notiziario tecnico

Speciale: Quantum Technologies

2/2020

TIM

Il Notiziario Tecnico è un social webzine, in cui è possibile discutere in realtime con gli autori i vari temi trattati negli articoli, restando in contatto su:
www.telecomitalia.com/notiziariotecnico

Proprietario ed editore
Gruppo Telecom Italia

Direttore responsabile
Michela Billotti

Comitato di direzione
Daniele Franceschini
Gabriele Elia
Elisabetta Romano
Paolo Snidero

Art Director
Enrico Gallo

Photo
123RF Archivio Fotografico
Archivio Fotografico TIM

Segreteria di redazione
Roberta Bonavita

Contatti
Via Reiss Romoli, 274
10148 Torino
Tel. 011 2285549
Fax 011 2285685
notiziariotecnico.redazione@telecomitalia.it

Editoriale

Le tecnologie quantistiche sono una delle cosiddette “hyper-next technologies” che TIM considera potenzialmente impattanti e disruptive nell’orizzonte dei prossimi 5- 10 anni, insieme p.es. a quelle di nuovi metamateriali per telecomunicazioni o alle future tecnologie di optical wireless integration.

Le tecnologie quantistiche, come descritto in questo numero del Notiziario Tecnico Telecom Italia, hanno campi di applicazione differenti: da quelli computazionali, per risolvere problemi matematici in tempi molto minori di quelli dei computer tradizionali, a sistemi di crittografia e sicurezza, dalle simulazioni quantistiche a nuovi tipi di sensori fino all’ipotizzare una vera e proprio “quantum Internet” o quantum network che si propone, nel lungo termine, di integrare il “teletrasporto” dell’informazione nelle tradizionali reti ottiche e radio.

Per conoscere e prepararsi all’impatto che sarà quindi visibile soprattutto dal medio termine, TIM sta agendo su vari filoni di attività innovativi; p.es. a inizio anno abbiamo usato per primi un annelear quantistico commerciale in cloud per confrontare alcune attività di pianificare della rete mobile rispetto a soluzioni classiche, con risultati molto promettenti ; abbiamo inoltre iniziato attività di divulgazione per studenti e professional nell’ambito dell’IEEE Industrial Distinguished Lecturer Program. Per le attività di standardizzazione sulle tecnologie quantistiche, che saranno come sempre indispensabili per il decollo dei servizi di telecomunicazione del futuro, siamo attivi come TIM nei principali enti come ITU, ETSI, IRTF, CEI e CEN-CENELEC e nei gruppi di studio del GSMA.

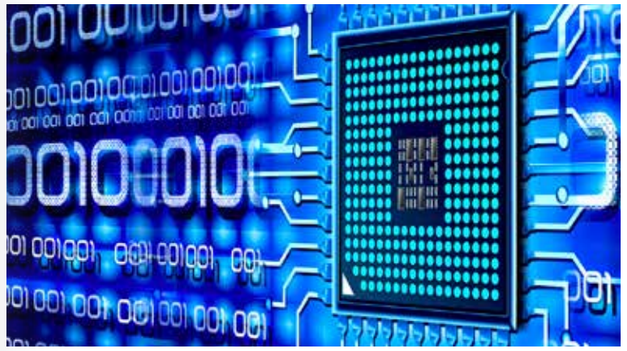
Infine, in ambito nazionale siamo in contatto con i principali centro di ricerca e università che si occupano di Quantum Computing e Communication, dai vari dipartimenti del CNR alle Università di Padova, Napoli, Parma, Firenze, il Politecnico di Torino e altre si aggiungeranno presto.

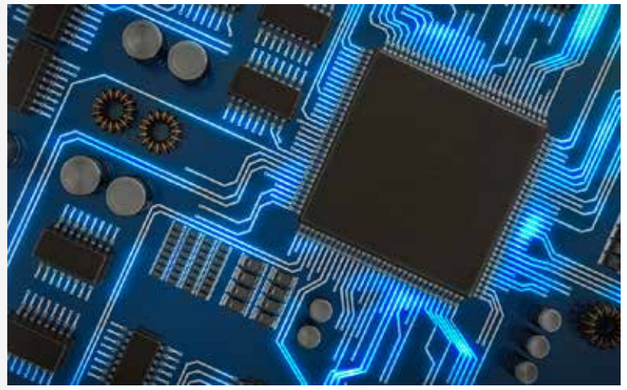
Non rimane che augurarvi buona lettura di un numero che affronta argomenti forse un po’ sofisticati matematicamente ma che abbiamo cercato di rendere accessibili e che sono indubbiamente molto affascinanti! ■

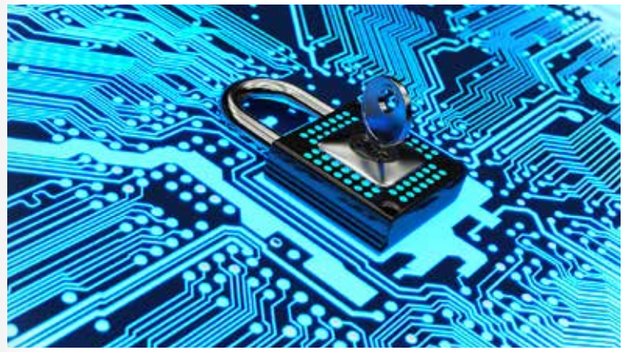
Buona lettura

Gabriele Elia

Indice







Davide Calonico

Tecnologie Quantistiche: Quantum Metrology & Sensing all'INRiM

L'INRiM dedica rilevanti attività all'uso di tecnologie quantistiche per migliorare le capacità di misura a livello nazionale e internazionale. Il paradigma metrologico con cui si declinano le tecnologie quantistiche è duplice: da un lato effetti quantistici consolidati e altri innovativi concorrono a migliorare le nostre capacità di misura; dall'altro il rigore della metrologia vuole garantire alle tecnologie livelli quantitativi propri di una proposta standardizzata alla società, che rispetti la qualità scientifica e le realtà del mercato.

Angela Sara Cacciapuoti, Marcello Caleffi

The Quantum Internet: the next ict revolution

Internet has dramatically progressed in a way that was unimaginable when it was conceived, by deeply changing our everyday lives. But the advent of the engineering phase of quantum technologies is imposing a new breakthrough within the ICT history: the design and the deployment of the QUANTUM INTERNET – a communication network enabling quantum communications among remote quantum nodes. In fact, the Quantum Internet will support functionalities with no direct counterpart in the classical Internet, likely in ways we cannot imagine yet.

Michele Amoretti

Quantum Software

Current progress in the field of quantum computer hardware makes it credible that, in just a few years, quantum computers will outperform classical ones. Many research groups and companies are working on the hardware, but the key questions of what a realistically-sized quantum computer can achieve, how to do this, and how to verify the results refer to quantum software. In this article, we stress the importance of quantum software and illustrate a few meaningful examples.

Daniele Ottaviani

Quantum Computing e HPC in Europa

Da qualche anno, la comunità HPC è chiamata a risolvere una sfida molto difficile. Se da una parte la crescente domanda di risorse computazionali di alto livello da parte di un mondo sempre più digitalizzato è ben compensata dalle altrettanto avanzate competenze di coloro che si occupano di High Performance Computing, dall'altra c'è l'annoso problema dell'evoluzione dei supercalcolatori.

THE SECOND QUANTUM REVOLUTION IS UNDERWAY

Antonio Manzalini

The transformative role of Telecommunications and Information Communication Technologies (ICT) has long been witnessed as a precursor of the scientific progress and economic growth in the modern world. Today, like never before, we are witnessing a pervasive diffusion of ultra-broadband fixed-mobile connectivity, the deployment of Cloud-native 5G network and service platforms and a wide adoption of Artificial Intelligence.

This is the so-called Digital Transformation, surely bringing far reaching techno-economic impacts on our Society. Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the ways of doing computation and communications have been already started. Will quantum technologies be the next breakthrough?

As a matter of fact, a first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. Now, a second revolution is underway.

This article, which has been presented by the Author as IEEE Distinguished Industrial Speaker, will provide an overview of the state of the art, challenges and opportunities posed by a coming second wave of quantum technologies and services.

Quantum technologies are already here

Today, Software Defined Network (SDN) and Network Function Virtualization (NFV) are offering the opportunity of designing and operating 5G infrastructures with unprecedent flexibility. In fact, an orchestrated use of Cloud, Edge-Fog computing and network virtual resources can deliver a continuum of capabilities, functions and micro-services through the so-called 5G Cloud-native infrastructures.

Sustainability of future network scenarios will have to face several techno-economic challenges, such as: the transmission and processing of enormous, and increasing, quantity of data with ultra-low latencies, automation of management and control processes, the fulfilment of the strict requirements of resilience, security and privacy, optimization of energy consumption, and so on.

Indeed today we are living a Digital Transformation, bringing far reaching techno-economic impacts on our Society. Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the ways of doing computation and communications have been already started. Will quantum technologies be the next breakthrough?

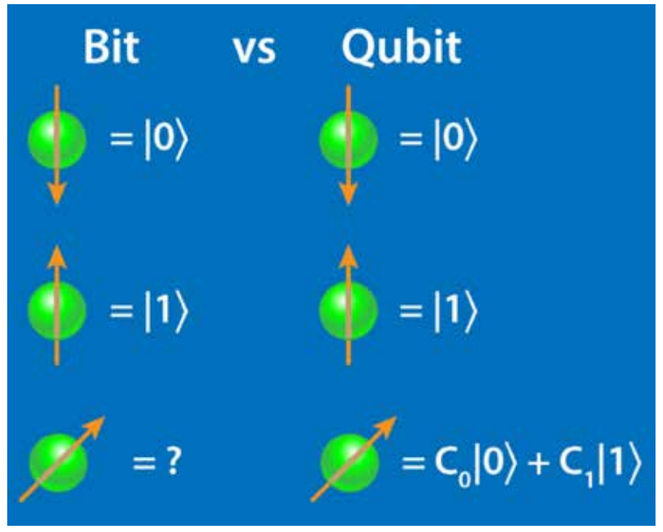
As a matter of fact, a first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.
Now a second revolution seems to be underway: in fact, there is a new impressive grow of interests for quantum, with several investments from public and private organizations worldwide (see Box 1) targeting new horizons of applications. In particular, there are three quantum phenomena, well known and well tested in Physics, which are not fully exploited yet by Industry.
These phenomena are: superposition, entanglement and measurement.

- Superposition concerns the property of quantum objects to stay in linear combination of multiple states until they are observed.
- Entanglement is defined as the possibility that two or more quantum objects to stay intrinsically linked, into an intertwined composite state, regardless of how far apart the objects are from one another. Recently hyper-entanglement has been discovered, defined as the entanglement in multiple degrees of freedom (DOFs) of a quantum system, such as polarization, spatial-mode, orbit-angular-momentum, time-bin and frequency DOFs of photons.
- Measurement regards the collapse and disruption of a quantum state from coherent probabilistic superposition state into a discrete one.

When quantum technologies will become mature enough to control and exploit these three phenomena, then there will be the impact of this second revolution over many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on. Significant work is still needed but, in light of the potential opportunities and threats of this second revolution, a lot of investments are being made worldwide.

Bits, Qubits and Quantum Gates

As a digital system manipulates Bits, a quantum system manipulates Qubits. A Qubit is the well-known basic unit of quantum information. A Qubit can be coded by a quantum system having two-states (or two-levels), for example: the spin of an electron (spin up and spin down).
Photons are special qubits in that they possess several independent properties such as polarization, spin angular momentum or orbital angular momentum. These degrees of freedom can all be employed to



1
Bits vs quantum bits (qubits)

encode quantum information. The number of accessible qubits can be increased beyond the number of particles by the simultaneous entanglement of multiple photons and multiple degrees of freedom (hyperentanglement). The three degrees of freedom of six photons, for example, can provide control over an 18-qubit ensemble.

A weird and remarkable property of quantum information is that a qubit can stay simultaneously with two values 0 and 1 (superposition of states), until it collapses, for example when a measurement is made.
In other words, while a Bit is either 0 or 1, a qubit can be seen as a linear combination of the two states (0, 1) with coefficients which are complex numbers. This allows representing the interactions between quantum states in terms of constructive and destructive interference of quantum information waves.

This means that two qubits can be in a superposition of four states, three qubits can be in a superposition of eight states... and so on. Therefore, generalizing while N bits can take one of 2N possible permutations, N qubits can stay in a superposition of all 2N possible permutations. This have remarkable consequences in computation.

A quantum register - associated to N qubits - may have a state which is the superposition of all 2N values simultaneously: therefore, by applying a quantum operation to the quantum register would result in altering all 2N values at the same time. This property allows quantum computers to elaborate qubits with "a sort of parallel computation" reducing the processing time (from exponential to polynomial time) for solving certain complex problems.
In general, there are two main classes of quantum computers: analog and gate-based.

Analog quantum computers include annealers, adiabatic computers, i.e., systems which solve problems by directly manipulating the interactions between qubits rather than breaking actions into more abstract gate operations.

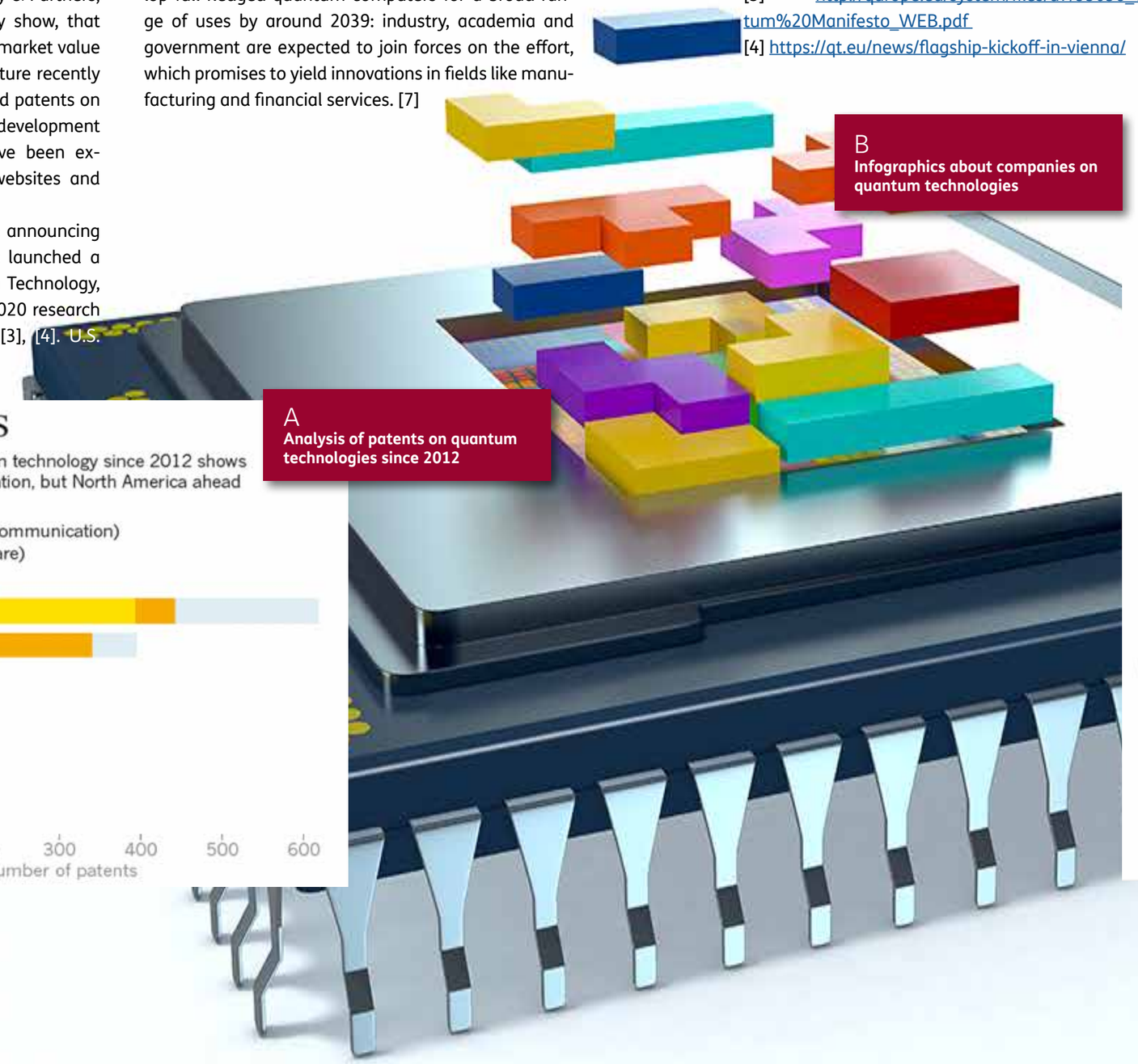
Gate-based quantum computers, sometimes referred to as universal quantum computers, use logical gate operations (AND, OR, etc.) on qubits. Quantum logic gates are the building blocks of quantum circuits:

