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 very easily some of the current most known standards and algorithms of *Cryptography*.**

***Index Terms*—Quantum Computing, Cryptography, Cybersecurity, Internet, Privacy**

I. Introduction

This article/paper will focus in the evolution of the history's timeline of the *Quantum Computing* in world's society, focusing more in its application on Internet's security and privacy, as also, the benefits and concerns to the *Cryptography* and *Cybersecurity*.

II. Timeline and History

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*.

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*.

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*.

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.

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* and a team of researchers 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.

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 *U.S.A.*, *Russia* and *Switzerland*, led by *Gordey Lesovik*, *Andrei Lebedev* and *Henning Bostelmann*, *"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*.

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**

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 is a cat enclosed in a box, so that it is not only alive or only dead, but "undead";

Fig. 1. 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*;

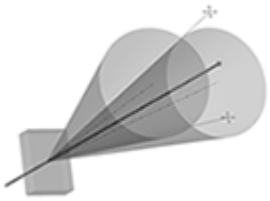

Fig. 2. How Quantum Entanglement works.

- *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 is 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 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 to Astrophysics* and *Condensed Matter*.

In *Quantum Computing*, the basic information unit is 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 three *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 (this compares 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:

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

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

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

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

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*, 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 Gate* 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* (*N.M.R.*). 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 $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$). This is true because any such system can be mapped onto an effective *spin-*$\frac{1}{2}$ *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 different atoms one can measure the resonances of the cores of some *atoms* without altering them, using *Nuclear Magnetic Resonance* (*N.M.R.*). It's sensitive to the interactions of the *nuclear moments* exposed to the *local electric* and *magnetic fields*, these interactions are called *hyper-fines*. Each type of spin has an angular velocity that depends on the applied field and the exchange interaction between them.

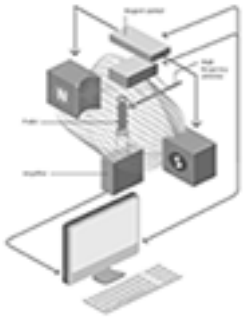

Fig. 3. Nuclear Magnetic Resonance (N.M.R.).

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

- **Input**: *The input qubits are considered together, mathematically what is called their tensor product*;
- **Horizontal Lines**: *The lines that appear aren't necessarily wires. They represent the evolution of a qubit, which may be only the passage of time or, for example, the displacement of a photon*;
- **Direction**: *The circuit describes the evolution of the quantum system in time, from left to right*;
- **Vertical Lines**:
  - *The vertical segment informs that the circuit acts simultaneously on both qubits. The vertical line represents the synchronization, not the sending of information*;
- **Control**:
  - *Indicates that the qubit represented in this line is a control qubit, that is*:
    - *If it's in the* $|\mathbf{1}\rangle$ *state, the port performs the operation*;
    - *If it's in the* $|\mathbf{0}\rangle$ *state, the port doesn't perform any operation*;
    - *If the control qubit is a superposed state or the 2 qubits are entangled, it's not possible to understand the individual behavior of the control qubit and the target qubit*;
    - *Must be considered the action of the unit operator, which represents the entire circuit, acting simultaneously on the 2 qubits*;
- **Output**:
  - *The qubits that make up the circuit output may or may not be measured*;
  - *As the lower qubit is being measured, the result will be zero (**'0'**) or one (**'1'**)*;

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 *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*. It's for that reason that it's almost mandatory use this kind of systems cooled with temperatures closer to *"absolute zero"*.

Actually, it's possible to perform any *classical operation* using only ***NAND*** ports. The same occurs in *Quantum Circuits* where the ports are:

- Hadanard (H)
- Controller (CNOT)
- Phase (S)
- $\frac{\pi}{8}$(T)

Some examples of *Quantum* ports are:

