



Quantum Computing

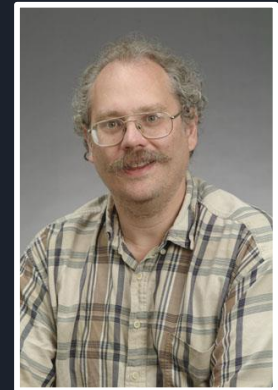
The possible growth of computing power and the consequences/repercussions that the same have on the security and privacy of users

Presented by:

- Bernardo da Palma Albergaria (no. 41931)
- Pedro Miguel Ribeiro (no. 43594)
- Rúben André Barreiro (no. 42648)
- Tomás António Pessanha (no. 41774)

Timeline and History of Quantum Computing over the Years [1]

- 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, *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* described the first *Quantum Computer*, a *Quantum Turing Machine*, it would simulate another *Quantum Computer*.
- In 1994, *Peter Shor* developed the *Shor's Algorithm*, capable of factoring large numbers at a much faster speed than *conventional computers*.





Timeline and History of Quantum Computing over the Years [2]

- In 1996, *Lov Grover*, 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, the first prototypes of *Quantum Computer* were built using thermal assembly.
- In 2007, was developed by *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*.



Timeline and History of Quantum Computing over the Years [3]

- 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 this year, *Guilherme Tosi*, 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.
- Also 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.



Timeline and History of Quantum Computing over the Years [4]

- In 2018, *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, *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, in New York.
- Also in 2019, a team of Physicists 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 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*.

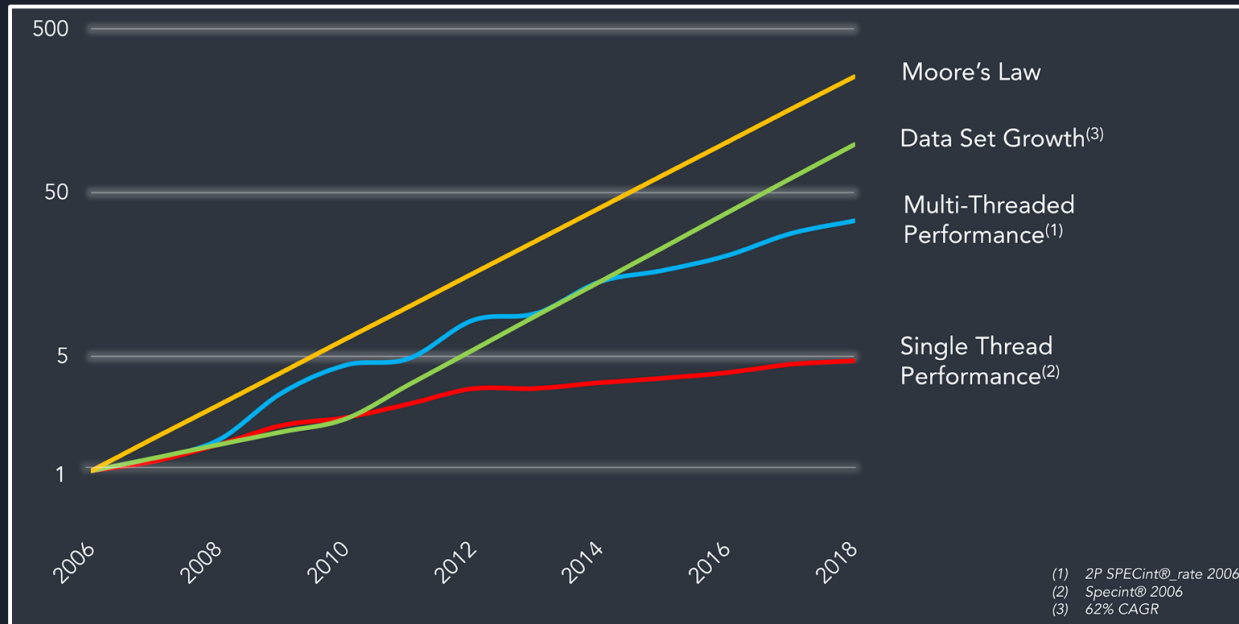
Tractable and Intractable Problems

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

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

Moore's Law

- 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:



Rate of CPU
Performance
Increase is
Slowing



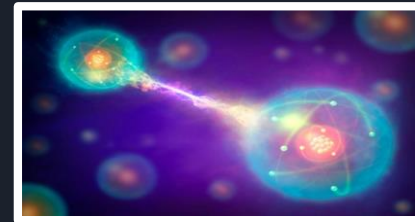
<https://cdn.wccftech.com/wp-content/uploads/2018/10/Intel-9th-Gen-Core-1-Custom-740x494.jpg>

Principles of Quantum Computing [1]

- The principles of *Quantum Computing*, come from some foundations of *Classical Physics*, where it can be highlighted:
 - 1) *Quantum Overlap*:
 - A partially existence of a *Physical System* in all theoretically possible states simultaneously before being measured. But when measured or observed, the system is shown in a single state;
 - 2) *Schrödinger's Cat Experience*:
 - An experiment seeking to illustrate *Copenhagen's Interpretation of Quantum Mechanics*, applied to a cat enclosed in a box, so that it's not only alive or only dead, but "undead";
 - 3) *Quantum Entanglement* or "*Ghostly Action at a Distance*":
 - Two or more objects to be somehow so connected that an object can't be correctly described without its counterpart be mentioned (even if may be spatially separated by millions of light years).