A growing interest on Quantum

We are witnessing increasing efforts and investments on innovation activities about quantum technologies and services. Notable examples of industries include: Microsoft, IBM, HP, Toshiba, Google, Intel, Alibaba, Tencent, Baidu, but also several Network Operators.
According to a new report from McKinsey & Partners, in partnership with the Viva Technology show, that quantum technologies will have a global market value of $1 trillion by 2035 [1]. The Journal Nature recently published [2] an overview about published patents on quantum methods and systems and the development of start-ups. Data and information have been extracted from various market-research websites and consultancy reports.
Also, public and governative sectors are announcing investments. European Commission has launched a €1 billion Flagship Initiative in Quantum Technology, starting in 2018 within the European H2020 research and innovation framework programme [3], [4]. U.S. Government has enacted legislation to coordinate and accelerate U.S. quantum research and development [5]. China has announced plans to spend more than $10 billion to build a national laboratory for quantum science, to open in 2020 [6]. Japan will aim to develop full-fledged quantum computers for a broad range of uses by around 2039: industry, academia and government are expected to join forces on the effort, which promises to yield innovations in fields like manufacturing and financial services. [7]

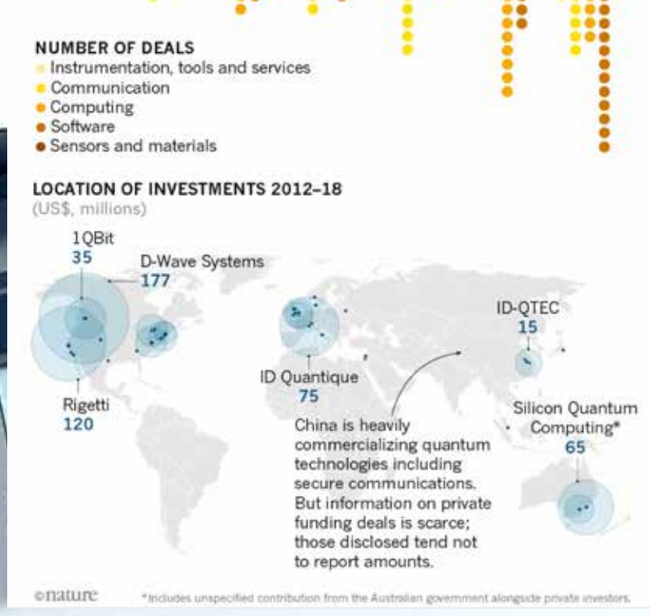
References

[1] https://www.consultancy.uk/news/24361/quantum-computing-market-to-reach-1-trillion-by-2035
[2] Quantum gold rush: the private funding pouring into quantum start-ups – Nature News Features 02nd October 2019 available at https://www.nature.com/articles/d41586-019-02935-4
[3] http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf
[4] https://qt.eu/news/flagship-kickoff-in-vienna/
[5] https://www.computer.org/csdl/magazine/co/2019/10/08848174/1dAq2PvlBkI
[6] https://www.economist.com/business/2018/08/18/the-race-is-on-to-dominate-quantum-computing?cid1=cust/ednew/n/bl/n/2018/08/16n/owned/n/n/nwl/n/n/EU/144433/n
[7] https://asia.nikkei.com/Business/Technology/Japan-plots-20-year-race-to-quantum-computers-chasing-US-and-China



A
Analysis of patents on quantum technologies since 2012

B
Infographics about companies on quantum technologies



Gate name	# Qubits	Circuit Symbol	Unitary Matrix	Description
Hadamard	1	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	Transforms a basis state into an even superposition of the two basis states.
T	1	T	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$	Adds a relative phase shift of π/4 between contributing basis states. Sometimes called a π/8 gate, because diagonal elements can be written as $e^{-i\pi/8}$ and $e^{i\pi/8}$.
CNOT	2		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$	Controlled-not; reversible analogue to classical XOR gate. The input connected to the solid dot is passed through to make the operation reversible.
Toffoli (CCNOT)	3		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$	Controlled-controlled-not; a three-qubit gate that switches the third bit for states where the first two bits are 1 (that is, switches |110⟩ to |111⟩ and vice versa).
Pauli-Z	1	Z	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$	Adds a relative phase shift of π between contributing basis states. Maps |0⟩ to itself and |1⟩ to −|1⟩. Sometimes called a "phase flip."
Z-Rotation	1	$R_z(\theta)$	$\begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$	Adds a relative phase shift of (or rotates state vector about z-axis by) θ.
NOT	1		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	Analogous to classical NOT gate; switches |0⟩ to |1⟩ and vice versa.

2
Quantum Logic Gates

for example, CNOTs and unitary single qubit operations form a universal set of quantum computing.

It should be mentioned that it is also possible to simulate quantum-gates computers by using classical computers. There exists a variety of software libraries that can be used, each with different purposes: a comprehensive list of tools is available on Quantiki [1].
Simulation can be made, for instance, using OpenCL (Open Computing Language) [2] which is a general-purpose framework for heterogeneous parallel computing on standard hardware, such as CPUs, GPUs, DSP (Digital Signal Processors) and FPGAs (Field-Programmable Gate Arrays).

There are multiple ways to build gate-based quantum computers manipulating qubits.

Table 1 provides an overview (not exhaustive): superconductors and trapped ions are presently the most advanced implementations [3].

Quantum Algorithms and Software

Most of the optimization problems in the fields of ICT and Telecommunications are currently solved with algorithms for finding suboptimal solutions, because of the excessive cost of finding an optimal solution.

Some of these problems includes: e.g., network planning, joint optimization of multiple functions, such as radio channel estimation, data detection and synchronization, Data Center resources and energy optimization.

Today, Quantum annealers (e.g., D-Wave) are already being used to solve some combinatorial and optimization problems. Nevertheless, quantum annealers are not properly quantum computers: they are specialized computing systems based on quantum heuristics.

In most cases, the problem to be solved is encoded into an Ising-type Hamiltonian, which is then embedded into a quantum hardware graph to be solved by a quantum annealer.

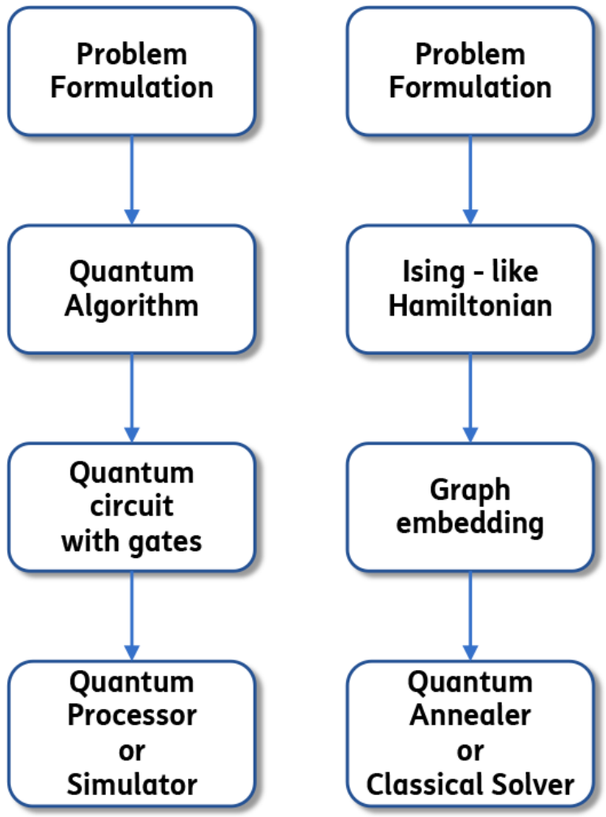
Gate-based quantum computers use another approach. For instance, figure 3 shows the comparison of the two approaches for the execution of quantum algorithms workflows. In the gate-based approach the problem is formulated in a way for selecting a proper quantum algorithm. Then the quantum algorithm is transformed in a quantum circuit (i.e., using quantum gates) which is either executed on a quantum processor or simulated.

In both cases, random fluctuations (e.g., heat or quantum-mechanical phenomena), could occasionally flip or randomize the state of qubits: this is introducing errors and potentially derailing the validity of the calculations. This is why many of these quantum systems require special vacuum environments, the adoption of cryogenic systems and error corrections methods. In particular, quantum error correction involves a substantial multiplication of resources: the number of physical qubits required may be orders of magnitude greater than the number of error-free logical qubits seen by the algorithm.

In general, we may say that there are two main classes of quantum algorithms, derived as generalization from the Shor's algorithm for factoring (capable of breaking a lot of public-key cryptography) and the Grover algorithm for searching. The website "Quantum Zoo" [4] has gathered a comprehensive list of said classes of algorithms, briefly describing their operation.

Table 1
Examples of gate-based approaches for developing quantum computers

Superconducting	Spin	Topological	Ion Trap	Neutral Atoms	Photonics
Superpositions of currents flowing in superconductors	Qubits encoded in spin of electrons confined in quantum dots	Topological quasi-particles (e.g., Majorana particles)	Ions trapped in electric fields (vacuum and lasers manipulate quantum states)	Atoms trapped in magnetic or optical fields (vacuum and lasers manipulate quantum states)	Qubits encoded in quantum states of photons
Players					
IBM Rigetti Google Alibaba	Intel	Microsoft	IonQ Honeywell AQT	CloudQuanta Atom Computing	Psi Quantum Xanadu ORCA



3
Quantum algorithms workflows: on a gate-model computer (left), on a quantum annealer (right)

It should be mentioned that for near term quantum applications, hybrid quantum/classical algorithms are also very promising.

A common characteristic of these approaches is that the quantum computer is rather simplified: it is only in charge of carrying out a subroutine, acting as a "coprocessor" while the larger scale algorithm is governed by a classical computer. In this case a higher error rate per operation is tolerable.

It may even be possible to implement such quantum algorithms without quantum error correction.
In summary, when comparing quantum algorithms with their classical counterparts, it appears that employing quantum systems specific performance targets may be reached at a lower computational complexity: on the other hand, an analytical demonstration of the levels of efficiency of quantum computers and algorithms in addressing computational complexity require further studies.

Concerning software languages and tools, the scenario is very active but still rather fragmented: the reference [5] provides an overview of

encourages the coalition of larger communities.

Sliq [6] is an example of recent progresses in the definition of a simple and powerful quantum language.

Sliq has been designed to address the challenge to enable Programmers to work at high level of abstraction. An intuitive semantics allows implicitly to drop temporary values, as in classical computation.
Soon we may even expect the emergence of quantum app stores. Not app stores like the one we access with our smartphone, but similar to code repositories, such as GitHub, types of library where quantum software developers make the code they have written available to anyone [7].

For more details see the article by M. Amoretti "Quantum Software", in this volume.
We conclude noting that the interest in quantum software is very high. The number and value of venture capital deals, particularly in quantum software and computing startups, is increasing, reaching a total of 32 deals in 2018 at a total value of US$173 million in 2018 [8].

Application areas for Quantum

International innovation activities and Standardization Bodies are pretty aligned in identifying four main applications areas of quantum technologies and services: commu-

Table 2
Examples of applications for quantum technologies (not exhaustive)

Domains	Quantum Communications	Quantum Computing	Quantum Simulation	Quantum Sensing & Metrology
Telecom and ICT	Quantum safe communication (e.g., QKD, QRNG)	Infrastructure optimization planning and operations; Artificial Intelligence (AI)	Infrastructure simulations: e.g., traffic,	Clocks synchronization; more accurate sensors
Medicine and Biology	Security and protection of patients' data	Improved diagnostics; drug design	Proteomics, Genomics, Drug simulations	Improved sensing for diagnostics imaging
Energy, Oil and Gas	Security for critical infrastructure	Optimizations; Logistics	Predictions and risks analysis	Through-ground imaging
Finance	Secure transactions	Portfolio management	Portfolio management and trading simulations	Clocks for trade synchronization
Smart Cities and Transport	Security and data protection	Traffic, resources optimization; complexity management	Predictions and risks analysis	Timing synchronization; more accurate sensors; quantum LiDAR

Entanglement-based QKD over 1,120 km

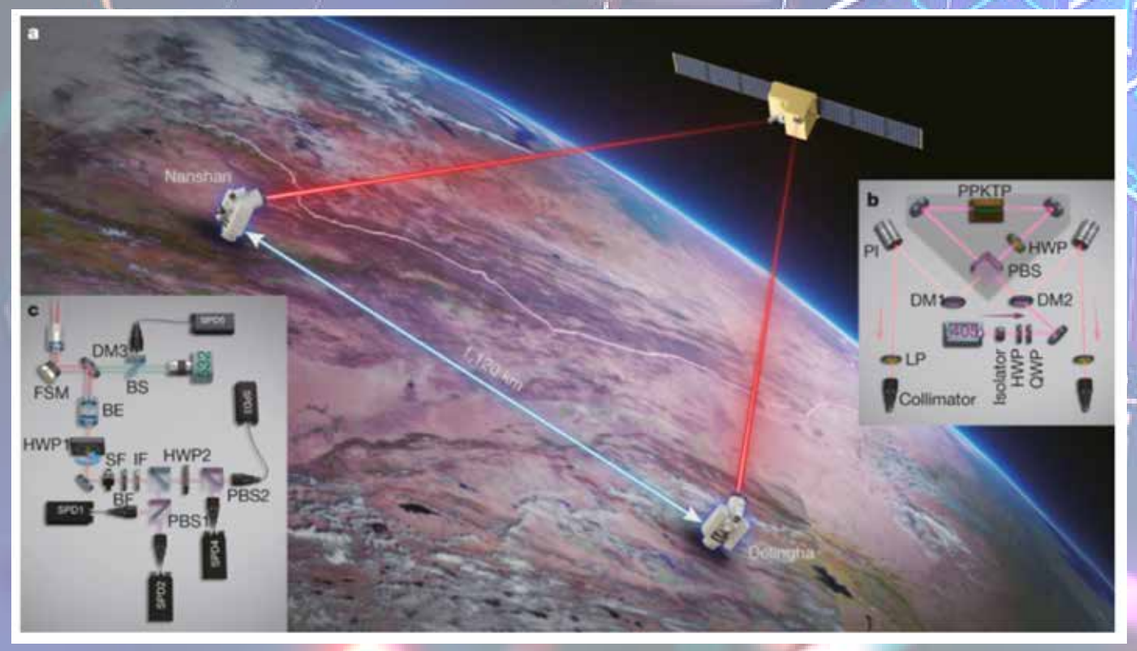
Quantum Key Distribution (QKD) is secure way of sharing cryptographic keys between remote users, leveraging on the quantum principles. The potential applications of QKD include not only securing communications networks but also critical infrastructures (for instance, the Smart Grid), transactions of financial institutions and national defense.

