

Quantum Computing:

The possible growth of computing power and the consequences/repercussions that the same have on the security and privacy of users

1st Bernardo da Palma Albergaria

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
bd.albergaria@campus.fct.unl.pt*

2nd Pedro Miguel Ribeiro

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
pmg.ribeiro@campus.fct.unl.pt*

3rd Rúben André Barreiro

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
r.barreiro@campus.fct.unl.pt*

4th Tomás António Pessanha

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
t.pessanha@campus.fct.unl.pt*

5th Prof. José Legatheaux Martins

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
jalm@fct.unl.pt*

6th Prof. Paulo Orlando Lopes

*Informatics Department
Faculty of Sciences and Technology of
New University of Lisbon
(FCT NOVA - FCT/UNL), Portugal
Almada, Portugal
poral@fct.unl.pt*

Abstract—*Begun in 1950s, the research for the development of the Quantum Computing promises to break many paradigms of Classical Computing (Von Neumann's Architecture), in which can be divided into "treatable problems" and "intractable problems". The recent developments in this area, also awaken some concerns in the study of Internet's Privacy and Cybersecurity. As, the progress of research on Quantum Computing advances, it will bring powerful Computing machines with the capability of make faster computing processes and operations, and this, will take us to a huge decrease of computing process time to crack easily most of the current known standards and algorithms of, Cryptography, used in both, Symmetric Encryption and Asymmetric Encryption.*

Keywords—*Quantum Computing, Quantum Communication, Quantum Cryptography, Cryptography, Cybersecurity, Internet*

I. INTRODUCTION

This paper will focus on the evolution of the history of *Quantum Computing* in world's society and its timeline over the years. It will be reviewed the continuous and recent developments in this area of study and research, focusing more, at last, in its application on Internet's security and privacy, as also, the benefits and concerns that the same can bring to the *Cryptography* and *Cybersecurity*, as known currently. Some developments in the studies of this area as, Quantum Systems, Quantum Networks, Quantum Communications and Quantum Cryptography, will, also, be approached in this paper. Will be also discussed, the impact that *Quantum Computing* may have in *Cryptosystems*.

II. TIMELINE AND HISTORY OF QUANTUM COMPUTING

A. The beginning of the Quantum Computing and its history over the years

The research for the development of the *Quantum Computing* began as early as the 1950s when was thought in the application of the laws of *Physics* and *Quantum Mechanics* to computers.

In 1981 at a conference at MIT, the *Physicist Richard Feynman* presented a proposal for using *Quantum Systems* in *Computers*, which would then have a higher processing capacity than ordinary *Computers*. [1]

As early as 1985, *David Deutsch* of *University of Oxford* described the first *Quantum Computer*, a *Quantum Turing Machine*, it would simulate another *Quantum Computer*. [2]

In 1994, at AT & T Bell Labs, in New Jersey, the *Applied Mathematics'* Professor *Peter Shor* developed the *Shor's Algorithm*, capable of factoring large numbers at a much faster speed than *conventional computers*. [3]

In 1996, *Lov Grover*, also of *Bell Labs*, developed *Speedup*, the first algorithm for *Quantum Database Research*. In that same year, a model for the *correction of the Quantum Error* was proposed. [4]

In 1999, at MIT, the first prototypes of *Quantum Computer* were built using thermal assembly.

In 2007, was developed by the Canadian company *D-Wave Systems*, a *Quantum* 16 *qubits* processor called *Orion* that performs practical tasks.

In 2011, *D-Wave Systems* launched the first *Quantum Computer* for commercialization, the *D-Wave One*, which has a 128-*qubit* processor. But the *D-Wave One* isn't yet fully independent, it needs to be used in conjunction with *conventional computers*.

In 2017, *D-Wave Systems* commercially launched the 2000Q, a *Quantum Computer* of 2,000 *qubits* at a meager \$ 15 million. The company's previous *Quantum Computer* had 1,000 *qubits*. The *D-Wave Systems' 2000Q* is capable to perform 2,2000 operations at the same time.

In 2017, *Guilherme Tosi* from the *University of New South Wales*, invented a radical new architecture for *Quantum Computing*, based on "flip-flop *qubits*" that can be used in a new type of *Quantum Computers* thus enabling the manufacture of large-scale *Quantum processors* can become much cheaper and easier than was thought possible. [5]

In 2017, *IBM* announced a *Quantum Computer* that handles 50 *qubits*. The company is also making a 20-*qubit* system available through its *Cloud Computing* platform.

In 2018, at the *APS March 2018 Conference*, *Google* announced it has created a 72 *qubits* chip called *Bristlecone* which will serve as a basis for its demonstration of *Quantum supremacy*.

