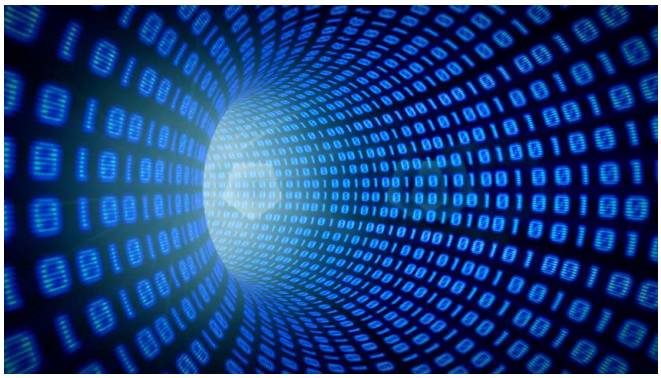
It's your time to imagine the futures

QC & Communication



Some definitions:

- ***Quantum cryptography:*** a branch of cryptography that uses quantum physics laws and properties for developing new cryptographic protocols for the exchange of information.
- ***Quantum internet:*** a kind of quantum network that allows communication between quantum computers on networks that are protected by quantum teleportation, which is the transmission of quantum information both through entanglement and classical channels.
- ***Quantum programming:*** a branch of computer science that develops algorithms for quantum computers in a programming language that is comprehensible to the user. While a classical computer works through classical logic gates (AND, OR, NOT), a quantum computer works through quantum logic gates (Hadamard, Pauli-X, Pauli-Y, Pauli-Z, Identity, Quantum-NOT, etc.).

Nowadays, communications via internet are essentially based on three elements: computers, networks between computers and cryptography. Classical cryptography is unbreakable by classical computer because it would take too much time for them to factorise huge numbers. The break of classical cryptography could be possible by the means of quantum algorithms and quantum computers, which are potentially enough powerful to do that. This would have an enormous impact on economic, political, military and social contexts, especially when it comes to privacy, surveillance and security of communications, and money and data transfer.
Game is on, not only in labs but also on a geopolitical level. It is not by chance that the US National Security Agency is one of the most involved institutions in this kind of research. Furthermore, the development of a secure quantum network would imply that whichever kind of cryptography would be "eavesdroppers-free": that would also lead to hiding illegal activities, maybe strengthening the so-called *deep* and *dark web*.

Some examples:

- **BB84**: it is a quantum cryptographic protocol developed by Charles H. Bennet and Gilles Brassard in 1984;
- **Quantum Internet Alliance:** it is an alliance between some European research groups with the aim of developing a quantum network for internet purposes.
- **IBM Q Experience:** within its research area on quantum technologies, IBM has developed a *software development kit* called "Qiskit" which contains tools for developing programmes with a real QC, localised in the IBM laboratories. The user programmes the quantum logic gates with packages for some classical programming languages (Python, Swift o Java), launches them on a designated provider and the latter translates classical instructions in quantum instructions for the QC, giving back the results.

Links	Descriptions
https://www.youtube.com/watch?v=UiJiXNEm-Go	Educational video by the YT channel "Physics Girl" on the differences between classical and quantum cryptography.
https://www.wired.it/scienza/lab/2018/03/09/internet-quantistica-punto-siamo/	[ITA] *Wired Italia* article on quantum internet
http://quantum-internet.team/	Quantum Internet Alliance website
https://www.scientificamerican.com/article/china-shatters-ldquo-spooky-action-at-a-distance-rdquo-record-preps-for-quantum-internet/	*Scientific American* article on the current record for quantum teleportation, made by China
https://www.accenture.com/us-en/insights/technology/quantum-cryptography	Report made by Accenture on how cryptography will change with the arrival of. Accenture is a multinational company of strategic consultancy.
https://quantumexperience.ng.bluemix.net/qx/experience	IBM Q Experience platform. It allows to create circuits made of quantum gates and to send them to a QC for analising.
https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf	Quantum Manifesto