QKD has a TRL 7-9: there are some pieces of equipment already commercially available even if as today the distances covered over optical fibres are still relatively limited (about 50 to 80 km) owing to the channel loss that occurs when using optical fibres (or terrestrial free space) that exponentially reduces the photon transmission rate.

Long-distance entanglement distribution can be realized using quantum repeaters: on the other hand, the technology is still immature for practical implementations but there are intensive innovation activities. For example, innovation activities demonstrated the feasibility of QKD over a coiled optical fibre of about 500 km.

In satellite communications, longer distances have been achieved, owing to the negligible photon loss and decoherence experienced in empty space. Therefore, tj satellite-based QKD has the potential to help to establish a global-scale quantum network: for example, a 1,200 km point-to-point QKD has been already demonstrated from a satellite to a ground station, even if with limited efficiency.

Recently [1] entanglement-based QKD has been demonstrated between two ground stations over 1,120 km at a finite secret-key rate of 0.12 bits per second, without the need for trusted relays. In particular, entangled photon pairs were distributed via two bidirectional downlinks from the Micius satellite to two ground observatories in Delingha and Nanshan in China.



Reference

[1] Yin, J., Li, Y., Liao, S. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature (2020). https://doi.org/10.1038/s41586-020-2401-y

nications, computing, simulations, sensing and metrology.

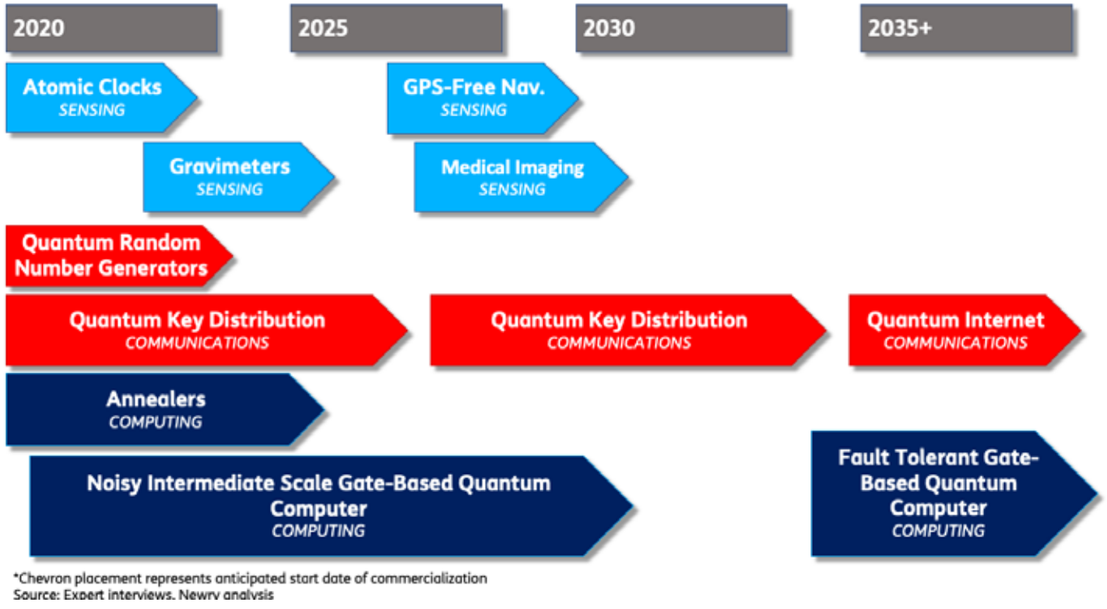
The area of Quantum Communications includes two main sub-domains: the so-called quantum-safe communications and the "teleporting" of qubits (e.g. Quantum Internet, whose TRL is 1-2). Quantum-safe communications leverage on systems such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG) which have a TRL 7-9. Regarding the status of the developments of the Quantum Internet see the article by S. Cacciapuoti and M. Caleffi "The Quantum Internet: the next ICT revolution", in this volume.

Quantum Computing has been already touched in the previous section. The area concerns the exploitation of the three principles of superposition, (hyper)entanglement and measurements, to speed up over classical computers in solving complex optimization and combinatorial problems.

Quantum simulations concerns all those applications where well-controlled quantum systems are used to simulate the behavior of other systems, which are less accessible and more complex for a direct simulation (TRL 6-9). Table 2 provides some examples of applications.
Quantum sensing and metrology includes those applications where high sensitivity of quantum systems to environmental influences can be exploited to measure physical properties and timing with more precision (e.g. magnetic and heat sensors, gravimeters, GPS-free navigators, clocks; TRL is 4-9).

Overall, while some quantum applications are already commercially available today (e.g., QKD and QRNG, quantum annealers, quantum simulations, atomic clocks and some quantum sensors) the current use of the second wave of quantum technologies is still relatively limited. This is due to both technical limitations and tradeoffs between technical performance and costs. Further progresses are needed. On the other hand, international community is recognizing the disruptive potentialities of these technologies in several markets when a breakthrough will be reached.

4
Tentative roadmap for quantum technologies and services [3]



*Chevron placement represents anticipated start date of commercialization
Source: Expert interviews, Newry analysis

Conclusions

A first quantum revolution has already brought quantum technologies in our everyday life, since decades. Chips for computers and smartphone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.

Now a second revolution seems to be underway, leveraging on the three quantum principles of superposition, (hyper-)entanglement and measurement. It is safe to predict that a second wave of quantum technologies could potentially have a major impact in many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on. Significant work is still needed to develop enabling components and systems but in light of the potential opportunities and threats, quite a lot of investments are being made worldwide across the public and private organizations.

In quantum communications, a technological breakthrough is need for developing quantum repeaters: this would be a key step for both long-distance QKD and distributed quantum computing. Concerning quantum computing, a roadblock is mitigating the random fluctuations that could occasionally flip or randomize the state of qubits during processing. Innovative qubits coding (e.g., in topological computing) and availability of efficient methods of quantum error correction are two to the main expected key milestones. Quantum software scenario is very active but rather fragmented: major efforts are directed to define languages to enable Programmers to work at high level of abstraction.

Standardization efforts are also set to help coordinating and accelerating progresses of quantum technologies. Multiple groups such as ANSI, ITU, IETF, ETSI, GSMA and IEEE are producing significant efforts. One key aspect concerns the integration of future quantum nodes and equipment (today for example QDK systems) in classic infrastructure (e.g., 5G): this requires the definition of interfaces and abstraction for management and control. The topics is also under study and experimentation in the Quantum Flagship projects of H2020 (e.g., QIA, CIVIQ and UNIQORN).

In conclusion, the following figure 4 provides a tentative roadmap for quantum technologies and services [3] ■

References

1. Quantum Information Portal and Wiki, available at https://quantiki.org/wiki/list-qc-simulators
2. Kelly, A. Simulating quantum computers using OpenCL. arXiv preprint arXiv:1805.00988 (2018).
3. OIDA QUANTUM PHOTONICS ROADMAP, Every Photon Counts - March 2020
4. Quantum Algorithms Zoo, available at http://quantumalgorithmzoo.org/#acknowledgments
5. Fingerhuth, M.; Babej, T.; Wittek, P. Open source software in quantum computing. PLoS ONE 2018, 13, e0208561.
6. https://ethz.ch/en/news-and-events/eth-news/news/2020/06/the-first-intuitive-programming-language-for-quantum-computers.html
7. The Quantum App Store Is Coming, Scientific American 9th June 2020, available at https://www.scientificamerican.com/article/the-quantum-app-store-is-coming/
8. Quantum gold rush: the private funding pouring into quantum start-ups, Nature News Features 02nd October 2019, available at https://www.nature.com/articles/d41586-019-02935-4

Antonio Manzalini *antonio.manzalini@telecomitalia.it*

Ingegnere elettronico, Ph.D è entrato in Telecom Italia nel 1990. Ha partecipato a diversi progetti di ricerca internazionali riguardanti reti di trasporto SDH ed ottico (WDM), occupando varie posizioni di responsabilità. Ha inoltre contribuito a molte attività di standardizzazione, guidando alcuni gruppi di lavoro in ITU-T, IEEE e GSMA. Attualmente si occupa di tecnologie ed architetture di reti 5G, basate sull'integrazione di SDN, NFV con Cloud-Edge Computing e sistemi di Intelligenza Artificiale. Nel 2019, IEEE gli ha assegnato il premio Industrial Distinguished Lecturer Award. È autore di oltre un centinaio di pubblicazioni internazionali e di sette brevetti ■

GOOGLE – BUILDING QUANTUM COMPUTERS

a cura della Redazione del Notiziario Tecnico TIM

Quantum Computing merges two great scientific revolutions of the 20th century: computer science and quantum physics. Quantum physics is the theoretical basis of the transistor, the laser, and other technologies which enabled the computing revolution. But on the algorithmic level, today's computing machinery still operates on "classical" Boolean logic. Quantum Computing is the design of hardware and software that replaces Boolean logic by quantum law at the algorithmic level. For certain computations such as optimization, sampling, search or quantum simulation this promises dramatic speedups. We are particularly interested in applying quantum computing to artificial intelligence and machine learning. This is because many tasks in these areas rely on solving hard optimization problems or performing efficient sampling scenarios where optical-radio networks requires automatic real-time joint optimization of heterogeneous computation, communication, and memory/cache resources and high dimensional fast configurations (e.g., selecting and combining optimum network functions and inference techniques). Moreover, the nexus of EI with distributed ledger technologies will enable new collaborative ecosystems which can include, but are not limited to: network operators, platform providers, AI technology/software providers and Users.

What the quantum computing milestones means

On 23 October 2019, Nature [1] published the news that Google's team of researchers have achieved a big breakthrough in quantum computing known as quantum supremacy.

"It's a term of art that means we've used a quantum computer to solve a problem that would take a classical computer an impractically long amount of time.

This moment represents a distinct milestone in our effort to harness the principles of quantum mechanics to solve computational problems", said Sundar Pichai, Google CEO, in his note What our quantum computing milestone means. [2]

"While we're excited for what's ahead, we are also very humbled by the journey it took to get here.

And we're mindful of the wisdom left to us by the great Nobel Laureate Richard Feynman: "If you think you understand quantum mechanics, you don't understand quantum mechanics." [2]

In many ways, the exercise of building a quantum computer is one long lesson in everything we don't yet understand about the world around us.

While the universe operates fundamentally at a quantum level, human beings don't experience it that way. In fact, many principles of quantum mechanics directly contradict our surface level observations about nature.

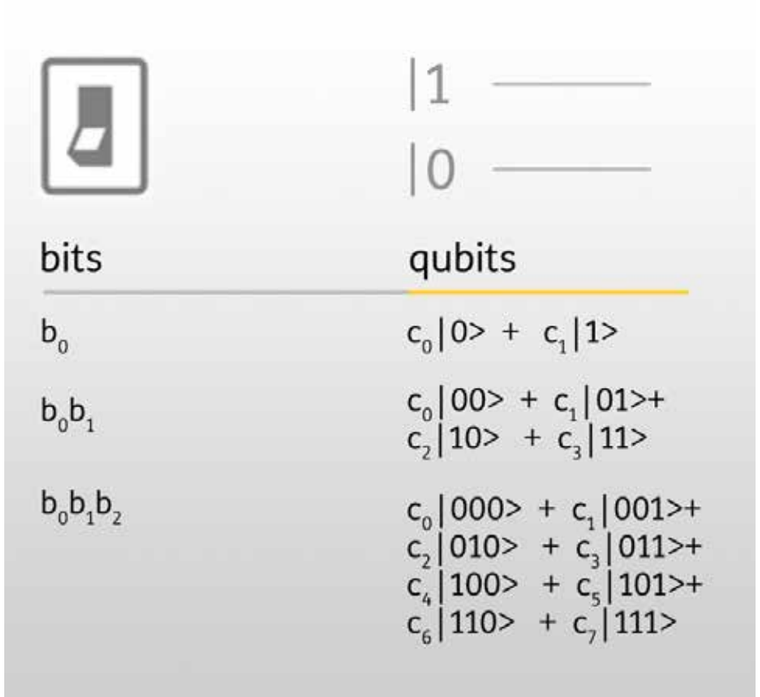
Yet the properties of quantum mechanics hold enormous potential for computing." [2]

What is a quantum computer?

The word quantum computer is a little bit misleading because it sounds like a computer, and when people think of computer, they think of a phone or a laptop.

The truth is the phone and the laptop and even a very powerful supercomputer all operate according to the same fundamental rules, and a quantum computer is fundamentally different [M1],[3].

Quantum hardware can be used as a tool for approaching certain kinds



of computational problems. "Our ongoing efforts are both to develop the hardware and to develop algorithms that leverage this hardware", said Marissa Giustina, Research Scientist and Quantum Electronics Engineer at Google. [M1]

To better understand a Quantum Computer, we'll have to introduce for a moment the Quantum Mechanics.

"The most fundamental model of nature we know was developed in the early 20th century and is known as quantum mechanics. The word "mechanics" refers to the mechanisms by which things happen. The word "quantum" refers to discrete quantities of energy or some other physical quantity.

Within quantum mechanics, energy comes in packets, sometimes called photons. And you cannot have fractional packets", Giustina continues.

"The word "quantum" doesn't dictate an object's size. A quantum object is one that relates in a well-defined way to a single quantum of energy. For instance, the photon mentioned before is a quantum object; similarly, atoms are quantum objects.

In a nutshell, a quantum object is one whose observable behavior reflects that nature only offers energy in discrete packets.

What differentiates quantum computing hardware from a regular computer? In essence, quantum hardware lives in a richer world than its conventional counterpart. Let's consider a simple, abstract, quan-

tum object, which is entirely described by the fact that it can be in one of two different energy levels. Let's call those levels 0 (|0>) and 1(|1>).

Because of the apparent similarity between our quantum object and that classical bit of information, we call this quantum analog a quantum bit, or qubit.

One peculiar feature about quantum mechanics is the existence of superpositions. A superposition is like a special mixture of the energy levels 0 and 1, where the weight of each energy level is given by complex constants C_0 and C_1 (C_0|0>) + C_1 (|1>).