In 2019, at *New York*, *IBM* unveiled *IBM Q System One™*, the world's first integrated universal approximate *Quantum Computer System* designed for scientific and commercial use. *IBM* also announced plans to open its first *IBM Q Quantum Computation Center* for commercial clients, also in *New York*.

In 2019, a team of Physicists from *USA*, *Russia* and *Switzerland*, led by *Gordev Lesovik*, *Andrei Lebedev* and *Henning Bostelmann*, from *ETH Zurich*, "experimentally demonstrate a time reversal" in a single *electron*, sending a *qubit* from a more complicated state to a simpler one. The experiment's results from the "reversal algorithm" got a success rate of 85% in a *Quantum Computer* of 2 *qubits*, occurring more errors and dropping to a success rate to 50%, when introduced a 3rd *qubit*. [6]

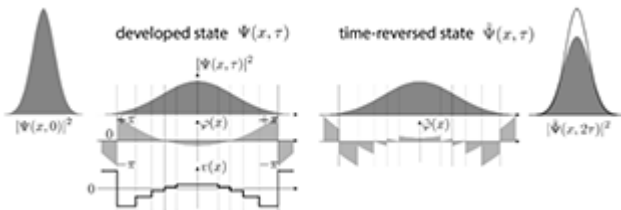


Fig. 1. The Time Reversal Procedure, using a *Quantum Computer*.

B. Principles of Quantum Computing

The *Quantum Computing* promises to break many paradigms of *Classical Computing*, in which we can divide the problems into "tractable problems", that are problems that have reasonable, polynomial-time solutions and "intractable problems", that are problems that don't have it:

TABLE I
TRACTABLE AND INTRACTABLE PROBLEMS IN CLASSICAL COMPUTING

Mathematical Notation	Complexity Time	Tractable/ Intractable
$O(1)$	Constant	Tractable
$O(\log(n))$	Logarithmic	Tractable
$O(n)$	Linear	Tractable
$O(n \times \log(n))$	N-Log-N	Tractable
$O(n^2)$	Polynomial (Quadratic)	Tractable
$O(n^3)$	Polynomial (Cubic)	Tractable
$O(k^n)$, e.g., $O(2^n)$	Exponential	Intractable
$O(n!)$	Factorial	Intractable
$O(n^n)$	Super-Exponential	Intractable

The Moore's law predicted that computing should reach its limits by 2020s, as it becomes harder to produce processors and chips, in smaller dimensions and geometries:

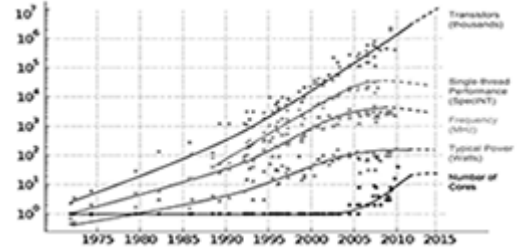


Fig. 2. The prediction of the evolution of *Computing* by *Moore's Law*.

However, it's already proved that it's possible (and feasible in the next 5 years) achieve the *Quantum Computing* that exceeds the reach of *Classical Computers*. This will mark the beginning of a new era of *Quantum Science and Computing*, at general.

All the elements that change the *Classical Structures* come from the changes that *Classical Physics* has brought. Physicists like *Heisenberg*, *Bohr*, *Schrödinger*, and *Einstein* studied these new foundations. Among them, it can be highlighted:

- *Quantum Overlap*:
 - The *Quantum Overlap* is a fundamental principle of *Quantum Mechanics* that states that a *Physical System* exists partially in all theoretically possible states simultaneously before being measured. But when measured or observed, the system is shown in a single state;

- *Schrödinger's Cat Experience:*

- The *Schrödinger's Cat* is a mental experiment, often described as a paradox, developed by *Erwin Schrödinger*, in 1935. The experiment seeks to illustrate *Copenhagen's Interpretation of Quantum Mechanics* by imagining it applied to everyday objects. In the example, there's a cat enclosed in a box, so that it's not only alive or only dead, but "undead";



Fig. 3. The *Schrödinger's Cat Experience*.

- *Quantum Entanglement or "Ghostly Action at a Distance":*

- The *Quantum Entanglement* is a phenomenon of *Quantum Mechanics* that allows two or more objects to be somehow so connected that an object can't be correctly described without its counterpart be mentioned (even though the objects may be spatially separated by millions of *light years*). This leads to very strong correlations between the observable *physical properties* of the various *subatomic particles*. The *Quantum Entanglement* was called "Ghostly Action at a Distance" by *Albert Einstein*, who believed it to be an impossible event under the laws of orthodox *Quantum Mechanics*;

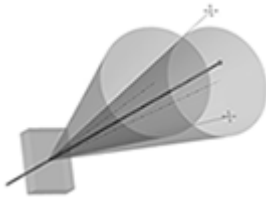


Fig. 4. *Parametric Scattering, using Quantum Entanglement*.