- *Quantum* ***NOT*** port:
  - In the *classic* case, the ***NOT*** port changes the zero ('0') by one ('1'), and vice versa;
  - The generalization for the *Quantum* case is given by an operator $\boldsymbol{X}$ that satisfies:
    $$* \quad \boldsymbol{X}|\mathbf{1}\rangle = |\mathbf{0}\rangle \textbf{ and } \boldsymbol{X}|\mathbf{0}\rangle = |\mathbf{1}\rangle$$
  - With this, it's easy to verify that the matrix representation of the operator $\boldsymbol{X}$ is given by:
    $$* \quad \boldsymbol{X} = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}$$
  - With the *Quantum* ***NOT*** port, there are unmatched situations in the *classical case*, because if the input $|\phi\rangle$ is a *Quantum Superposition* of the states $|0\rangle$ and $|1\rangle$:
    $$* \quad |\phi\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \ ,$$
    the output will be:
    $$* \quad \boldsymbol{X}|\phi\rangle = \beta|\mathbf{0}\rangle + \alpha|\mathbf{1}\rangle \ ;$$
  - The $\boldsymbol{X}$ port is just one of the 1 *qubit* ports, since there are infinite unit arrays of $\mathbf{2}\times\mathbf{2}$;
- *Quantum* ***CNOT*** port:
  - It operates in 2 *qubit* states, is the *Quantum* counterpart of the *Classic* ***XOR*** *Gate Circuit*;
  - It has 2 *input qubits*, the *control* and the *target*;
  - A *controlled port* acts depending on the value of the *control qubit*;
  - This port it's "enabled" if the *control qubit* it's in the $|\mathbf{1}\rangle$ state, and does nothing if it's in the $|\mathbf{0}\rangle$ state;
  - This description is appropriate only when the *control qubit* it's in the states $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$;
  - However, what distinguishes the *Quantum* ***CNOT*** *Gate* from the *classical* one is that, in the *Quantum* ***CNOT*** *Gate*, the *target* and *control qubits* may be overlapping states;
  - The action of the ***CNOT*** port can be characterized by the transformations carried out in the elements of the associated computational base, *i.e.*:
    $$* \ |\mathbf{00}\rangle \rightarrow |\mathbf{00}\rangle$$
    $$* \ |\mathbf{01}\rangle \rightarrow |\mathbf{00}\rangle$$
    $$* \ |\mathbf{10}\rangle \rightarrow |\mathbf{11}\rangle$$
    $$* \ |\mathbf{11}\rangle \rightarrow |\mathbf{10}\rangle$$
  - Note that it's possible to represent this action in the *computational base* in a more schematic form by:
    $$* \ |\boldsymbol{i,j}\rangle \rightarrow |\boldsymbol{i,i} \oplus \boldsymbol{j}\rangle,$$
    where $\boldsymbol{i,j} \in \{\mathbf{0,1}\}$ and $\oplus$ it's the *addition module 2*;

B. Current research in Quantum Computing Worldwide and in Portugal

There is no such thing as a fully functioning quantum computer today. However, companies such as the Canadian *D-Wave System* and the Americans *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 around the world, but their large-scale development may still be far away and dependent on much research and investment.

In 2018, the *Group of Physics of Information and Quantum Technologies of the Institute of Telecommunications (IT)*, headquartered at *Instituto Superior Técnico*, in *Lisbon*, won a total funding of € 13 million supported by *Quantum Flagship* for two research projects called *"Quantum Internet Alliance"* and *"Quantum Microwave Communication and Sensing"*.

The *"Quantum Internet Alliance"* project, worth € 10 million, 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*, in *Netherlands*, the *Max-Planck-Institut for Quantum Optics*, in *Munich* (*Germany*), the *Niels Bohr Institute*, in *Copenhagen* (*Denmark*) and the *Austrian Academy of Science*, among others.

This is the first time, that 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 indeed a *Quantum Internet*, never tried before.

Also in 2018, the Portuguese consortium *QuantaLab*, led by the *University of Minho*, in *Braga* and composed of three other entities, started to be part of the largest international *Quantum Computing Network*. With the entry into the *IBM Q Network*, as an academic partner, this consortium puts the name of *Portugal* for the first time in what is seen as one of the great technologies of the future.

In 2019, the *F.C.T.* (*Foundation for Science and Technology* or, *Fundação para a Ciência e Tecnologia*, in Portuguese) launched an initiative called *Quantum Portugal* that aims 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 or Artificial Intelligence*.

This contest will be managed by the *I.N.L.* (*Iberian International Nanotechnology Laboratory* or, *Laboratório Ibérico Internacional de Nanotecnologia*, in Portuguese), also in *Braga* and will make their infrastructures available to all universities in *Portugal*, as a host institution for *PhD* students from universities all over the country.

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

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.

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

After a long explanation of the *Quantum Computing*'s properties, it's already possible to see some of its applications in the present and possible (near) future of *Computer Science* and *Informatics*.

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

For a better comprehension of the amounts of *computing processing* that will be analysed in this *subsection*, will be considered some statistics collected from *Dell's Statistica* (an advanced analytics software package originally developed by *StatSoft*, which was acquired by *Dell*, in 2014).