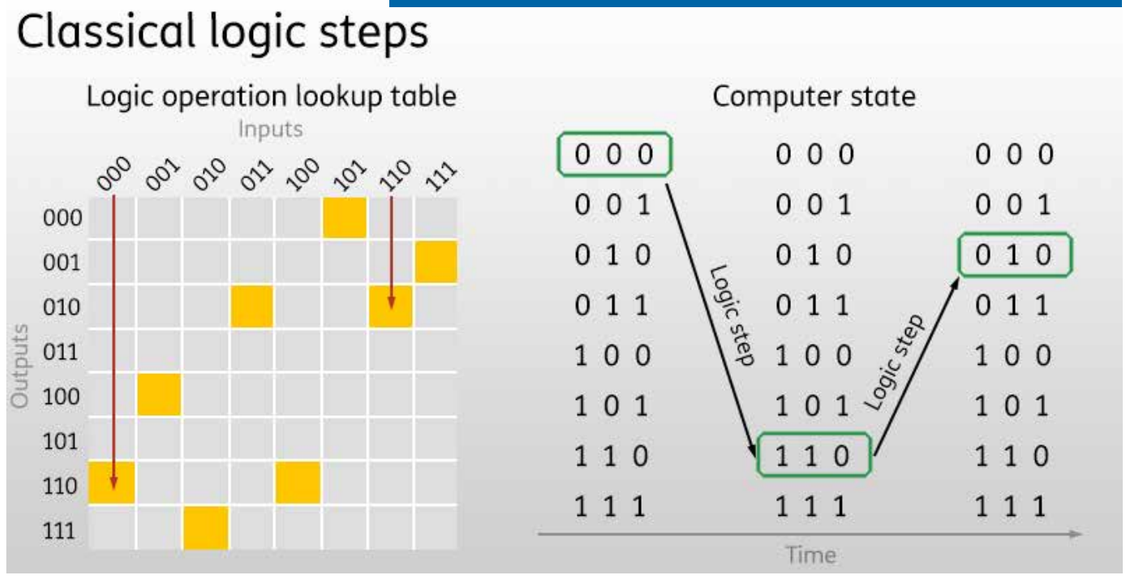
If we measure the energy of our qubit, we will sometimes observe 0, and sometimes 1, where the value of sometimes is given by the constants C. An individual measurement will yield an outcome of 0 or 1. There are no other options.

But before the measurement occurs, we know at most the chances of getting a 0 or a 1.

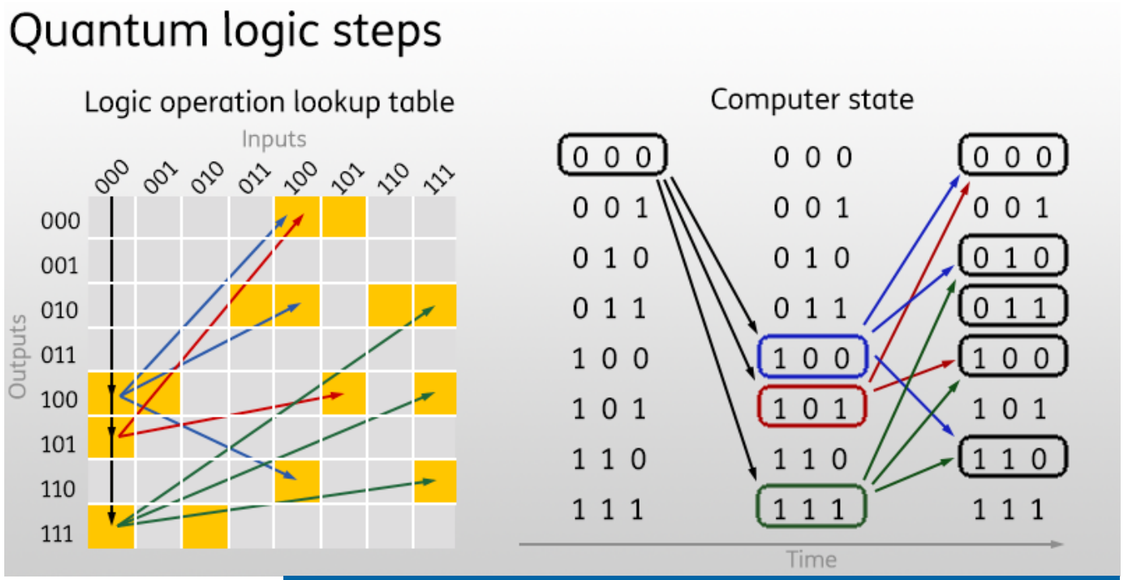
We can't know the actual outcome for sure until we measure it. Therefore, when we want to talk about the energy state of the qubit before we've made the measurement, we use this superposition to represent that the qubit hasn't decided yet which outcome to display, even though the chances of getting each outcome are fixed.

Suppose we add a second qubit. If these were conventional switches, we could think about each switch independently. But qubits are different. Just as one qubit can be in a superposition state, two qubits can share a superposition state, where, for instance, the measurement outcome is unknown but will certainly be the same for both objects or opposite for both objects.

This means that in order to fully describe two qubits, we need to consider C's for all possible measurement outcomes we could see. To describe three qubits, we need



The logic operation shown in the picture takes the state 0-0-0 to 1-1-0. If we were to apply the same operation again, we'd go from 1-1-0 to 0-1-0.



For example, starting in 0-0-0, we go to a superposition of 1-0-0, 1-0-1, and 1-1-1.Then each of those three parts of the super post state branches out to even more states.

eight C's. Describing four qubits takes 16 C's, and so on. Each time we add another qubit, it takes twice as much information to describe the whole pile of them." [M1]

That is the crux of what differentiates quantum hardware. The quantum system lives in a richer space, so that representing n qubits with a classical computer requires 2n bits

A classical computer's state is the value of its memory bits and computer programs determine how the computer goes from one state to the next. But because we're based in classical physics, the state of the computer is just one of these states at each point in time. On each step of a classical algorithm, we go from one state to the next. [M2]

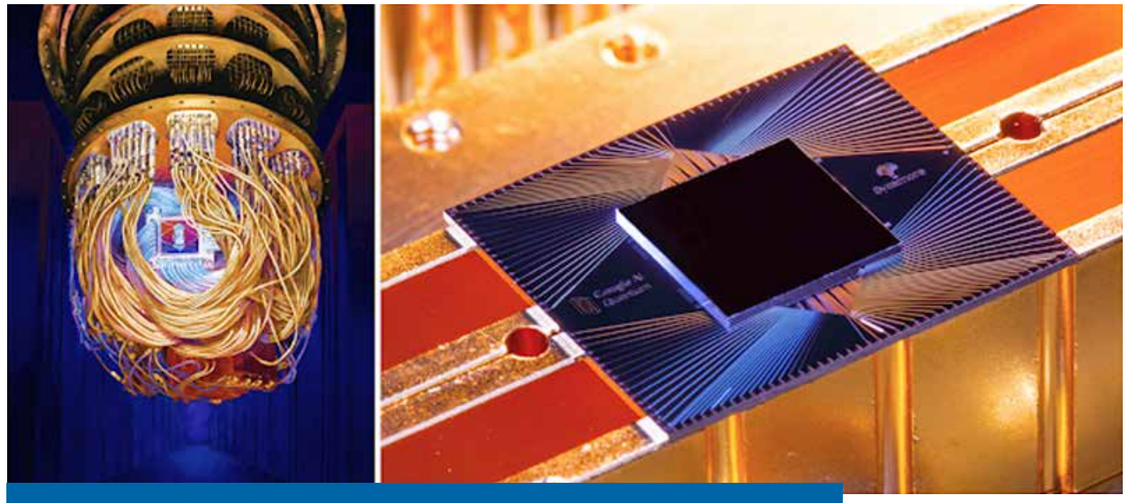
"Compared to classical states, quantum states are more rich. They can have weight in all possible classical states, a situation physicists call superposition.

Each step of a quantum algorithm mixes the states into complex superpositions", explains Daniel Sank, Quantum Electronics Engineer at Google. [M2] The extra complexity of quantum computers allows them to solve some problems faster than a classical computer ever could.

But does this mean that a quantum memory with 100 qubits corresponds to a conventional memory with 2100 bits? Not so fast...

Quantum hardware is very effective at encoding and processing certain kinds of information. But it cannot efficiently mimic many useful aspects of its classical counterpart. [M1]
The exponentially growing complexity of quantum systems also gives a clue about where quantum hardware could be useful.

In the fields of chemistry and materials development, simulation of molecules could be a powerful technique to learn about the properties of a new molecule before fully synthesizing it in the lab.



Left: Artist's rendition of the Sycamore processor mounted in the cryostat. (Forest Stearns, Google AI Quantum Artist in Residence) Right: Photograph of the Sycamore processor. (Erik Lucero, Research Scientist and Lead Production Quantum Hardware)

However, our ability to simulate chemistry on computers is limited. At its heart, chemistry is an application of quantum mechanics. In fact, chemistry and materials simulations have appeared as an appealing near-term problem to approach using quantum hardware. [M1]

Demonstrating quantum supremacy

"Physicists have been talking about the power of quantum computing for over 30 years, but the questions have always been: will it ever do something useful and is it worth investing in?" said John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum.

"For such large-scale endeavours it is good engineering practice to formulate decisive short-term goals that demonstrate whether the designs are going in the right direction.

So, we devised an experiment as an important milestone to help answer these questions.

This experiment, referred to as a quantum supremacy experiment [4], provided direction for our team to overcome the many technical challenges inherent in quantum systems engineering to make a computer that is both programmable and powerful.
To test the total system performance we selected a sensitive computational benchmark that fails if just a single component of the computer is not good enough.
We developed a new 54-qubit processor, named "Sycamore", that is comprised of fast, high-fidelity quantum logic gates, in order to perform the benchmark testing.

Our machine performed the target computation in 200 seconds, and from measurements in our experiment we determined that it would take the world's fastest supercomputer 10,000 years to produce a similar output." [4]

The Experiment

To actually demonstrate quantum supremacy, we have these three steps: first, pick a circuit, second, run it on the quantum computer, third, simulate what the quantum computer is doing on a classical computer and we gradually increase the complexity of that circuit.At some point, it becomes completely impossible for the classical computer to keep up.

Then we say we have achieved quantum supremacy. [M3]

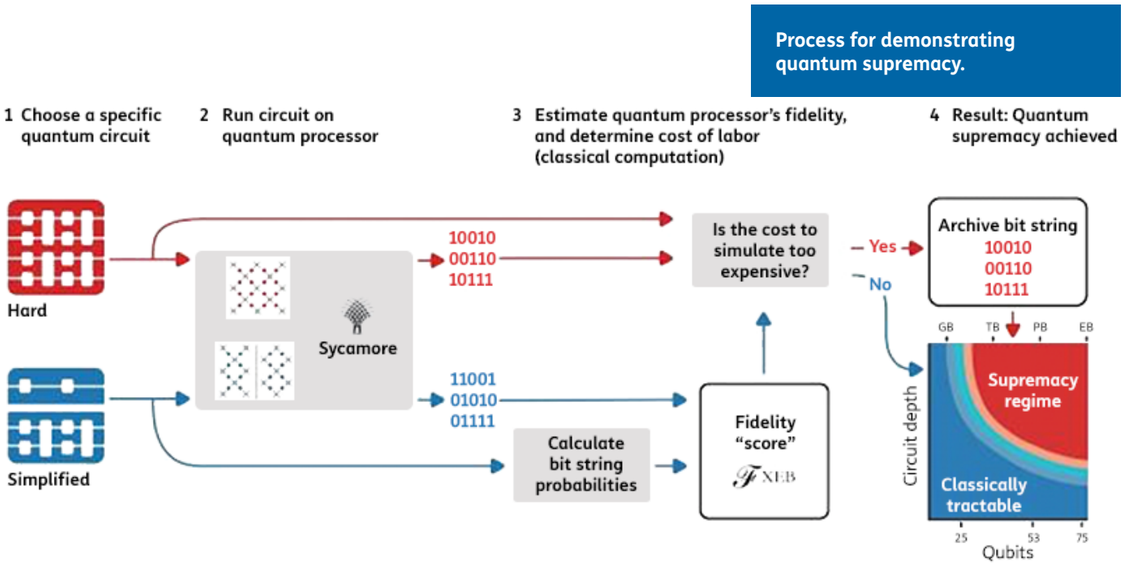
To get a sense of how this benchmark works, imagine enthusiastic quantum computing neophytes visiting our lab in order to run a quantum algorithm on our new processor.

They can compose algorithms from a small dictionary of elementary gate operations. Since each gate has a probability of error, our guests would want to limit themselves to a modest sequence with about a thousand total gates.

Assuming these programmers have no prior experience, they might create what essentially looks like a random sequence of gates, which one could think of as the "hello world" program for a quantum computer. Because there is no structure in random circuits that classical algorithms can exploit, emulating such quantum circuits typically takes an enormous amount of classical supercomputer effort. [4]

Each run of a random quantum circuit on a quantum computer produces a bitstring, for example 0000101.
Owing to quantum interference, some bitstrings are much more likely to occur than others when we repeat the experiment many times. However, finding the most likely bitstrings for a random quantum circuit on a classical computer becomes exponentially more difficult as the number of qubits (width) and number of gate cycles (depth) grow. [4]

Process for demonstrating quantum supremacy.



In the experiment, we first ran random simplified circuits from 12 up to 53 qubits, keeping the circuit depth constant.

We checked the performance of the quantum computer using classical simulations and compared with a theoretical model.

Once we verified that the system was working, we ran random hard circuits with 53 qubits and increasing depth, until reaching the point where classical simulation became infeasible. [4]

This result is the first experimental challenge against the extended Church-Turing thesis [6], which states that classical computers can efficiently implement any "reasonable" model of computation.
With the first quantum computation that cannot reasonably be emulated on a classical computer, we have opened up a new realm of computing to be explored. [4]

The sycamore processor

"The quantum supremacy experiment was run on a fully programmable 54-qubit processor named "Sycamore." It's comprised of a two-dimensional grid where each qubit is connected to four other qubits.

As a consequence, the chip has enough connectivity that the qubit states quickly interact throughout the entire processor, making the overall state impossible to emulate efficiently with a classical computer.

The success of the quantum supremacy experiment was due to our improved two-qubit gates with enhanced parallelism that reliably achieve record performance, even when operating many gates simultaneously.

We achieved this performance using a new type of control knob that is able to turn off interactions between neighboring qubits. This greatly reduces the errors in such a multi-connected qubit system.

We made further performance gains by optimizing the chip design to lower crosstalk, and by developing new control calibrations that avoid qubit defects.

We designed the circuit in a two-dimensional square grid, with each qubit connected to four other qubits. This architecture is also forward compatible for the implementation of quantum error-correction. We see our 54-qubit Sycamore processor as the first in a series of ever more powerful quantum processors."

"To ensure the future utility of quantum computers, we also needed to verify that there are no fundamental roadblocks coming from quantum mechanics." John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum continue.

"Physics has a long history of testing the limits of theory through experiments, since new phenomena often emerge when one starts to explore new regimes characterized by very different physical parameters. Prior experiments showed that quantum mechanics works as expected up to a state-space dimension of about 1000.

Here, we expanded this test to a size of 10 quadrillion and find that everything still works as expected. We also tested fundamental quantum theory by measuring the errors of two-qubit gates and finding that this accurately predicts the benchmarking results of the full quantum supremacy circuits. This shows that there is no unexpected physics that might degrade the performance of our quantum computer.