- *Quantum Teleportation:*

- The *Quantum Teleportation* is a technology that allows teleportation of information, such as spin or polarization (there's no transport of energy or matter) by exclusively *Quantum* means, which are independent of transmission media. The bandwidth for *Quantum Teleportation* doubled in 2015. It's a Chinese technique of transferring information about one particle so that another particle takes two instead of just one of the *Quantum* properties of the initial particle;

- *Rutherford Scattering:*

- In Physics, *Rutherford's Dispersion* is a phenomenon that was explained by *Ernest Rutherford*, in 1909, and led to the development of the *orbital theory of the atom*. It's now exploited by the *Rutherford's Dispersion Spectrometry Material Analysis* technique. The *Rutherford's Dispersion* is also sometimes referred to as *Coulomb's Dispersion* because it's based on *Electrostatic Forces (Coulomb)*. A similar process proved the core interior in the 1960s, called *Inelastic Deep Dispersion*;

- *Existence of Multiverse:*

- The *Quantum Multiverse* (also known as *Multiverse Theory* or *Many-worlds' Interpretation*) is an interpretation of *Quantum Mechanics* that asserts the objective reality of the universal wave-function and denies the actuality of wave-function collapse. The existence of the other worlds makes it possible to remove randomness and action at a distance from *Quantum Theory* and thus from all *Physics*. The *Quantum Multiverse* implies that all possible alternate histories and futures are real, each representing an actual "world" (or "universe");

And it was thanks to these principles that the development of *Quantum Computing* was possible.

III. LEARNING ABOUT QUANTUM

A. *Understanding the Quantum Computing*

The *Quantum Mechanics* is considered to be the most successful *Physical Theory*. For from its creation to the present day, it has been applied in diverse branches, from *Particle Physics*, *Atomic and Molecular Astrophysics*, and *Condensed Matter Physics*.

In *Quantum Computing*, the basic information unit's the *Quantum Bit* or *Qubit*. The fact that *Quantum Computing* it's so powerful lies in the fact that in addition to assuming zero ('0') and one ('1'), as in *Classical Computing's* memory (following the *Von Neumann's Architecture*) made up of *bits*, it can assume both zero ('0') and one ('1') states at the same time by *Quantum Superposition* of those 2 *qubit* states.

A pair of *qubits* can be in any *Quantum Superposition* of 4 states, and 3 *qubits* in any superposition of 8 states. In general, a *Quantum Computer* with *n qubits* can be in any superposition of up to 2^n different states (in comparison to a normal computer that can only be in one of these 2^n states at any one time).

It's hard to assume the two different states at the same time, but *Schrödinger's Cat's Mental Experience* can give an intuitive sense to the situation. And it's thanks to this property of the *Quantum Superposition* of states that motivated the studies in *Quantum Computing*. If in *Classical Computing*, the processing is sequential, in the *Quantum Computing*, the processing is simultaneous.

The *qubit* is described by a states' vector in a two-level *Quantum System*, which is equivalent to a two-dimensional space's vector over complex numbers. The *bra-ket's notation* is used to represent them:

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ or even, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Thus, the state of a *qubit* can be represented by:

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

The set $\{|0\rangle, |1\rangle\}$ forms a two-dimensional *Hilbert's Space* called the *Computational or Hadamard Transformed Basis*.

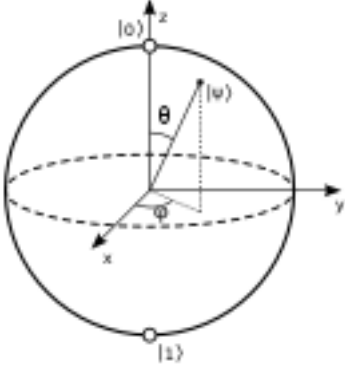


Fig. 5. Bloch Sphere representation of a Qubit.

For the manipulation of *Quantum States*, some kind of *Optical Techniques*, i.e., *Electromagnetic Radiation*, are used. These devices constitute *Quantum Logic Gates*. A *Quantum Computer* operates on its *qubits* using this *Quantum Logic Gates* and measurement (which also alters the observed state). This manipulation can be performed using *atoms* that can be excited or not, or even, the both, at the same time.