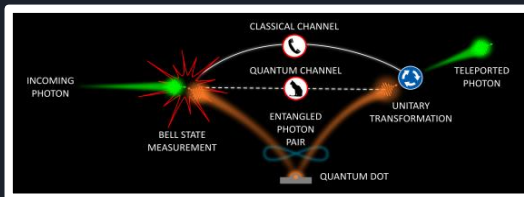
<http://astronimate.com/wp-content/uploads/2017/03/schrodingers-cat-explained-setup.jpg?x70168>



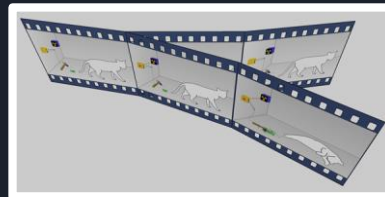
<http://www.astronomy.com/-/media/Images/News%20and%20Observing/News/2018/08/quantumentanglement.jpg?mw=600>

Principles of Quantum Computing [2]

- The principles of *Quantum Computing*, come from some foundations of *Classical Physics*, where it can be highlighted:
 - 4) *Quantum Teleportation*:
 - A technology that allows teleportation of information, such as spinor polarization, (there's no transport of energy or matter) with the help of classical communication.
 - 5) *Rutherford Scattering*:
 - A phenomenon that led to the development of the orbital theory of the atom. It's now exploited by the *Rutherford's Dispersion Spectrometry Material Analysis* technique.
 - 6) *Existence of Multiverse*:
 - An interpretation 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*.



https://www.phys.uniroma1.it/fisica/sites/default/files/teleportation%20highlight_3.1%20-%20Rinaldo%20Trotta.png



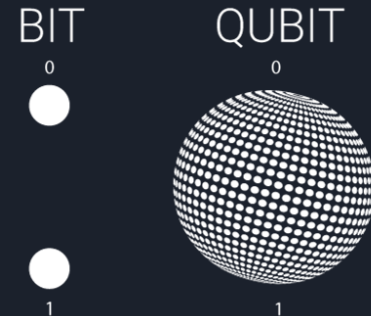
https://upload.wikimedia.org/wikipedia/commons/b/b7/MWI_Schrodingers_cat.png

The existence of many "worlds", could explain also the *Schrödinger's Cat Experience*:

- In this case, in one "world", the cat would be alive and in the another, the cat would be dead.

The Quantum Bit or Qubit

- In *Quantum Computing*, the basic information unit is the *Quantum Bit* or *qubit*.
- The reason why *Quantum Computing* is so powerful lies in its capacity to represent *both the zero ('0') and one ('1') states* at the same time, via *Quantum Superposition* of those 2 states, instead of a single state, such as in *Classic Computing*.
- 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.
- The *Schrödinger's Cat Experience* may give some insight into this situation, as the titular cat is in a *Quantum Superposition* state. In *Quantum Computing*, the processing is simultaneous, instead of sequential as in *Classical Computing*.



The power of Quantum Computing

- The following table shows the increase of data that can be processed and represented by *qubits*, compared to *bits*:

As a practical example, the volume of information in the entire Internet, in 2016, was estimated at 1.3 zettabytes.

72 qubits (0.5 zettabytes) would represent almost half of this huge amount of data.

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

Qubits (Quantum Bits) vs. Bits	
# Qubits	# Bits
13 qubits	8,192 bits ≈ 1 kilobyte
23 qubits	8,388,608 bits ≈ 1 megabyte
33 qubits	8,589,934,592 bits ≈ 1 gigabyte
43 qubits	8,796,093,022,208 bits ≈ 1 terabyte
44 qubits	17,592,186,044,416 bits ≈ 2 terabytes
45 qubits	35,184,372,088,832 bits ≈ 4 terabytes
50 qubits	1,125,899,906,842,624 bits ≈ 128 terabytes
72 qubits	4,722,366,482,869,645,213,696 bits ≈ 536,870,912 terabytes ≈ 512 exabytes ≈ 0.5 zettabytes
2,000 qubits	1.15×10^{602} bits ≈ 1.44×10^{586} terabytes ≈ 1.44×10^{579} exabytes ≈ 1.44×10^{576} zettabytes ≈ 1.44×10^{573} yottabytes ≈ $144,000,000,000 \times 10^{562}$ yottabytes
n qubits	2^n bits

How can Quantum Computing impact Internet Security?