Our experiment therefore provides evidence that more complex quantum computers should work according to theory, and makes us feel confident in continuing our efforts to scale up." [4]

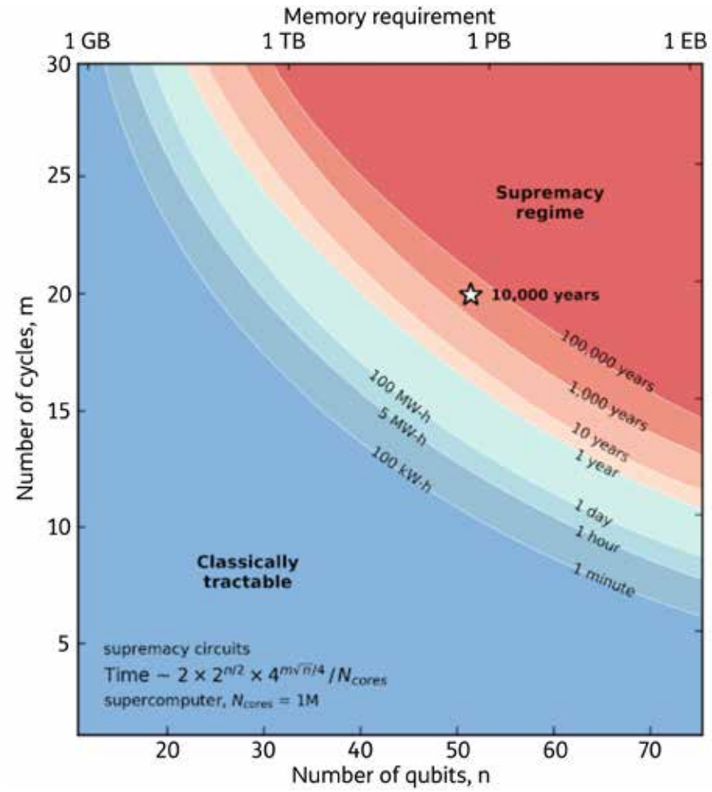
What's next?

"Our team has two main objectives going forward, both towards finding valuable applications in quantum computing", said John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum.
"First, in the future we will make our supremacy-class processors available to collaborators and academic researchers, as well as companies that are interested in developing algorithms and searching for applications for today's NISQ processors.

Creative researchers are the most important resource for innovation — now that we have a new computational resource, we hope more researchers will enter the field motivated by trying to invent something useful.

Second, we're investing in our team and technology to build a fault-tolerant quantum computer as quickly as possible. Such a device promises a number of valuable applications.

For example, we can envision quantum computing helping to design new materials — lightweight bat-



Schrödinger-Feynman algorithm

Estimate of the equivalent classical computation time assuming 1M CPU cores for quantum supremacy circuits as a function of the number of qubits and number of cycles for the Schrödinger-Feynman algorithm. The star shows the estimated computation time for the largest experimental circuits.

teries for cars and airplanes, new catalysts that can produce fertilizer more efficiently (a process that today produces over 2% of the world's carbon emissions), and more effective medicines. Achieving the necessary computational capabilities will still require years of hard engineering and scientific work. But we see a path clearly now, and we're eager to move ahead." [4] ■

Reference

1. Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5
2. Sundar Pichai, "What our quantum computing milestone means", https://www.blog.google/perspectives/sundar-pichai/what-our-quantum-computing-milestone-means/
3. Hartmut Neven, "Computing takes a quantum leap forward", https://www.blog.google/technology/ai/computing-takes-quantum-leap-forward/
4. John Martinis, Sergio Boixo, Quantum Supremacy Using a Programmable Superconducting Processor
5. https://research.google/teams/applied-science/quantum/
6. https://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis#Variations

Media

1. [M3] Demonstrating Quantum Supremacy https://www.youtube.com/watch?v=-ZNEzzDcllU
2. [M2] Building a quantum computer with superconducting qubits https://www.youtube.com/watch?v=uPw9nkJAwDY
3. [M1] What is a quantum computer? https://www.youtube.com/watch?v=k-21vRCC0RM
4. [M4] Quantum supremacy explained https://www.youtube.com/watch?v=gylmjTOUfCQ
5. [M5] Programming a quantum computer with Cirq https://www.youtube.com/watch?v=16ZfkPRVf2w

QUANTUM COMPUTING TUTORIAL

Giovanni Amedeo Cirillo, Filippo Gandino,
Edoardo Giusto, Giovanni Mondo

Il Quantum Computing (QC) è rimasto a lungo un'idea nell'immaginario della comunità scientifica, ma grazie agli enormi progressi degli ultimi decenni sta acquistando una credibilità crescente al punto da ritenere realistica la sua applicazione su larga scala su un orizzonte temporale relativamente vicino.

I computer quantistici implementano una nuova modalità di processare le informazioni e, se la tecnologia riuscirà a rendere disponibile la capacità di calcolo che promette, potranno essere utilizzati per analizzare problemi non trattabili dai computer classici, aprendo nuove opportunità in termini di scoperte, innovazione e applicazione con impatti che potrebbero essere rivoluzionari in tutti i settori.

Anche se la tecnologia non ha raggiunto ancora la piena maturità, è già conveniente utilizzare il QC eventualmente con opportuni adattamenti, capendo le modalità e le logiche della programmazione quantistica, beneficiando dei vantaggi e delle opportunità di sviluppo di nuovi use cases e di apertura di nuovi scenari.

L'articolo si propone di fornire una panoramica sulle applicazioni, le tipologie di quantum computer, gli ambienti di sviluppo e la modellizzazione algoritmica per mostrare come il QC possa a tutti gli effetti essere preso in considerazione per sviluppare use case reali.

In fondo il quantum non è poi così "spooky" come potrebbe sembrare...

Applicazioni del Quantum Computing

Il QC è considerato la prossima futura grande rivoluzione dell'Information Technology e promette di avere grossi impatti in tutti i settori grazie alle enormi potenzialità di calcolo che renderà disponibili. I quantum computer si distinguono dai computer classici perché implementano una diversa modalità di elaborazione dei dati e sono pertanto adatti per processare classi di problemi differenti non risolvibili in tempi ragionevoli dai computer tradizionali.

La motivazione iniziale alla base dello sviluppo dei computer quantistici nasce dall'idea di superare i limiti mostrati dai computer classici, quando la ricerca avanzata nel campo della fisica e della chimica si è spinta a livello di particelle subatomiche. Su queste dimensioni intervengono i principi della meccanica quantistica e quindi, per progredire ulteriormente, si è pensato che fosse necessario disporre di nuovi computer che, funzionando secondo le stesse leggi, fossero in grado di modellare e simulare questi fenomeni in maniera più accurata.

Successivamente ci si è resi conto che un computer quantistico potesse essere utilizzato non solamente come simulatore, ma per trattare in maniera efficiente una più ampia gamma di problemi complessi, grazie alla sua modalità di elaborazione probabilistica intrinseca nei principi della meccanica quantistica [1],[2].
Essendo una tecnologia in gran parte ancora in uno stadio di ricerca, l'utilizzo del QC si diffonderà nel tempo, coerentemente con la crescita della sua capacità computazionale che, come verrà descritto nella sezione sulle Tipologie di Quantum Computer, si misura in qubit.
Il progressivo aumento della capacità di calcolo ne abiliterà, corrispondentemente, l'applicazione a casi d'uso di complessità crescente.

Partendo dall'idea originaria, l'impiego del QC ai settori della chimica e alla scienza dei materiali richiede una potenza di calcolo di almeno un centinaio di qubit. Considerando che nel 2017 il quantum computer di IBM gestiva 16 qubit e oggi 50, si può pensare che un centinaio di qubit non saranno disponibili prima del 2025.

L'applicazione del quantum a questi settori potrebbe avere conseguenze importanti come lo sviluppo di batterie per le automobili elettriche con maggior autonomia, nuovi processi industriali (il processo Haber - Bosch, per la sintesi industriale dell'ammoniaca, responsabile del consumo dell'1-2% dell'energia a livello globale e del 2-3% della produzione di CO_2, è impiegato da oltre un secolo per la produzione di fertilizzanti e prodotti per la pulizia perché finora non si è riusciti a sviluppare un processo alternativo meno dispendioso), così come nuovi materiali per realizzare Quantum Computer con prestazioni superiori alle attuali.

Un'altra area di possibile utilizzo è rappresentata dai problemi di ottimizzazione. Con metodi di ricerca di un minimo funzionale (annealing) si risolvono già da 40 anni problemi di ottimizzazione combinatoria, sfruttando il fatto che, il principio fisico della ricerca di un equilibrio molecolare corrisponde alla minimizzazione di una funzione.

Questo ha portato l'azienda canadese D-Wave, a partire dal 2007, allo sviluppo di un Quantum Annealer di migliaia di qubit (ma utilizzati in maniera diversa rispetto a IBM) e ispirato Fujitsu nello sviluppo di annealer basati su tecnologia CMOS tradizionale.

Un esempio di ottimizzazione combinatoria in cui questi metodi sono chiamati ad operare è quello della determinazione, nel minor tempo possibile, del miglior portafoglio di investimenti in un ventaglio di titoli in continua evoluzione.

Un settore interessato al QC è quindi quello della finanza, ma anche, generalizzando il concetto di ottimizzazione, la logistica per sfruttare al meglio le risorse, individuare i percorsi migliori per il trasporto, gestire l'approvvigionamento delle materie prime e dei prodotti. Sempre nel settore finanziario, l'interesse riguarda anche l'analisi dei rischi e le previsioni di mercato, per sfruttare l'applicabilità del QC a problemi complessi in cui intervengono molte variabili che sono caratterizzati da un certo grado di incertezza.
Promettenti sono anche le aspettative del QC per accelerare maggiormente l'evoluzione dell'Artificial Intelligence/Machine Learning (AI/ML), grazie alla capacità di processare grosse moli di dati, funzionale alla classificazione delle informazioni o per individuare pattern o aree di ottimizzazione (minimo o massimo).
Ne beneficerebbero di conseguenza quei settori come la medicina, che già utilizzano l'AI/ML, per migliorare le capacità di analisi

Attività \ Pianificazione	Short Term (2020 ÷2025)	Medium Term (> 2025)	Long Term (>2030)
Simulazione	**Manifattura** (Analisi molecolare)	**Chimica** (Ingegneria molecolare, Nuovi Processi industriali) **Manifattura** (Nuovi materiali) **Agricoltura** (Nuovi fertilizzanti) **Medicina** (Nuove medicine, nuove proteine) **Logistica** (Simulazione scenari) **Finanza** (Previsioni sui derivati, Analisi di rischio)	**Medicina** (Previsioni diffusione malattie)
Ottimizzazione	**Logistica** (Routing trasporto, ottimizzazione rete di distribuzione) **Telecomunicazioni** (Pianificazione, Gestione risorse non e near real-time) **Medicina** (Finanziamento nuove medicine, Analisi struttura proteine)	**Finanza** (ottimizzazione portfolio, gestione transazioni) **Logistica** (Gestione supply chain) **Medicina** (Gestione supply chain) **Manifattura** (Ottimizzazione processi produttivi, Gestione Supply chain, Programmazione produzione)	**Telecomunicazioni** (Gestione risorse real-time)
Artificial Intelligence/ Machine Learning	**Finanza** (stime patrimoniali)	**Logistica** (Gestione imprevisti, previsioni di approvvigionamento) **Finanza** (Gestione frodi) **Telecomunicazioni** (Analisi di mercato) **Medicina** (Diagnosi mediche, Analisi genetiche, Sperimentazioni di farmaci) **Manifattura** (Controllo qualità)	**Finanza** (Raccomandazioni di acquisto) **Manifattura** (Progettazione strutturale, Fluido dinamica) **Telecomunicazioni** (Automazione (SON-like) real-time su larga scala)
Calcolo		**Crittografia** (Nuovi protocolli di sicurezza quantum-proof per comunicazioni e dati)	**Crittografia** (Cracking RSA, nuovi sistemi di protezione quantum-proof per comunicazioni e dati)

Tabella 1
Previsione di applicazione del QC a casi d'uso specifici di vari settori

e diagnosi, ma anche altri settori, come le Telecomunicazioni, per attività analoghe ma su dati di altra natura [3].
Infine, nell'ampia gamma dei servizi legati alla sicurezza delle comunicazioni e alla protezione dei dati, il QC ha già avuto e continuerà ad avere grossi impatti. Si può dire che tutta l'attività di ricerca e sviluppo e gli enormi investimenti sulle tecnologie quantistiche sono stati innescati dal rischio legato alla capacità di un computer quantistico, con sufficiente potenza di calcolo (migliaia di qubit per un quantum computer tipo quello di IBM), di poter crackare facilmente gli attuali sistemi di cifratura (RSA) utilizzando un algoritmo creato da Peter Shor nel 1994.

Molti sistemi di cifratura a protezione delle comunicazioni, transazioni e dati sensibili nei settori finanziario, sanitario, militare... si basano sulla difficoltà matematica di scomporre un numero grande nei suoi fattori primi (fattorizzazione).

Il QC riesce ad analizzare facilmente i dati in frequenza (FFT) e questo permette di risolvere il problema della fattorizzazione in tempi esponenzialmente più veloci se confrontati anche con quelli del più potente, ad oggi, supercomputer classico.

Si presume che computer quantistici tipo quello di IBM, in grado di violare gli attuali sistemi di sicurezza, saranno disponibili non prima di 10 anni. Di fronte a questo rischio sono in corso molte iniziative volte a favorire lo sviluppo di nuovi algoritmi e sistemi di protezione delle comunicazioni e delle informazioni.

Sulla base del trend di sviluppo del QC la tabella seguente mostra gli ambiti di applicazione del QC e una previsione dei tempi in cui possono esserci ricadute pratiche.

Si tratta ovviamente di stime che derivano dallo stato dell'arte della tecnologia e che potrebbero subire rivisitazioni a seguito di accelerazioni o rallentamenti che potrebbero verificarsi nell'ambito dell'attività di ricerca e sviluppo [4].

Tipologie di Quantum Computer

Il computer quantistico è stato teorizzato negli anni Ottanta del secolo scorso, quando Richard Feynman, Jurij Manin e David Deutsch arrivarono autonomamente alla conclusione che un sistema quantistico avrebbe consentito di superare gli intrinseci limiti dei computer classici - in termini di accuratezza e tempistiche di esecuzione - nell'ambito della simulazione di sistemi fisici quantistici quali atomi, molecole o materiali. Deutsch per primo introdusse il concetto di Universal Quantum Computer [5], una macchina di Turing quantistica capace di simulare qualsiasi sistema fisico finito e realizzabile con sistemi idealmente isolati (temperatura richiesta pari a 0 K) con accuratezza arbitrariamente elevata.

Il modello di Deutsch si riferisce chiaramente ad un dispositivo di difficile realizzazione, in quanto richiederebbe un hardware assolutamente fault-tolerant ed interamente quantistico [6], ovvero costituito non solo da un'unità di esecuzione quantistica ma anche da una memoria quantistica, al momento non disponibile.

Tuttavia nel mondo della computer science si è mantenuto l'interesse per l'idea originaria di integrare i principi della meccanica quantistica nella logica di calcolo. Questo ha portato allo sviluppo di varie tipologie di computer quantistici, il cui principio di funzionamento comune consiste nell'applicazione di eccitazioni esterne al sistema quantistico codificante l'informazione associata al problema da risolvere, con l'intento di provocarne un'evoluzione temporale che consenta di raggiungere uno stato finale corrispondente alla soluzione del problema.

In particolare, i principi della fisica quantistica maggiormente adoperati per cercare di ottenere un vantaggio quantistico, ovvero una risoluzione computazionalmente più efficiente della migliore corrispettiva classica, sono la sovrapposizione e l'entanglement
Secondo il principio di sovrapposizione uno stato quantistico può essere rappresentato dalla combinazione di due o più stati quantistici.