Another device used is the manipulation of *photons*. The advantage of using them lies in the fact that these *photons* can constitute highly stable carriers of *Quantum Information*.

However, *photons* don't interact directly with each other, requiring the use of an *atom* as a mediator, which introduces additional noise and complications in the experiments. In this case, a *photon* interacts with an *atom* which in turn interacts with the second *photon*, leading to the complete interaction between the two *photons*.

A *Quantum Algorithm* is composed of a fixed sequence of *Quantum Logic Gates* and a problem is encoded by setting the initial values of the *qubits*, similar to how a *Classical Computer* works.

The calculation usually ends with a measurement, collapsing the system of *qubits* into one of the 2^n *eigenstates* (or *pure states*), where each *qubit* is zero ('0') or one ('1'), decomposing into a classical state. The outcome can, therefore, be at most n classical *bits* of information. If the algorithm didn't end with a measurement, the result is an unobserved *Quantum State* (such unobserved states may be sent to other computers as part of *Distributed Quantum Algorithms*).

The *Quantum Algorithms* are often probabilistic, in that they provide the correct solution only with a certain known probability. Note that the term *non-deterministic computing* mustn't be used in that case to mean probabilistic (*computing*) because the term non-deterministic has a different meaning in *Computer Science and Informatics*.

In order to store the *qubits*, *ion's traps* are used, in which a small number of charged *atoms* are trapped, and also, *neutral ion's traps* to trap uncharged *atoms*.

In this scheme, the *photons* are used to manipulate the information contained in the *atoms*, in this way they constitute a type of *Quantum Logic Gates* that applies appropriate *pulses of electromagnetic radiation* so that the *atoms* in the neighborhood can interact with each other like via, per example, *dipole forces*.

Another class of *Quantum Information Processing* is based on *Nuclear Magnetic Resonance (NMR)*. In this case, the *Quantum Information* is stored in the *nuclear spins* of the *atoms* in *molecules* and the *Quantum Logical Gates* manipulate that information using the *electromagnetic radiation*.

This is an example of an implementation of *qubits* in a *Quantum Computer*, where could start with the use of *particles (electrons)* with two *spin states*: "down" and "up", as also, the both at the same time (typically written $|\downarrow\rangle$ and $|\uparrow\rangle$, or $|0\rangle$ and $|1\rangle$). This is true because any such system can be mapped onto an effective *spin-1/2 system*.

The *nuclear magnetic moments* make a natural *precession movement* in the presence of *magnetic fields*. The *Quantum States* of the cores can be manipulated by irradiating the cores with *radio frequency pulses* tuned to the *precession frequency* of these.

In a given compound made up of *atoms*, can be measured the resonances of the cores of some of them, without altering them, using *Nuclear Magnetic Resonance (NMR)*. It's sensitive to the interactions of the *nuclear moments* exposed to the *local electric and magnetic fields*, called *hyper-fines*. Each type of *spin* has an *angular velocity* that depends on the applied field and the exchange interaction between them.

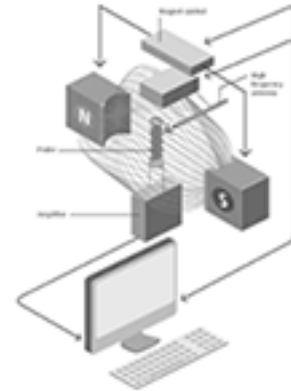


Fig. 6. Nuclear Magnetic Resonance (NMR).

Just as in *Classical Computing*, in *Quantum Computing* are used *Circuits*, but these *Circuits* are *Quantum*.

So, *logical operations* or even *algorithms*, can be described by a *Quantum Circuit*. In these *Circuits*, can be used the *Logic Gates* used in *Classical Computing*, but it's possible to use others that may allow, per example, the construction of a possible circuit for the teleportation of data.

However, in the same way that, the property of *Superposition of States* allows the creation of the *Quantum Computer*, it's this same property that makes it impossible to create them.

The difficulties of creating a *Quantum Computer* lie in the fact that the computational processes happen to be in the *atomic universe*, that lacks of technologies of manipulation still.

One of the main problems, for example, is the high error rate caused by the environment due to the extreme sensitivity of the technology. The *Superposition of States* is very sensitive to any *electromagnetic micro-disturbance* that can alter the state of the *qubit* causing the information contained in it to be lost.

Another important fact in question is the *overheating of the machines*. For that reason it's almost mandatory use this kind of systems cooled with temperatures close to "*absolute zero*".



Fig. 7. The IBM Q's *Quantum Computer*.