- With the huge computational power offered by *Quantum Computing*, some of the currently used *Encryption Algorithms*, aren't secure anymore.

This table demonstrates that the long-term security offered by many cryptosystems is under severe threat.


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, RSA-2048, RSA-4096	Insecure
ECC-256, ECC-512	Insecure
Diffie-Hellman	Insecure
Elliptical Curve Diffie-Hellman	Insecure

However, *Quantum Systems* would allow us to build safer *Cryptosystems*, through *Quantum Networks*, *Quantum Communications*, *Quantum Cryptography* and *Quantum Key Distribution*, using the added computational power to create longer secret keys and generating them faster, creating more secure communications.



Some challenges on Communication with Quantum Cryptography and Cybersecurity [1]

- Being a recent and expanding area, it has many theoretical and practical challenges that need to be addressed so that *Quantum Communication* can grow. Some of the main challenges are:
 - Development of photon sources of small size and low cost;
 - Development of *Quantum* repeaters to increase the reach of a *Quantum Network*;
 - Development of new *Quantum Cryptography Protocols* using *Quantum Systems* with more than 2 states;
 - Development and dissemination of new *Public Key Distribution, Authentication, and Digital Signature protocols*;
 - Promoting the integration of *Quantum Networks* with existing infrastructure;
 - Training specialised *Quantum Hackers* to test the security of newly developed protocols.



Some challenges on Communication with Quantum Cryptography and Cybersecurity [2]

- This also has a direct impact on the buying decisions of *Chief Information Security Officers (CISOs)* and *Chief Technology Officers (CTOs)* today, because privacy legislation often requires information like medical records to be kept confidential even after a person dies (e.g., *German* law stipulates that medical and legal data remain confidential from third parties even after the death of a patient or client).
- A buyer/adopter of *encryption products* will then face two choices:
 - Purchase a *cryptosystem* that's secure in the long-term, but less widely deployed, and with a smaller selection; such *cryptosystems* may be easily identifiable as *quantum resistant* or *post-quantum cryptography*;
 - Purchase a *cryptosystem* that's not secure against quantum-based attacks, and accept that encrypted data will only remain confidential until *quantum computers* are readily accessible.



Social, Ethic and Moral Analysis of Quantum Cryptography [1]

- Socially, it's possible to argue that the applications based on *Quantum Computing* will be good, at general, because they can be a great evolution in *Science* and *Engineering*, when applied to some of fields in daily lives of the people.
- But, it's debatable if, per example, to train some *Quantum Hackers* will be good for the global society:
 - The act utilitarianism supports the idea of training these *Hackers*, because it could help the developers to build more secure *cryptosystems* for the final users and clients, in a long-term.
 - However, the rule utilitarianism is opposed to it, because a *Hacker* that uses a *Quantum Computer* can hack and break some of the current most secure and almost unbreakable *cryptosystems*, causing harm to some people, in a short-term.
 - Additionally, hacking it's a violation of people's privacy rights, also, illegal and punishable by law.
 - Also, in the theoretical moral analysis of Kant, it's reasonable to say that a *Hacker* that possibly, has bad intentions and wants to cause harm to the people, shouldn't ever accept to be trained to test these kinds of *cryptosystems* and possibly, be a *Quantum Hacker*, in the future.



Social, Ethic and Moral Analysis of Quantum Cryptography [2]

- In analysis of the ethic code, generally used in computing professional area, it's possible to argue the following:
 - The society can benefit with these new kinds of *cryptosystems* because they promise to be much more secure than the current ones. But the global society and some enterprises using the current *cryptosystems*, aren't prepared yet, to handle a *Security* and *Cryptography* attack made by a powerful *Quantum Computer* and can be seriously harmed by that;
 - A *Quantum Hacker* currently being trained, shouldn't omit to his supervisor, his possible bad intentions to harm people and violate their privacy rights using *Quantum Computer*;
 - The clients that are seeking and demanding these cryptosystems should be always informed about its development, because it addresses the protection of the user's private data;



Social, Ethic and Moral Analysis of Quantum Cryptography [3]

- In analysis of the ethic code, generally used in computing professional area, it's possible to argue the following:
 - An enterprise or organization that is trying to implement these kinds of cryptosystems and develop them unsuccessful, causing harm to the society, at general, should be severely punished;
 - A colleague of a developer of a cryptosystem based on Quantum Computing should be alert to his possible vulnerabilities and risks, warn him and try to show him that aspects;
 - At the core of computing, at general, shouldn't be developed software that, possibly, can cause some harm to the global society and try to avoid some aspect that can denigrate the profession itself;

Thank you very much!!!