Questo implica che l'unità di informazione quantistica, il qubit (quantum bit), può trovarsi nella sovrapposizione di due stati codificanti 0 e 1, ovvero può avere nello stesso tempo probabilità non nulle di valere tanto 0 quanto 1.

Questa proprietà risulta estremamente vantaggiosa nell'ambito della computazione in quanto la stessa operazione può essere simultaneamente valutata su più campioni "in sovrapposizione" di un dataset, ciascuno dei quali associato ad uno stato quantistico. La sovrapposizione è inoltre strettamente legata al fenomeno dell'interferenza, che nella computazione quantistica è sfruttata come un meccanismo di incremento della probabilità della soluzione del problema.

L'entanglement è una proprietà dei sistemi quantistici costituiti da più sottosistemi che possono essere soggetti ad un'intrinseca correlazione che rende impossibile la loro analisi individuale. Nell'ambito dell'informazione quantistica la correlazione intrinseca tra i qubit implica che se si esegue una misurazione/lettura su uno di loro, il risultato influenza istantaneamente i corrispettivi valori degli altri. Dal momento che il principio dell'entanglement vale anche se i qubit sono spazialmente distanti, questo trova spazio non solo nell'ambito della computazione quantistica ma anche in quello delle comunicazioni quantistiche.

I principi di sovrapposizione ed entanglement sono gli elementi che conferiscono ai computer quantistici quelle potenzialità che li rendono superiori rispetto ai computer classici nel trattare certe famiglie di problemi complessi.

Sono tuttavia stati instabili, che tendono ad esaurirsi a causa della decoerenza (disturbi dell'ambiente circostante) i cui effetti, aumentando nel tempo, determinano un progressivo incremento della probabilità di errore fino alla perdita totale delle proprietà quantistiche e quindi della possibilità di sfruttare le capacità di calcolo dei computer quantistici.

Quantum Gate Array

Il computer quantistico basato su modello Quantum Gate Array (QGA) è caratterizzato dall'esecuzione di operazioni sotto forma di porte quantistiche - una sorta di estensione al qubit della progettazione logica dell'elettronica digitale classica - con le quali è possibile approssimare tutte le possibili evoluzioni unitarie di un sistema quantistico (per approfondimenti sulle porte quantistiche si rimanda a [7]).

Questo modello assume dal punto di vista hardware che l'unità di esecuzione costituisca l'unica sezione prettamente quantistica del calcolatore.
A differenza delle porte logiche classiche, che possono essere progettate con un opportuno circuito a transistor, le porte quantistiche sono implementate da campi elettromagnetici oscillanti ad una frequenza di risonanza caratteristica di ciascun qubit costituente l'hardware e il cui valore assoluto dipende dalla tecnologia di fabbricazione (per esempio per i qubit superconduttivi nella banda delle microonde, per gli ioni intrappolati nella stessa banda o addirittura in banda ottica).

In Figura 1a è riportato un generico schema a blocchi – ciascuno dei quali è costituito da porte quantistiche, come riporta il dettaglio del modulo Valutazione – di un programma quantistico basato su modello QGA, anche detto circuito quantistico per analogia con i circuiti digitali costituiti da porte logiche.
Sinteticamente il flusso processivo prevede:

FORMALISMO DEL QUANTUM GATE ARRAY

Nel modello Quantum Gate Array lo stato quantistico di un sistema a N qubit è descritto da un vettore di stato

$|\psi> = [c_0\ c_1 \dots c_{(2^N)-1}]^T = \Sigma_i c_i|i>$

dove c_i è un numero complesso chiamato ampiezza di probabilità, il cui modulo quadro $|c_i|^2$ è pari alla probabilità che il sistema si trovi nell'autostato corrispondente al vettore $|i>$ (pertanto $\Sigma_i|c_i|^2 = 1$). Nel caso di un singolo qubit gli autostati sono 2 ($|0> = [1\ 0]^T$ e $|1> = [0\ 1]^T$), mentre per N qubit sono 2^N ($|00\dots0> = [1\ 0 \dots 0]^T \div |11\dots1> = [0 \dots 0\ 1]^T$). La sfera di Bloch, che costituisce la rappresentazione geometrica di un qubit $[c_0\ c_1]T$, è osservabile in Figura Aa. Tutti i vettori delimitati dall'origine degli assi cartesiani e da un punto sulla superficie della sfera sono associabili ad uno stato di un qubit; in particolare, i due vettori paralleli all'asse z sono associati agli autostati $|0>$ e $|1>$, mentre i rimanenti descrivono uno stato con sovrapposizione. I vettori che giacciono sullo stesso parallelo differiscono per fase ϕ e sono accomunati dall'angolo ϑ e soprattutto dalle probabilità $|c_0|^2$ e $|c_1|^2$.

Le porte quantistiche corrispondono a rotazioni del vettore di stato attraverso matrici complesse unitarie U

$U\ |\psi> = U\ \Sigma_i c_i|i> = \Sigma_i c_i U|i>$

L'espressione precedente mette in evidenza la linearità del modello, per cui è possibile valutare l'effetto di una porta su ciascun autostato individualmente ($U|i>$). Questo approccio è matematicamente più agevole del prodotto matrice-vettore e consente di progettare circuiti quantistici in maniera più intuitiva. Alcune porte quantistiche notevoli sono riportate in Figura Ab (per approfondimenti si rimanda a [15]). La reversibilità è una peculiarità delle evoluzioni unitarie, per cui per ciascuna porta quantistica descritta da matrice U è possibile definire una porta duale con matrice U' che ne annulla l'effetto, ovvero $U' = U^{-1}$, dove U^{-1} è la matrice inversa di U.

Le porte a sinistra coinvolgono un solo qubit e sono riconducibili a rotazioni degli assi cartesiani di un angolo ϑ: la porta in alto si chiama X ($R_x(\pi)$) ed è la corrispettiva quantistica della NOT classica (sostanzialmente scambia le ampiezze di probabilità di $|0>$ e $|1>$), la porta Z ($R_z(\pi)$) cambia il segno dell'ampiezza di probabilità di $|1>$, la porta $R_z(\vartheta)$ è associata ad una generica rotazione di un angolo ϑ dell'asse z, infine la porta H di Hadamard ($R_x(\pi)$ seguita da $R_y(-\pi/2)$) consente di generare una sovrapposizione uniforme di stati quando applicata ad un autostato.

Le porte a destra coinvolgono due o più qubit e sono operazioni di tipo controllato, per cui applicano un'evoluzione unitaria U diversa dall'identità ad uno o più qubit target in funzione del valore di uno o più qubit di controllo: la porta CNOT in alto inverte un qubit target se un altro di controllo vale 1, mentre la porta CCNOT o di Toffoli in basso inverte un qubit target se i due qubit di controllo valgono entrambi 1. In altre parole, le porte CNOT e CCNOT modificano il qubit target secondo l'operazione booleana XOR coinvolgente il qubit target stesso e il valore controllante (il valore del qubit di controllo nel caso della CNOT, il risultato dell'operazione AND coinvolgente i due qubit di controllo nel caso della CCNOT), pertanto sono adoperabili anche con bit classici e sono dette di tipo booleano-reversibile (la reversibilità può essere dimostrata applicando due CNOT o due CCNOT consecutivamente sugli stessi qubit). L'aspetto prettamente quantistico di queste porte è chiaramente legato al fatto che sono applicabili ad uno stato quantistico in sovrapposizione, le cui coppie di ampiezze di probabilità c_{10}-c_{11} e c_{110}-c_{111} risultano scambiate in seguito all'applicazione della CNOT e della CCNOT rispettivamente.

È possibile dimostrare che H, $R_z(\pi/2)$, $R_z(\pi/4)$ e CNOT costituiscono un set universale di porte quantistiche, con le quali è possibile approssimare qualsiasi altra porta quantistica.

Le porte quantistiche introdotte in precedenza sono adoperabili negli algoritmi di Grover e variazionali. Nel primo caso la soluzione è etichettata da un circuito che cambia il segno dell'ampiezza di probabilità della soluzione e che è implementato con porte quantistiche di tipo booleano-reversibile, per asserire un qubit ausiliario di flag secondo un meccanismo analogo a quello della progettazione delle reti logiche classiche basate su tavole di verità, con la porta esclusivamente quantistica Z, per codificare il valore del qubit di flag sul segno dell'ampiezza di probabilità dello stato. Per quanto concerne i circuiti di tipo variazionale la topologia delle porte è fissata mentre gli angoli di rotazione ϑ sono aggiornati dal minimizzatore classico ad ogni iterazione.

La notazione vettoriale può essere anche adoperata per definire algebricamente l'entanglement. In un sistema a N-qubit privo di entanglement il vettore di stato può essere scomposto in N vettori, ciascuno associato ad un qubit. Per esempio, il vettore di stato coinvolgente due qubit

$|\psi> = 1/\sqrt{2}*[1\ 1\ 0\ 0]^T = 1/\sqrt{2}|00> + 1/\sqrt{2}|01>$

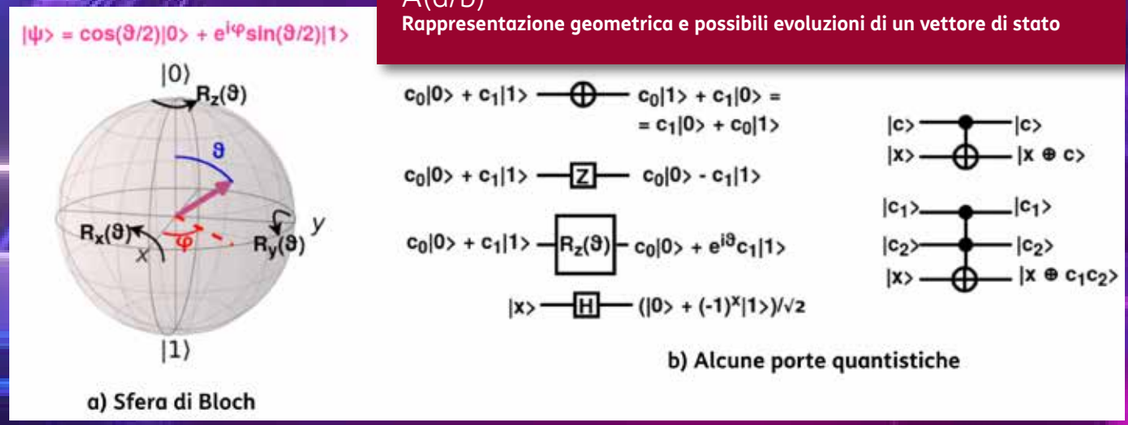
può essere scomposto in due vettori $|0>$ e $(|0> + |1>)/\sqrt{2}$. Se al contrario la scomposizione non è algebricamente possibile, allora il vettore descrive uno stato entangled. L'esempio più noto di stato entangled è il cosiddetto $|\Phi^+>$ di Bell per due qubit, il cui vettore di stato

$|\psi> = 1/\sqrt{2}*[1\ 0\ 0\ 1]^T = 1/\sqrt{2}|00> + 1/\sqrt{2}|11>$

non può essere scomposto in due vettori disgiunti. In tal caso se si misura $|0>$ sul qubit di sinistra si è certi che il qubit di destra varrà $|0>$, viceversa se si misura $|1>$ sul qubit di sinistra quello di destra varrà sicuramente $|1>$.

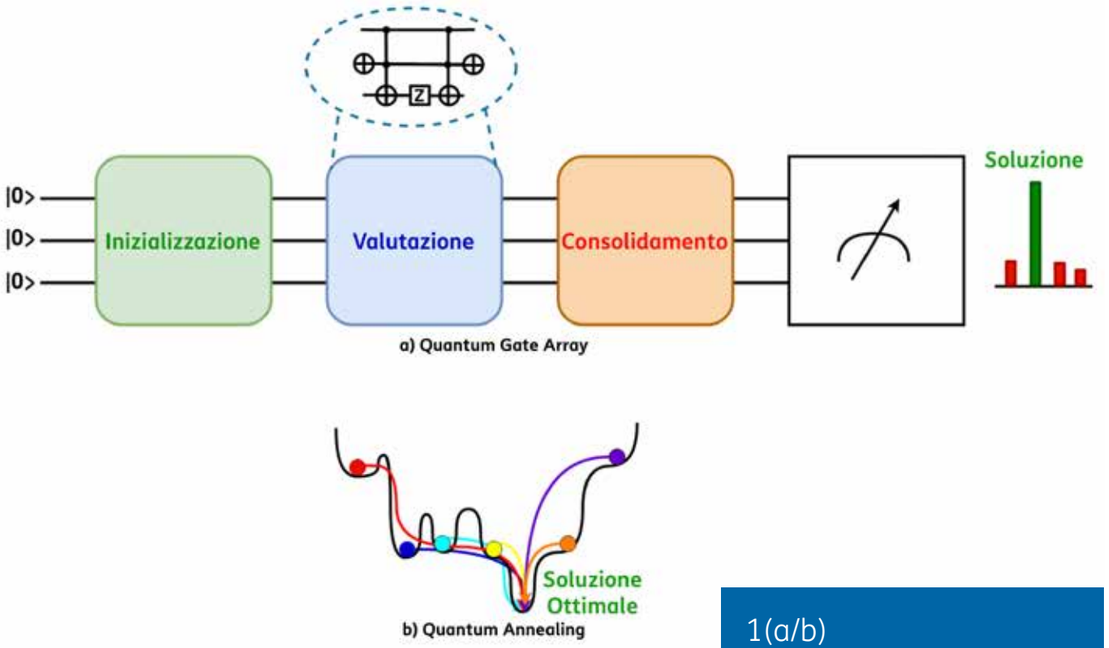
giovanni_cirillo@polito.it, edoardo.giusto@polito.it

A(a/b)
Rappresentazione geometrica e possibili evoluzioni di un vettore di stato



a) Sfera di Bloch

b) Alcune porte quantistiche



1(a/b)
Meccanismi concettuali di funzionamento di un Quantum Gate Array e di un Quantum Annealer

1. predisposizione del sistema allo stato ground |00...0>;
2. configurazione del sistema in uno stato corrispondente alla mappatura dei dati del problema (inizializzazione);
3. sfruttando il meccanismo della sovrapposizione, elaborazione simultanea su tutti gli autostati associati ai dati al fine di individuare od etichettare le soluzioni del problema (valutazione);
4. applicazione di ulteriori porte quantistiche per variare lo stato del sistema, così che la soluzione del problema presenti una probabilità di misura significativamente maggiore degli altri risultati (consolidamento).

Il modello QGA si è affermato negli anni Novanta del secolo scorso con l'individuazione dei primi problemi caratterizzati da un vantaggio quantistico.

I casi più emblematici sono rappresentati dal problema di fattorizzazione dei numeri interi, risolvibile con l'algoritmo di Peter Shor (1994) [8] con complessità polinomiale anziché esponenziale come nel caso classico e la ricerca in un insieme non ordinato, risolvibile con l'algoritmo di Grover (1996) [9] con complessità proporzionale alla radice quadrata del numero degli elementi costituenti il dataset, inferiore rispetto alla complessità lineare dell'elaborazione classica.

Pur essendo ancora basso il grado di maturità del QGA e distante dal modello computazionale del computer quantistico universale di Deutsch, questa tecnologia è la più investigata per l'analogia di funzionamento con i computer classici e quindi la versatilità di utilizzo con algoritmi in grado di risolvere problemi strettamente applicativi (per esempio di ottimizzazione o di simulazione di molecole) con evidente vantaggio quantistico.