B. Current research in *Quantum Computing* Worldwide and in Portugal

There's no such thing as a fully functioning *Quantum Computer* today. However, companies such as *D-Wave System*, *Google* and *IBM*, among others, have made promises, which if fulfilled, will announce a new horizon for the reality and market of home, scientific and corporate computers.

Many *Quantum Computer Prototypes* have already been tested in laboratories worldwide, but their large-scale development may still be far away and dependent on much research and investment.

In 2018, the *Physics of Information and Quantum Technologies Group of the Instituto de Telecomunicações*, headquartered at *Instituto Superior Técnico*, won a total funding of € 13 million supported by *Quantum Flagship* for 2 research projects called "*Quantum Internet Alliance*" and "*Quantum Microwave Communication and Sensing*".

The "*Quantum Internet Alliance*" intends to build in the next three years, the first prototype of the future *Quantum Internet*, a network that could allow private long distance communications, as well as *Networking Quantum Computers* and *Quantum Sensor Systems*.

In this challenge, the researchers of the *Instituto Superior Técnico* have the partnership of researchers from the *Technical University of Delft*, the *Max-Planck-Institute for Quantum Optics*, the *Niels Bohr Institute* and the *Austrian Academy of Science*, among others.

For the first time, will be tried to be built a *Quantum Network* that will serve any *Quantum Application*: *Secure Communications*, *Distributed Computing*, *Quantum Sensor Networks*, etc. It's a *Quantum Internet*, never tried before.

The "*Quantum Microwave Communication and Sensing*", with the involvement of the *Walther-Meissner-Institut*, the *cole Normale Supérieure de Lyon* and *Oxford Instruments*, among others, is a fundamental research project, which is the superconductor of a program that operates at "*absolute zero*" temperature to generate interwoven *microwaves*.

The goal it's to build a system without the knowledge or interaction with itself, using *Quantum Interlacing*. This research can leads it to have important applications such as, for example, *Quantum Radars*, much more sensitive than the current radars.

Recently, the *Faculty of Sciences of University of Porto* also already adopted a course of *Quantum Computing* in their *Informatics' PhD* degree.

Also in 2018, the *QuantaLab*, led by the *University of Minho*, and composed also by, *Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)* and the *Centro de Excelência para a Inovação da Indústria Automóvel (CEiIA)*, started to be part of the largest international *Quantum Computing Network*, entering into the *IBM Q Network*, as an academic partner.

In 2019, the *Fundação para a Ciência e Tecnologia*, launched an initiative called *Quantum Portugal* aiming to attract new researchers for *Quantum Computing*, with the funding of *PhD* scholarships.

The goal of this initiative it's, essentially, the *Creation of New Medicines and Materials*, *Financial Risk Analysis*, *Inventory Management*, *Facial Recognition*, *Artificial Intelligence*, as also, *Simulation and Testing of, Condensed Matter Physics*, *Materials Science*, *Process Optimization* and *Cybersecurity*.

This contest will be managed by the *Laboratório Ibérico Internacional de Nanotecnologia* and will make their infrastructures available, as a host institution for *PhD* students from universities over all Portugal.

Also, in 2019, *Miguel Ramalho*, of *Faculty of Engineering of University of Porto* won the "*IBM Q Teach Me Quantum*", initiative that challenges the creation of a course in *Quantum Computing* that integrates the tools developed by *IBM* in recent years.

C. Understanding (better) the Quantum Bit (or Qubit)

Since, a *Quantum State* can represent 2 states, at the same time, it's reasonable to think that a *qubit* also could represent 2 *bits*, at once. So, n *qubits* can be represented as 2^n *bits*.

For comprehension of the *computational power* that will be analysed, consider some statistics from *StatSoft's Statistica*:

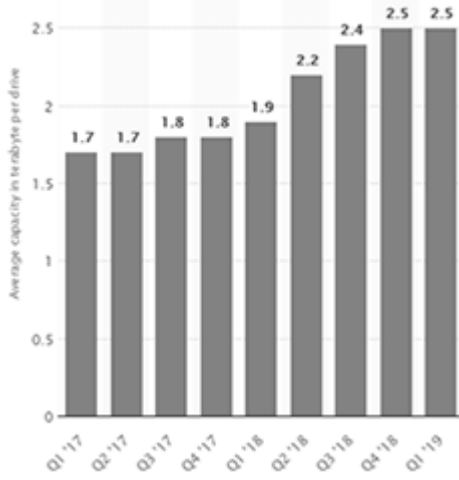


Fig. 8. Average capacity of *Seagate Hard Disk Drives* worldwide from 2017 to 2019, by quarter (in *terabyte per drive*).

This statistics revealed that the average capacity of *Seagate's Hard Disk Drives*, at the first quarter of 2019 year was approximately 2.5 *terabytes* per drive.