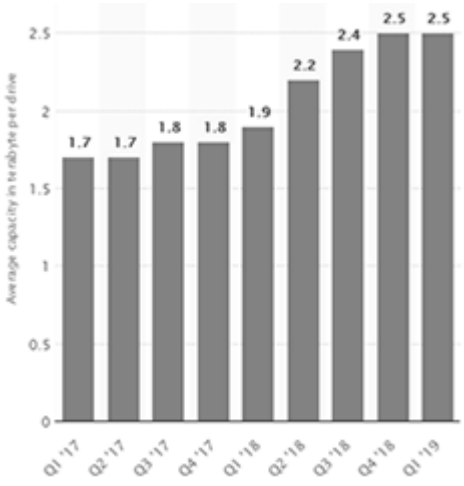

Fig. 4. Average capacity of Seagate hard disk drives (HDDs) worldwide from FY2017 to FY2019, by quarter (in terabyte per drive).

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

To see clearly, the increase of data and information, that can be kept in a *qubit*, the following table illustrates a simple comparison of Quantum Values (*SuperDense Coding*, most precisely, *Quantum Bits* vs. *Classical Bits*):

TABLE II
COMPARISON OF QUANTUM VALUES (SUPERDENSE CODING, MOST PRECISELY, QUANTUM BITS VS. CLASSICAL BITS)

Qubits (Quantum Bits)* vs. *Bits	
# Qubits	**# Bits**
1 qubit	2 bits
2 qubits	4 bits
3 qubits	8 bits = 1 byte
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 kilobyte
23 qubits	8,388,608 bits $\approx$ 1 megabyte
33 qubits	8,589,934,592 bits $\approx$ 1 gigabyte
43 qubits	8,796,093,022,208 bits $\approx$ 1 terabyte
44 qubits	17,592,186,044,416 bits $\approx$ 2 terabytes
45 qubits	35,184,372,088,832 bits $\approx$ 4 terabytes
50 qubits	1,125,899,906,842,624 bits $\approx$ $\approx$ 128 terabytes
72 qubits	4,722,366,482,869,645,213,696 bits $\approx$ $\approx$ 536,870,912 terabytes $\approx$ $\approx$ 512 exabytes $\approx$ $\approx$ 0.5 zettabytes
2,000 qubits	$\approx 1.1481\times10^{602}$ bits $\approx$ $\approx 1.4351\times10^{586}$ terabytes $\approx$ $\approx 1.4351\times10^{579}$ exabytes $\approx$ $\approx 1.4351\times10^{576}$ zettabytes $\approx$ $\approx 1.4351\times10^{573}$ yottabytes $\approx$ $\approx 143{,}510{,}000{,}000\times10^{562}$ yottabytes
n qubits	2^n bits

So, in reference to the previously mentioned statistics collected from *Dell's Statistica* and believing that, every person, worldwide, that have a *conventional computer* (as a *Desktop* or a *Laptop*) with a *Hard Disk Drive* of 2.5 *terabytes* of capacity, at average. A *Quantum Computer* with a *Quantum chip* of 72 *qubits* (like *Google* claimed, in 2018) would be 214,748,364$\times$ more powerful than the most of the current globally used *conventional computers*' computing processing capabilities.

In another perspective, which can be analysed, is also to think that was predicted that in 2016, the volume of the entire Internet in the world would be 1.3 zettabytes. The same *Quantum chip* of 72 *qubits* from *Google* would represent almost half of this huge amount of data.

So, it's possible to imagine the processing power that a *Quantum Computer*, as *D-Wave's 2000Q* could have. A huge quantity of the problems that *conventional computers* couldn't resolve at a reasonable time or couldn't resolve at all, would be resolved very easily and fast, at a linear or polynomial time.

After understanding the previously principles about *Quantum Computing* and *Quantum Bits*, it's reasonable to say that *Quantum Computing* may have some powerful applications in *Computer Science* and *Informatics* in a near future, in some areas as, *Quantum Programming*, *Quantum Processors*, *Cloud-based Quantum Computing*, *Quantum Networks*, *Quantum Cryptography*, *Quantum Machine Learning*, among many others.

IV. Quantum Computing in Internet's Security

A. How can Quantum Computing affect Cryptography and Cybersecurity?

As was previously said, the *Quantum Computing* can have a lot of applications in *Computer Science* and *Informatics*. In this article/paper, it will be focused just on its applications in *Cryptography* and *Cybersecurity* and some related concerns that it can, possibly, awake in the future.

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

TABLE III
Encryption Algorithms breakable from the current Quantum Computing

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

Article/Paper made in TEX
for 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 - FCT/UNL*)

This Article/Paper it's hosted in the following *GitHub*'s Repository/Host Service hyperlink:

- https://github.com/rubenandrebarreiro/quantum-computing-security-and-privacy-of-users