L'hardware QGA può essere quantistico a tutti gli effetti, per esempio superconduttivo-o a ioni intrappolati o spin molecolari, oppure può essere costituito da simulatori classici in cui ci si limita a riprodurre il funzionamento di un calcolatore quantistico, calcolando la distribuzione di probabilità a fine esecuzione di un circuito e tenendo eventualmente conto delle non-idealità dell'hardware quantistico sotto forma di modelli di rumore semplificati.

Le soluzioni basate su tecnologia classica sono interessanti anche per il loro possibile impiego on-premises in particolare a livello di edge computing nel 5G per gestire applicazioni time-critical, dal momento che non necessitano di essere installate in ambienti isolati e mantenute a temperature prossime allo 0 assoluto.

Per un approfondimento sul Quantum Gate Array si rimanda al box "Formalismo del Quantum Gate Array" e per un esempio di algoritmo quantistico al box "Un esempio di algoritmo per Quantum Gate Array - Algoritmo di Grover".

Quantum Annealer vero e inspired

Il simulated annealing è un algoritmo che si è diffuso a partire dagli anni Ottanta per risolvere problemi di ottimizzazione, per individuare il minimo globale di una funzione di costo che presenta più minimi locali.

La sua variante quantistica si chiama quantum annealing [10] ed il suo corrispettivo calcolatore è chiamato Quantum Annealer (QA).
La funzione di costo di un problema risolvibile con QA viene mappata sul profilo dell'energia - quindi nell'orientazione - di un insieme di spin/qubit che interagiscono lungo un asse con altri spin e/o con un campo magnetico esterno.

Il profilo di potenziale del sistema (vedasi Figura 1b) presenta dei minimi locali ed uno globale, il cui autostato (minimo assoluto) corrisponde alla soluzione ottimale del problema.

È possibile constatare che il profilo dell'energia di un insieme di spin/qubit è assimilabile alla funzione di costo di un problema classico di ottimizzazione combinatoria Quadratic Unconstrained Binary Optimization (QUBO) [11], una categoria di problemi risolvibili classicamente con algoritmi di complessità computazionale non-polinomiale.

Elaborare un algoritmo QUBO su un QA, si traduce nell'applicazione di un campo nel piano trasverso a quello di interazione dei qubit che, come osservabile nella Figura 1b, genera una sovrapposizione di stati - in questo contesto corrispondente alla simultanea presenza del sistema in tutte le buche di potenziale del profilo energetico – e facilita il raggiungimento del minimo assoluto della funzione di costo attraverso l'effetto tunnel, secondo cui un sistema quantistico può attraversare una barriera arbitrariamente alta di energia potenziale; questa modalità di funzionamento determina il vantaggio quantistico.
Analogamente alla famiglia QGA, anche per il QA l'hardware può essere effettivamente quantistico, vedasi i chip superconduttivi di D-Wave Systems, oppure classico quantum-inspired, ovvero costituito da emulatori come quello fabbricato da Fujitsu.

Il termine quantum-inspired trae origine dal fatto che l'emulatore classico cerca di imitare il funzionamento a run-time di un ambiente quantistico (solitamente ideale) attraverso delle routine ottimizzate per la riproduzione delle evoluzioni unitarie quantistiche.
Un approccio quantum-inspired, pur mostrando dei limiti legati all'overhead di risorse classiche richieste, risulta attualmente vantaggioso in termini di numero di qubit utilizzabili (ottomila emulati

UN ESEMPIO DI ALGORITMO PER QUANTUM GATE ARRAY

Algoritmo di Grover

Pubblicato nel 1996 , fornisce un approccio nuovo al problema della ricerca di un elemento in una lista non ordinata, di tipo NP (nondeterministic polynomial time), che non è risolvibile classicamente se non con una ricerca esaustiva, che consiste banalmente nel leggere uno dopo l'altro tutti gli elementi fino a trovare quello desiderato.

Un'analogia visiva del problema può essere questa: consideriamo una fila di N cassetti, dei quali uno soltanto contiene una pallina. Per sapere dov'è, con la ricerca esaustiva dovremo aprire uno dopo l'altro al più N-1 cassetti. Ripetendo molte volte l'esperimento avremo un valore atteso per il numero di tentativi pari a N/2.

L' algoritmo di Grover ci permette invece di trovare la soluzione in un numero di passaggi pari a √N, decisamente inferiore al crescere di N.

Per restare nell' analogia della pallina nei cassetti, è come se, invece di aprire cassetti, potessimo assestare dei colpetti alla cassettiera, per individuare dall'eco dove si trova quello pieno.

Naturalmente si tratta di un'analogia che però, seppur grossolanamente, sottolinea quanto l'incremento di prestazioni dato dal Quantum Computing rispetto a quello classico non consista in un semplice aumento di velocità o di parallelismo, ma nella possibilità di mettere in atto strategie di calcolo precedentemente impossibili da realizzare.

Descrizione del funzionamento

Codifichiamo l'insieme delle N possibili soluzioni in un registro di n qubit, dove $n = \log_2(N)$.

Il primo step consiste nel preparare i qubit del registro in una sovrapposizione di stati equiprobabile, usando l'operatore $H^{\otimes n}$, chiamato porta universale di Hadamard di ordine n.

Successivamente vengono applicati al registro, in sequenza, l'operatore Oracolo (U_ω)e l'operatore diffusione di Grover ($H^{\otimes n}\cdot(2|0^n\rangle\langle 0^n| - I_n)\cdot H^{\otimes n}$).

Questa operazione altera lo stato del registro, amplificando la probabilità che in fase di lettura venga osservata la configurazione x_ω.

Per massimizzare questa probabilità la sequenza Oracolo – Grover va eseguita per un numero di iterazioni pari a √N.

Oracolo U$_\omega$

L'operatore oracolo serve per marcare un particolare stato x_ω del registro, rappresentante la soluzione. Detta x la configurazione di qubit in ingresso, l'operatore restituisce lo stesso stato x se $x \neq x_\omega$, lo stato negato $\bar{x}_\omega$ per $x = x_\omega$.

Operatore diffusione

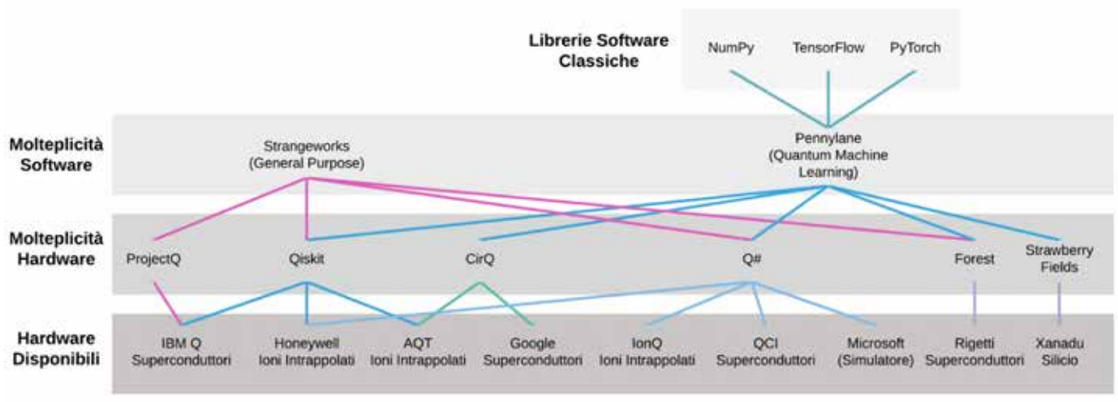
L'operatore diffusione di Grover è così definito:

$H^{\otimes n}\cdot(2|0^n\rangle\langle 0^n| - I_n)\cdot H^{\otimes n}$

A valle dell'oracolo concorre a sbilanciare la configurazione di qubit, indirizzandola verso quella marcata.

L' espressione tra parentesi altro non è, se non una regola simile a quella dell'oracolo, che però restituisce 1 per la configurazione $|0^n\rangle$ (tutti i qubit a 0) e –1 per tutte le altre.

vincenzo.cuciti@telecomitalia.it



2
Hardware/Software stack per QGA

per Fujitsu anziché duemila fisici di D-Wave), connettività tra gli stessi per stabilire le relazioni tra qubit e di conseguenza la loro fruizione (l'architettura emulata Fujitsu è fully-connected mentre in quella D-Wave la connettività tra qubit è limitata) ed assenza di effetti legati alla decoerenza durante l'esecuzione.

Le piattaforme classiche su cui eseguire gli emulatori non si limitano a dei calcolatori; infatti sono disponibili risolutori QUBO sotto forma di acceleratori hardware su Field Programmable Gate Array [12] pensati per poter ottenere vantaggi computazionali immediati on-premises.

Oltre a Fujitsu anche Toshiba e Microsoft sviluppano soluzioni hardware o software classiche (quantum-inspired) per la risoluzione di problemi di ottimizzazione.

Anche per la famiglia degli annealer valgono le stesse considerazioni evidenziate nella sezione relativa ai QGA, sull'impiego dei quantum-inspired in modalità on-premises e in particolare a livello di edge.

Annealing con Quantum Gate Array ed evoluzioni

Anche i computer QGA possono risolvere problemi di ottimizzazione attraverso tecniche ibride quanto-classiche di tipo variazionale.

In questo modello lo stesso circuito quantistico – inizializzato anche in questo caso nello stato di ground - è eseguito più volte, con i contributi delle porte quantistiche iterativamente aggiornati da un minimizzatore classico di una funzione di costo, finché non si converge ad uno stato in cui la probabilità corrispondente alla soluzione del problema è predominante rispetto a quelle di tutti gli altri stati possibili.

Le due procedure variazionali più adoperate sono il Quantum Approximate Optimization Algorithm (QAOA) [13], che emula l'evoluzione temporale di un QA, ed il Variational Quantum Eigensolver (VQE) [14], un algoritmo concepito per determinare l'energia minima di un sistema quantistico.

Ambienti di sviluppo per Quantum Computing

Sviluppo software ed accessibilità hardware

Oggigiorno il software per QC consiste principalmente in librerie Python interfacciabili ad hardware quantistico via-cloud o ad hardware classico adoperato come simulatore od emulatore a cui si accede o localmente o via-cloud.

Queste librerie sono sviluppate o da produttori di hardware quantistico – vedasi Qiskit di IBM Q, Cirq di Google, Forest di Rigetti, Strawberry Fields di Xanadu e Leap di D-Wave - o da startup che si dedicano allo sviluppo di soluzioni software - per esempio Orquestra di Zapata Computing - o da realtà accademiche come ProjectQ di ETH.

Microsoft si distingue per aver sviluppato il linguaggio di programmazione Q# (derivato da C#) attualmente utilizzabile nel Microsoft Quantum Development Kit.

La disponibilità piuttosto limitata di hardware programmabili rende necessario la definizione di ambienti multipiattaforma, che consentano quindi l'utilizzabilità del software sviluppato su quante più piattaforme possibili, tanto hardware quanto software.

Nel caso dell'hardware, la stessa libreria è interfacciabile ad hardware differenti non necessariamente dello stesso costruttore, previa autorizzazione all'accesso all'hardware.

Per esempio, Qiskit consente l'esecuzione di algoritmi quantistici sui quantum computer di IBM Q a superconduttori e di Alpine Quantum Technologies e Honeywell a ioni intrappolati, mentre il codice sviluppato in ambiente Microsoft può essere eseguito tramite i servizi cloud di Azure Quantum su hardware superconduttivo di Quantum Circuits, Inc. (spin-off dell'università di Yale) e su hardware a ioni intrappolati Honeywell e IonQ.

Per quanto concerne il software, la stessa libreria special-purpose o lo stesso ambiente general-purpose possono essere adoperate in sinergia con software sviluppato da terzi. Il caso più emblematico è costituito da Pennylane di Xanadu, una libreria Python per il Quantum Machine Learning ed interfacciabile con framework per computazione quantistica quali Qiskit, Cirq, Forest e Strawberry Fields attraverso librerie classiche e diffuse per il Machine Learning quali NumPy, Tensorflow e PyTorch. A questa categoria appartiene anche il software general-purpose sviluppato da Strangeworks che può interagire con software Qiskit, Cirq, ProjectQ e Forest.

Si potrebbero definire delle linee guida per la scelta della piattaforma di esecuzione di un algoritmo quantistico:

- se il numero di operazioni richieste per risolvere un problema è tale per cui la decoerenza è trascurabile, è in generale preferibile adoperare hardware quantistico, tenendo anche conto che l'esecuzione non risentirebbe dell'overhead computazionale intrinseco della simulazione o dell'emulazione classiche di un sistema quantistico;
- se al contrario il problema risulta irrisolvibile da un quantum computer reale, la simulazione in assenza di rumore con hardware classico risulta la scelta più ragionevole.

Dal momento che l'accesso via-cloud all'hardware reale è condiviso da migliaia di utenti ogni giorno, ogni costruttore stabilisce un limite massimo di esecuzioni giornaliere o mensili per ciascun utente.
La simulazione classica in presenza di rumore potrebbe risultare pertanto preferibile per la prototipizzazione o l'ingegnerizzazione del software, dal momento che consentirebbe di stimare i risultati attesi da un dispositivo reale e di ottimizzare l'esecuzione

senza dover “consumare” accessi all’hardware quantistico.

Modellizzazione algoritmica

Sebbene non si sia ancora consolidata una metodologia di definizione di algoritmi per QA o QGA, sia per la complessità del formalismo sia per i limiti intrinseci dell’hardware, in entrambi i casi è riscontrabile un chiaro orientamento verso un approccio ibrido iterativo in cui un computer classico non solo pilota un processore quantistico, ma ne elabora anche le soluzioni per ripresentargli un sotto-problema.

Il QA ha sostanzialmente ridotto i tempi ed aumentato l’affidabilità della risoluzione di problemi QUBO, per i quali erano già disponibili dalla fine del secolo scorso delle metodologie risolutive classiche.

Da un punto di vista metodologico due possibili approcci possono essere adoperati per la risoluzione di problemi di ottimizzazione: uno che porta allo sviluppo di una funzione di costo (Hamiltoniana) da minimizzare, l’altro basato su metodi che legano la rappresentazione del problema all'architettura del QA.
Il problema dell'assegnazione dei PCI nelle reti LTE e 5G, descritto in un articolo del notiziario tecnico di aprile [16], è stato affrontato con entrambi gli approcci.

L’approccio legato all’Hamiltoniana riconduce il problema ad un modello che consiste nel trovare la combinazione ottimale (Optimization) di un set di variabili binarie (Binary), che possono cioè assumere due soli valori mutuamente esclusivi (0/1, si/no, on/off...), minimizzando un polinomio quadratico (Quadratic) che, oltre a modellare il problema, include anche i vincoli a cui le variabili devono sottostare, arrivando così ad una formulazione matematica compatta, formalmente senza vincoli, perché inglobati e quindi Unconstrained.

Mettendo assieme le varie parole chiavi in inglese si ottiene l’acronimo QUBO. La definizione del polinomio segue regole codificate [11] da cui si può costruire una matrice QUBO che, ad esempio, associa un peso tra ogni variabile e ad ogni risorsa ed è fornita come input al QA. La costruzione di questa matrice a partire dall'Hamiltoniana può essere semplificata e automatizzata attraverso librerie quali PyQUBO [17] accessibili via API, anche se rispetto ad uno sviluppo ad-hoc potrebbe essere meno performante.