The following table shows the increase of the data that can be processed and kept by *qubits*, in comparison to *bits*:

TABLE II
COMPARISON OF QUANTUM VALUES (SUPERDENSE CODING)

<i>Qubits (Quantum Bits) vs. Bits</i>	
# Qubits	# Bits
1 qubit	2 bits
2 qubits	4 bits
3 qubits	8 bits = 1 B
4 qubits	16 bits
5 qubits	32 bits
6 qubits	64 bits
7 qubits	128 bits
8 qubits	256 bits
9 qubits	512 bits
10 qubits	1,024 bits
13 qubits	8,192 bits \approx 1 KB
23 qubits	8,388,608 bits \approx 1 MB
33 qubits	8,589,934,592 bits \approx 1 GB
43 qubits	8,796,093,022,208 bits \approx 1 TB
44 qubits	17,592,186,044,416 bits \approx 2 TBs
45 qubits	35,184,372,088,832 bits \approx 4 TBs
50 qubits	1,125,899,906,842,624 bits \approx 128 TBs
72 qubits	4,722,366,482,869,645,213,696 bits \approx \approx 536,870,912 TBs \approx 512 EBs \approx 0.5 ZBs
2,000 qubits	\approx 1.15×10^{602} bits \approx 1.44×10^{586} TBs \approx \approx 1.44×10^{579} EBs \approx 1.44×10^{576} ZBs \approx \approx 1.44×10^{573} YBs \approx 144,000,000,000 \times 10^{562} YBs
n qubits	2^n bits

Following the statistics from *StatSoft's Statistica*, at average, each *classic computer* would have a *HDD* of 2.5 *terabytes* of capacity. A *Quantum chip* of 72 *qubits*, such as *Bristlecone*, would be $214,748,364 \times$ more powerful than each one of them.

In another perspective, could be thought that was predicted that, the volume of the entire *Internet* in the world, in 2016, would be 1.3 *zettabytes*. The same *Quantum chip* of 72 *qubits* would represent almost half of this huge amount of data.

So, it's unthinkable the computing power that a *Quantum Computer*, as *D-Wave's 2000Q* could have. A huge quantity of the problems that *classic computers* couldn't resolve at a reasonable time, would be resolved easily, at polynomial-time.

IV. QUANTUM COMPUTING IN SECURITY OF INTERNET AND WORLD WIDE WEB (WWW)

A. How can Quantum Computing impact Internet's Security?

The main limitation of *Symmetric Cryptography* is the keys' distribution, since after their generation they've to be sent to the endpoints. Although, the message with the key can also be intercepted and would need a secure means to be sent.

In the 1970s, with the development of systems that used *Asymmetric Cryptography*, the problem became semi-resolved, since it would no longer be necessary to distribute the keys.

Currently, the most common *Public Key Cryptosystem*, the *Rivest-Shamir-Adleman (RSA)*, is based on numbers' factorization, that only offer some safety due to the current computational limitation, such as the difficulty of factorization of large prime numbers, discrete logarithms, among others.

Improved approaches to factoring large numbers, such as *Shor's Algorithm* running on a sufficiently powerful *Quantum Computer*, will improve the likelihood of breaking an algorithm of *Public-Key Encryption*.

The *Quantum Computing* offers the potential for breaking the *Public-Key Encryption* standards that protect all of the data, safely stored, shared and used, through the *Internet*.

The following table provides which of these encryption algorithms are breakable using current *Quantum Computing*:

TABLE III
ENCRYPTION ALGORITHMS BREAKABLE FROM QUANTUM COMPUTING

Encryption Algorithm	Security against <i>Quantum Computing</i>
Asymmetric (Public and Private) Key Encryption	
3DES	Insecure
AES-128	Insecure
AES-256	Secure
Symmetric Key Encryption	
RSA-1024, RSA-2048, RSA-4096	Insecure
ECC-256, ECC-512	Insecure
Diffie-Hellman	Insecure
Elliptical Curve Diffie-Hellman	Insecure

The previous table, demonstrates that, the long-term *security* offered by many *Cryptosystems* is under severe threat.

In opposite way, could be built safest *Cryptosystems*, through *Quantum Networks*, *Quantum Communications*, *Quantum Cryptography* and *Quantum Key Distribution*.

B. The beginning of the Quantum Cryptography and its history over the years

The *Quantum Cryptography* begun by the work of both, *Stephen Wiesner* and *Gilles Brassard*. In the early 1970s, *Wiesner*, at *Columbia University*, introduced the concept of *Quantum Conjugate Coding*.

