conference on Computing, Communication & Automation", Noida, 2015, pp. 887-890. doi: 10.1109/CCAA.2015.7148500.

[4] Tao Xie, Fanbao Liu, Dengguo Feng. Fast Collision Attack on MD5. 2013. [Quoted apr 23rd 2019]. Available at: https://pdfs.semanticscholar.org/a9d4/833698895915d34f2ac5509f1bf0887b4c5b.pdf.

[5] D.J. Griffiths. Introduction to Quantum Mechanics. Prentice Hall - New Jersey. 1995. [Quoted apr 15th 2019]. Available at: http://gr.xjtu.edu.cn/c/document_library/get_file?p_l_id=21699&folderId=2383652&name=DLFE-82647.pdf.

[6] Ahmed Banafa. Understand quantum cryptography. nov 19th 2015. BBVAOPENMIND. [Quoted may 9th 2019]. Available at: https://www.bbvaopenmind.com/tecnologia/mundo-digital/entender-la-criptografia-cuantica/.

[7] Quantum cryptography - Cryptography concepts. jun 24th 2005. Scientific texts. [Quoted may 9th 2019]. Available at: https://www.textoscientificos.com/criptografia/quantica.

[8] Nithin Nagaraj, Vivek Prabhakar Vaidya, Prabhakar Govind Vaidya. Re-visiting the One-Time Pad. 2008. GE Global Research. [Quoted apr 28th 2019]. Available at: https://www.researchgate.net/publication/220284469_Re-visiting_the_One-Time_Pad.

[9] Javier Blanco. Quantum computers could break RSA 2048-bit encryption in 8 hours?. dec 29th 2019. Agency6. [Quoted jan 30th 2020]. Available at: https://agencia6.com/index.php/2019/12/29/ordenadores-cuanticos-podrian-romper-el-cifrado-rsa-de-2048-bits-en-8-horas/.

[10] Leander Kahney. Quantum Leap in Searching. jul 3rd 2011 [Quoted jun 4th 2019]. Available at: https://web.archive.org/web/20110703044742/http://www.wired.com/science/discoveries/news/2000/05/36574.

[11] Z. Sakhi, R. Kabil, A. Tragha and M. Bennai, "Quantum cryptography based on Grover's algorithm," Second International Conference on the Innovative Computing Technology (INTECH 2012), Casablanca, 2012, pp. 33-37, doi: 10.1109/INTECH.2012.6457788.

[12] David Moreno Centeno. Post-quantum cryptography: McEliece implementation and a new version. University of Valladolid. [Quoted feb 19th 2020]. Available at: https://uvadoc.uva.es/bitstream/handle/10324/38361/TFG-B.1368.pdf?sequence=1&isAllowed=y.

[13] Cryptography in the financial world. sep 2nd 2014. Media-Tics Information and communication in the digital age. [Quoted oct 3rd 2019]. Available at: https://www.media-tics.com/noticia/2585/blogs/la-criptografia-en-el-mundo-financiero.html.

[14] A. Einstein, B. Podolsky and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?". Physical Review. Vol. 47 N° 10, pp.777-780. May 15th of 1935. DOI: 10.1103/PhysRev.47.777.

[15] Javier Paniagua. Cryptography in banking. jul 7th 2017. Research IT Now. [Quoted may 7th 2020]. Available at: https://revistaitnow.com/criptografia-en-la-banca/.

[16] Steve Jurvetson. A quantum computer will break RSA 2048-bit encryption in eight hours. jun 9th 2019. Source Sites. [Quoted may 21th 2020]. Available at: https://sitiosfuente.info/ciencias/13147-ordenador-cuantico-cifrado.html.

[17] Mónica Tilves. IBM Cloud to deliver quantum security cryptography services starting in 2020. aug 26th 2019. Silicon. [Quoted jun 4th 2020]. Available at: https://www.silicon.es/ibm-cloud-entregara-servicios-de-criptografia-de-seguridad-cuantica-a-partir-de-2020-2402341.

[18] IBM to offer quantum-safe encryption services over public cloud in 2020. aug 26th 2019. Digital Security. [Quoted nov 14th 2019]. Available at: https://www.itdigitalsecurity.es/cloud/2019/08/ibm-ofrecera-servicios-de-cifrado-quantumsafe-sobre-nube-publica-en-2020.

[19] Josep Corbella. Google proves quantum supremacy. oct 23th 2019. [Quoted nov 14th 2019]. Available at: https://www.lavanguardia.com/ciencia/20191023/471156519790/ordenador-cuantico-google-supremacia-computacion-cuantica.html.

[20] Celia Valdeolmillos. AWS re:Invent 2019: Amazon bets on quantum computing with Bracket. dec 3rd 2019. [Quoted feb 2nd 2020]. Available at: https://www.muycomputerpro.com/2019/12/03/aws-re-invent-2019-amazon-computacion-cuantica-braket.

[21] Lara Olmo. Google sees new possibilities for its cloud business in quantum computing. jul 17th 2017. [Quoted nov 10th 2019]. Available at: https://www.ticbeat.com/tecnologias/google-ve-en-la-computacion-cuantica-nuevas-posibilidades-para-su-negocio-cloud/.

[22] New record in quantum teleportation lays the foundation for global quantum communication. sep 6th 2012. [Quoted oct 10th 2019]. Available at: https://tendencias21.levante-emv.com/nuevo-record-en-teleportacion-cuantica-sienta-las-bases-para-una-comunicacion-cuantica-global_a13021.html.

[23] Llewellyn. Powerful boost to the quantum Internet. jan 3rd 2020. [Quoted mar 13rd 2020]. Available at: https://tendencias21.levante-emv.com/potente-impulso-al-internet-cuantico_a45631.html.

[24] A. K. Mandal, C. Parakash and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, 2012, pp. 1-5.

[25] The world's most powerful supercomputer identified chemicals that could stop the spread of the coronavirus. mar 21st 2020. Infobae. [Quoted apr 4th 2020]. Available at: https://www.infobae.com/america/mundo/2020/03/21/la-supercomputadora-mas-potente-del-mundo-identifico-los-quimicos-que-podrian-detener-la-propagacion-del-coronavirus/.

[26] Google publishes how it has achieved quantum supremacy. oct 23rd 2019. [Quoted apr 4th 2020]. Available at: https://www.publico.es/ciencias/ordenador-cuantico-google-publica-logrado-supremacia-cuantica.html.

[27] Cassio Gusson. Bitcoin and Ethereum developers prepare for quantum computers. oct 12nd 2019. [Quoted apr 4th 2020]. Available at: https://es.cointelegraph.com/news/bitcoin-and-ethereum-developers-prepare-cryptocurrencies-for-quantum-computing.