This concept was introduced in a paper titled "*Conjugate Coding*" which was rejected by the *IEEE Information Theory Society*, but eventually published at *SIGACT News*, in 1983.

The paper showed how to store or transmit 2 messages by encoding them in 2 "conjugate observables", such as linear and circular polarization of photons, so that either, but not both, of which may be received and decoded.

It wasn't until *Charles Bennett*, of the *IBM's Thomas J. Watson Research Center* and *Gilles Brassard* met at the 20th *IEEE Symposium held in Puerto Rico* that they discovered how to incorporate the findings of *Wiesner*.

The main breakthrough came when they realized that photons were never meant to store information, but rather to transmit it.

In 1984, building upon this work *Bennett* and *Brassard* proposed a method for secure communication, which is now called *BB84 Protocol*.

In 1991, *Artur Ekert* developed a different approach to *Quantum Keys Distribution* based on peculiar *Quantum Correlations*, known as, *Quantum Entanglement*.

In 2005, random rotations of the polarization by both parties have been proposed in *Kak's Three-Stage Protocol*. In principle, this method can be used for continuous, unbreakable encryption of data if single *photons* are used.

C. Understanding the Quantum Cryptography

The *Quantum Communication* doesn't require prior secret communications, allows the detection of intruders, and is safe even if the attacker has unlimited computational power.

Thus, this *Cryptography* method would be safer than currently used because it's based on laws of *Physics* and on the *Quantum Communication*. In fact, it's completely secure, except in situations where the intruder can remove and insert messages from the *broadcast channel*.

The *Heisenberg's Uncertainty Principle* assures that it's not possible to simultaneously determine all the physical states of a *micro-particle* without interfering or altering it. The *Quantum Communication* involves encrypting information in *qubits*, rather than the *bits* used in classical communication. In this case, normally, *photons* are used as *qubits*.

In the same way, a person in the middle of a *Cryptography* attack, specifically while exchanging the *encryption key* can be ruled out by use of *Quantum Computing* because it's impossible to eavesdrop on a connection if it's based on a single *micro-particles* transmission, since measuring one parameter of a *micro-particle* will alter another parameter of the same.

Each attempt of espionage or interception of messages on a *Quantum Communication* will alter the transmitted message. In *Quantum Communications*, significant interference means that an unwanted third party is monitoring the connection.

The algorithm most commonly associated with *Quantum Cryptography* is the *One-Time Pad (OTP)*, since it has proven to be a perfect security when used with a random key and the same size as the message.

It's important to note that *Quantum Cryptography* will only be used to produce and distribute the keys, not to transmit the messages. The generated key with the *Quantum Cryptography* can be used with any encryption algorithm. This introduces a new concept known as *Quantum Key Distribution (QKD)*.

D. Quantum Keys Distribution (QKD)

The *Quantum Cryptography* exploits certain properties of these *Quantum States* to ensure their safety. There are different ways of *Quantum Keys Distribution (QKD)*, but they can be divided into two main categories, depending on which property they use:

Protocols to Prepare and Measure:

- Unlike *Classical Physics*, the act of measuring is an important part of *Quantum Mechanics*. In general, measuring an unknown *Quantum State* will modify that state in some way. This can be exploited to detect an intruder in communication, which will necessarily have to measure a *Quantum State* and eventually change it;

Quantum Entanglement Based Protocols:

- The *Quantum State* of 2 (or more) separate objects may become connected in such a way that they've to be described as a matched *Quantum State*, not as individual objects. This is known as *Quantum Entanglement* and means, for example, that performing a measurement on one object will affect the other. If a pair of tangled objects is shared by sender and receiver, anyone attempting to intercept one of the *particles* will alter the entire system, allowing its presence to be detected;

The basic polarization rotation scheme on the *Kak's Three-Stage Protocol* has been implemented and represents a method of purely *Quantum Cryptography* as against *Quantum Keys Distribution (QKD)* where the actual *encryption* is classical. Note also that, the *BB84 Protocol* is at the basis of *Quantum Keys Distribution (QKD)* methods.

Additionally, the *E91 Protocol* created by *Ekert*, which uses entangled pairs of *photons*. The *photons* are distributed so that the two endpoints each end up with one *photon* from each pair.

E. The Current State of Quantum Cryptography

The application of the theory of *Quantum Cryptography* has already been performed in the laboratory among others by *IBM*. However, only satisfactory results were obtained for short distances between the emitter and the receiver.

High-purity *fiber optic cables* were able to communicate at a distance of around 70km. At a greater distance, the *bit error rate*, caused by the "*Heisenberg Uncertainty Principle*" and microscopic impurities in the *optical fiber*, grows and makes the method inapplicable.

Communication through air was also tested, which was only successful with distances of 200m and with ideal climatic conditions. It's hoped that technological development will allow these distances to grow.

Some companies already manufacture *Quantum Cryptography Systems*, such as *MagiQ Technologies, Inc.*, in USA, *ID Quantique (IDQ)*, in Switzerland, *QuintessenceLabs*, in Australia and *SeQureNet*, in France.

The *ID Quantique*, commercialize devices that perform *Quantum Cryptography*. The *NOW Wireless* has entered into a contract to distribute the *MagiQ QPN Gateway*, a "*Migic-Qtech*" *Quantum Encryption* solution that allows communication over 120km of distance.

According to the "*New Scientist*" magazine, a project called "*Quantum Network (Qnet)*" is being operated in the *Massachusetts, USA* and is funded by the *Defense Advanced Research Projects Agency (DARPA)*. Currently, this project has only 6 servers, but can connect to other servers through the *Internet* and using *Quantum Cryptography*. The objective of this project is to use this technology in credit companies, banks and other financial services that enable their clients to make electronic transactions. The network is 10km in extension and connects *BBN* to *Harvard University* through standard fiber optic cables.

F. Some challenges on Communication with Quantum Cryptography and Cybersecurity

Being this a recent and expanding area, the same has many theoretical and practical challenges that need to be addressed so that *Quantum Communications* can grow. Some of the main challenges are:

- The development of *photon* sources of small size and low cost;
- The development of *Quantum* repeaters to increase the reach among users of a *Quantum Network*;
- The development of new *Quantum Cryptography Protocols* using *Quantum Systems* with more than 2 states;
- The development of new *Public Key Distribution, Authentication, and Digital Signature* protocols;
- The promotion of the integration of the *Quantum Network* with the existing infrastructure;
- The training of *Quantum Hackers* to test the security of the new protocols developed;

This, also, directly impacts the technology buying decisions of *Chief Information Security Officers (CISOs)* and *Chief Technology Officers (CTOs)* today, because privacy legislation requires information like medical records to be kept confidential even after a person dies (The German law stipulates that medical and legal data remain confidential from third parties even after the death of a patient or client).

This means that a buyer of *encryption products* will start to face two choices:

- Purchase a *cryptosystem* that's secure for long-term but only a minority of systems currently meet this requirement. They can be easily identified by their name, either *quantum resistant* or *post-quantum cryptography*;
- Purchase a *cryptosystem* that's not long-term secure, and accept that *encrypted data* will only remain confidential until about another decade or so;

CONCLUSIONS

So, in conclusion, it's reasonable to think that, the *Quantum Computing* can be, at the same time, the redemption and the destruction of the *Cryptography* and, *Cybersecurity*, as also, *Internet's Security and Privacy*, as is known currently.

REFERENCES

- [1] Richard P. Feynman, "Simulating Physics with Computers", *International Journal of Theoretical Physics*, Vol. 21, Nos. 6/7, May 1981.
- [2] David Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proceedings of the Royal Society of London A* 400, pp. 97-117, July 1984.
- [3] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, IEEE Computer Society Press, pp. 124134, November 1994.
- [4] Lov K. Grover, "A fast quantum mechanical algorithm for database search", *Proceedings, STOC 1996*, Philadelphia PA, USA, pages 212-219, November 1996.
- [5] Guilherme Tosi, Fahd A. Mohiyaddin, Vivien Schmitt, Stefanie Tenberg, Rajib Rahman, Gerhard Klimeck & Andrea Morello, "Silicon quantum processor with robust long-distance qubit couplings", *Nature Communications* vol. 8, Article number: 450, September 2017.
- [6] G. B. Lesovik, I. A. Sadovskyy, M. V. Suslov, A. V. Lebedev & V. M. Vinokur, "Arrow of time and its reversal on the IBM quantum computer", *Scientific Reports* vol. 9, Article number: 4396, March 2019.

This paper was made in \LaTeX and \LaTeX during the course of Social-Professional Aspects of Informatics (2018/2019) of the Integrated Master of Computer Science and Engineering at Faculty of Sciences and Technology of New University of Lisbon (FCT NOVA - FCTUNL), Portugal

This paper it's hosted in the following GitHub's Repository/Host Service hyperlink:
<https://github.com/rubenandrebarreiro/quantum-computing-security-and-privacy-of-users>

Some papers, articles and slides of Quantum Computing, as also, experiments and tutorials of Quantum Programming, using QisKit and IBM Q Experience are hosted in the following GitHub's Repository/Host Service hyperlink:
<https://github.com/rubenandrebarreiro/learning-quantum-computing>