Il secondo approccio (di prossima pubblicazione) risolve l'assegnazione dei PCI tramite una serie di bisezioni. Il set iniziale di siti viene ripartito in due sottogruppi distinti, compilando la matrice QUBO in modo che siano minime le relazioni tra i due sottogruppi (minima l’interferenza). Il procedimento è iterato su ogni sottogruppo che si è generato nella suddivisione precedente, finché le dimensioni si riducono al punto da trovare una soluzione che minimizza il numero di PCI assegnati.

Una volta completata la serie di bisezioni successive si esegue una fase di retroazione, che consiste nel raggruppare un numero di sottogruppi pari ad una potenza di due, smantellando quindi parte del lavoro di ripartizione e creando così un nuovo sottogruppo maggiore sul quale viene applicato nuovamente il processo di suddivisione; questa retroazione permette di uscire da eventuali minimi locali. Il procedimento termina assegnando i PCI alle singole antenne.
Le dimensioni dei sottogruppi si riducono progressivamente ad ogni iterazione fino ad arrivare a dimensioni gestibili con le attuali potenze di calcolo dei quantum computer QA e quindi il processo scala efficacemente anche per migliaia di celle, senza la necessità di dover applicare algoritmi di partizionamento sui set di celle.

I computer QGA, pur essendo teoricamente più completi e versatili dal punto di vista computazionale rispetto ai QA, risultano meno maturi per applicazioni pratiche tanto in termini di qubit equipaggiati (decine anziché migliaia) quanto in termini di metodologie di sviluppo di algoritmi.

Tuttavia l’esperienza acquisita negli ultimi due decenni consente di definire delle procedure progettuali generalmente valide. Innanzitutto si

potrebbe osservare che, pur essendo i fenomeni alla base della computazione quantistica in molti casi controintuitivi, il formalismo matematico che li descrive è preciso.

L'approccio generalmente più affidabile è costituito dall’algebra lineare complessa, secondo cui tutte le operazioni sono matrici di evoluzioni unitarie che modificano lo stato del sistema quantistico.

Cercando una declinazione più prettamente circuitale, si può osservare che entrambi gli algoritmi di Grover e variazionali – i quali sono oggigiorno quelli di maggiore utilizzo per la loro versatilità - presentano delle ripetizioni delle fasi di valutazione e di consolidamento (si veda la Figura 1) finalizzate ad una massimizzazione della probabilità di ottenere la migliore soluzione del problema, con la sostanziale differenza che nel caso di Grover l’iterazione è eseguita interamente sul Quantum Computer mentre nel caso variazionale questa coinvolge anche un computer classico.

Si può dunque concludere che nella formulazione di un algoritmo per architettura QGA è solitamente richiesto di ripetere delle operazioni per consolidare il risultato finale.
La scelta dell’uno o dell’altro algoritmo dipende notevolmente dalla complessità del circuito da progettare e dal tipo di soluzione da individuare.
Se la soluzione del problema è assoluta (una e una sola, eventualmente comune a più dati) è possibile adoperare l’algoritmo di Grover, la cui valutazione corrisponde all’etichettatura della soluzione con un apposito circuito chiamato oracolo, che valuta simultaneamente la condizione di etichettatura su tutti i possibili stati in sovrapposizione/dati del dataset. L’oracolo potrebbe tuttavia risultare troppo complesso - in termini di numero totale di porte quantistiche e numero di qubit ausiliari richiesti - per un’esecuzione su hardware reale, pertanto i risolutori Grover per casi d’uso concreti sono attualmente eseguiti su simulatori classici di qubit ideali.

Se la soluzione del problema è invece relativa (ottimale tra una serie di soluzioni possibili), l’approccio variazionale è preferibile.

Si potrebbe partire dal QAOA, riproponendo quindi le metodologie di modellizzazione del QA su un QGA, con l’evidente limite legato al minor numero di qubit adoperabili.

Questo algoritmo si basa su un circuito quantistico fissato (simulatore del QA) e una funzione di costo non specifica e scelta dal progettista.

Un interessante vantaggio dei circuiti variazionali rispetto a quelli fissati come quello di Grover è che l'ottimizzatore classico cerca di compensare gli effetti della decoerenza durante l’esecuzione; tuttavia se il numero di operazioni richieste è tale per cui la decoerenza risulta in ogni caso significativa, potrebbe essere preferibile il VQE.

Questo si distingue per l’utilizzo di una specifica funzione di costo - il valore atteso di un sistema quantistico, che risulta sempre maggiore o uguale all’energia minima del sistema - ed adopera come circuito un ansatz, ossia un circuito parametrico non strettamente legato al problema e concepito per ispezionare lo spazio delle soluzioni in funzione del valore atteso, garantendo la possibilità di generare entanglement [18].

Pur essendo un ansatz potenzialmente più semplice del circuito del QAOA, il calcolo del valore atteso potrebbe richiedere un numero maggiore di operazioni di quello della funzione di costo del QAOA, aumentando così i tempi di esecuzione dell’intera procedura iterativa.

Conclusioni

L’utilizzo su larga scala del QC è ancora lontano, ma può essere utilizzato fin da subito traendo i benefici che derivano dal cosiddetto vantaggio quantistico.

Proprio perché non si dispone ancora del “Universal Quantum Computing”, gli use cases trattabili devono essere selezionati in funzione delle potenzialità e delle modalità di impiego attuali della tecnologia, secondo un processo di verifica che

tenga conto indicativamente di alcune linee guida:

1. l'area annealing è più matura e pronta all'uso rispetto ai modelli che si ispirano al universal quantum computer (gate array)
2. l'annealing è più adatto per problemi di ottimizzazione (combinatoria), categoria tra le più importanti e diffuse in vari campi in particolare anche nel settore delle telecomunicazioni
3. la complessità computazionale degli use cases deve essere commisurata alla potenza di calcolo delle soluzioni attuali di QC e può essere gestita dimensionando i dati con tecniche di partizionamento di cui esiste una consolidata esperienza di algoritmi classici
4. l'accesso alle soluzioni di QC avviene via cloud e quindi questa modalità può essere utilizzata per use case non-real o near-real time
5. sono disponibili soluzioni quantum-inspired basate su tecnologia tradizionale, che possono essere installate on-premises, con una maggiore maturità nell'area annealing e che possono essere impiegate per applicazioni real-time, eventualmente dimensionando opportunamente il problema (vedi punto 3 precedente)

Prendendo come riferimento questo quadro ci si rende conto come il numero delle applicazioni candidabili per essere sviluppate già adesso in ottica QC è elevato. Il loro numero è destinato col tempo ad ampliarsi, coerentemente con il miglioramento della tecnologia e di conseguenza delle "linee guida" che progressivamente imporranno sempre meno limiti.

Siamo ormai nella fase in cui possiamo sfruttare la potenza computazionale del QC ■

Riferimenti

1. KATWALA, A. (2020, 03 18). Inside big tech's high-stakes race for quantum supremacy. Tratto da Wired: https://www.wired.co.uk/article/quantum-supremacy-google-microsoft-ibm
2. KATWALA, A. (2020, 03 05). Quantum computers will change the world (if they work). Tratto da Wired: https://www.wired.co.uk/article/quantum-computing-explained
3. Moltzau, A. (2019, 10 13). Quantum Information and AI. Tratto da Medium: https://towardsdatascience.com/quantum-computing-and-ai-789fc9c28c5b
4. A Quantum Computing Use Case Roadmap from IBM. (s.d.). Tratto da Quantum Computing Report: https://quantumcomputingreport.com/a-quantum-computing-application-roadmap-from-ibm/
5. David Deutsch and Roger Penrose - 1997 - Quantum theory, the Church–Turing principle and the universal quantum computer, Proc. R. Soc. Lond. A40097-117, http://doi.org/10.1098/rspa.1985.0070
6. Jack Krupansky - 2019- What Is a Universal Quantum Computer?, https://medium.com/@jackkrupansky/what-is-a-universal-quantum-computer-db183fd1f15a
7. Travis S. Humble, Himanshu Thapliyal, Edgard Munoz-Coreas, Fahd A. Mohiyaddin, Ryan S. Bennink - 2018- Quantum Computing Circuits and Devices, https://arxiv.org/pdf/1804.10648.pdf
8. Peter W. Shor - 1994 - Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134, doi:10.1109/sfcs.1994.365700
9. Lov Grover - 1996 - A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996), https://arxiv.org/abs/quant-ph/9605043
10. 10. Tadashi Kadowaki, Hidetoshi Nishimori - 1998 - Quantum annealing in the transverse Ising model, Physical Review E 58.5, https://journals.aps.org/pre/abstract/10.1103/PhysRevE.58.5355
11. Fred Glover, Gary Kochenberger, Yu Du - 2019 - A Tutorial on Formula ting and Using QUBO Models, https://arxiv.org/abs/1811.11538
12. 3. Yu Zou, Mingjie Lin - 2020 - Massively Simulating Adiabatic Bifurcations with FPGA to Solve Combinatorial Optimization, https://dl.acm.org/doi/pdf/10.1145/3373087.3375298
13. Edward Fahri, Jeffrey Goldstone - 2014 - A Quantum Approximate Optimization Algorithm, https://arxiv.org/pdf/1411.4028.pdf
14. Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, Jeremy L. O'Brien - 2014 - A variational eigenvalue solver on a photonic quantum processor, https://www.nature.com/articles/ncomms5213.pdf
15. Travis S. Humble, Himanshu Thapliyal, Edgard Munoz-Coreas, Fahd A. Mohiyaddin, Ryan S. Bennink - 2018- Quantum Computing Circuits and Devices, https://arxiv.org/pdf/1804.10648.pdf
16. Andrea Boella, Michele Federico, Giuseppe Minerva, Mauro Alberto Rossotto - 2020 - Quantum computing per l'ottimizzazione delle reti mobili (4.5G e 5G), https://www.telecomitalia.com/content/tiportal/it/notiziariotecnico/edizioni-2020/n-1-2020/Quantum-Computing-ottimizzazione-delle-reti-mobili.html
17. Kotaro Tanahashi, Shinichi Takayanagi, Tomomitsu Motohashi, Shu Tanaka – 2019 - Application of Ising Machines and Software Development for Ising Machines, https://journals.jps.jp/doi/full/10.7566/JPSJ.88.061010
18. Samuel Yen-Chi Chen, Chao-Han Huck Yang, Jun Qi, Pin-Yu Chen, Xiaoli Ma, Hsi-Sheng Goan - 2019 - Variational Quantum Circuits for Deep Reinforcement Learning, https://arxiv.org/pdf/1907.00397.pdf

Librerie software per Quantum Computing e di supporto

1. NumPy - https://numpy.org/
2. TensorFlow - https://www.tensorflow.org/
3. PyTorch - https://pytorch.org/Pennylane - https://pennylane.ai/
4. Qiskit - https://qiskit.org/
5. Cirq - https://cirq.readthedocs.io/en/stable/
6. Strawberry Fields - https://strawberryfields.readthedocs.io/en/stable/#
7. Forest - http://docs.rigetti.com/en/stable/
8. Q# - https://www.microsoft.com/en-us/quantum/development-kit
9. ProjectQ - https://projectq.ch/

Costruttori di hardware per Quantum Computing

1. IBMQ - https://www.ibm.com/quantum-computing/
2. Honeywell - https://www.honeywell.com/en-us/company/quantum
3. IonQ - https://ionq.com/
4. AQT - https://www.aqt.eu/
5. Google - https://research.google/teams/applied-science/quantum/
6. Microsoft - https://www.microsoft.com/en-us/quantum
7. Rigetti - https://rigetti.com/
8. Xanadu - https://www.xanadu.ai/
9. Quantum CIrcuits, Inc. - https://quantumcircuits.com/
10. D-Wave - https://www.dwavesys.com/

Servizi cloud per Quantum Computing

1. IBM Quantum Experience - https://quantum-computing.ibm.com/
2. Microsoft Azure Quantum - https://azure.microsoft.com/en-us/services/quantum/#features
3. Strangeworks - https://strangeworks.com/
4. DWave - https://cloud.dwavesys.com/

Giovanni Amedeo Cirillo *giovanni_cirillo@polito.it*

Ha conseguito la Laurea e la Laurea Magistrale in Ingegneria Elettronica al Politecnico di Torino nel 2016 e nel 2018 rispettivamente. È attualmente dottorando in Ingegneria Elettronica presso il laboratorio VLSI del Dipartimento di Elettronica e Telecomunicazioni del Politecnico di Torino, sotto la supervisione del Prof. Maurizio Zamboni, della Prof.ssa Mariagrazia Graziano e della Dott.ssa Giovanna Turvani. Le sue attività di ricerca sono principalmente dedicate allo sviluppo di un framework multilivello per la simulazione e l'ingegnerizzazione di tecnologie per Quantum Computing, con attuale particolare interesse per quelle molecolari (per ulteriori informazioni https://www.vlsilab.polito.it/quantumcomputing/) ■

Filippo Gandino *filippo.gandino@polito.it*

Filippo Gandino (Socio IEEE) ha conseguito i diplomi M.S. e Ph.D. in Ingegneria Informatica presso il Politecnico di Torino, rispettivamente nel 2005 e nel 2010. Attualmente è Professore Associato presso il Dipartimento di Automatica e Informatica del Politecnico di Torino. I suoi interessi di ricerca includono ubiquitous computing, RFID, WSN, sicurezza e privacy, modellazione di rete e quantum computing ■

Edoardo Giusto *edoardo.giusto@polito.it*

Ha conseguito la Laurea e Laurea Magistrale in Ingegneria Informatica al Politecnico di Torino nel 2015 e nel 2017 rispettivamente. È attualmente dottorando in Ingegneria Informatica presso il Dipartimento di Automatica e Informatica (DAUIN) del Politecnico di Torino, sotto la supervision del Prof. Maurizio Rebaudengo, del Prof. Bartolomeo Montrucchio e del Prof. Filippo Gandino. I suoi interessi di ricerca comprendono le Wireless Sensor Networks, l'IoT e il Quantum Computing ■

Giovanni Mondo *giovanni.mondo@telecomitalia.it*

Laurea in Ingegneria Elettronica e Dottorato in Robotica presso l'Università di Genova, Laurea triennale in Economia presso UniNettuno. Inizia a collaborare nella ricerca di TIM (all'epoca CSELT) nel 1998 e viene assunto nel 2001. Ha collaborato a diversi progetti legati ai servizi per le reti mobili cellulari, principalmente come sviluppatore lato server. Da fine 2018 alle attività di amministrazione server e Information Visualization affianca quella di analisi del Quantum Computing in generale e dello sviluppo di modelli ispirati al Quantum Annealing in particolare ■

QUANTUM COMMUNICATION: I PRIMI PASSI VERSO LA QUANTUM INTERNET

Andrea Boella, Mauro Alberto Rossotto

Negli ultimi anni si è assistito ad uno sviluppo crescente delle tecnologie quantistiche, con una serie di innovazioni a livello sperimentale di portata tale da poter parlare di una nuova quantum revolution. Questa nuova fase cambierà il ruolo della meccanica quantistica, trasformandola da un dominio accessibile ad un ristretto numero di persone che si occupano di ricerca avanzata nel campo della fisica ad una tecnologia di uso comune.

Nell'arco di una o due decadi tutti avranno accesso a computer quantistici connessi ad una Internet quantistica, con i quali potranno lavorare utilizzando e sviluppando nuove applicazioni.

Ci troviamo quindi agli albori di una nuova era, in una fase simile a quella che ha visto la nascita di Internet.

La Quantum Internet sarà portatrice di nuove applicazioni, alcune delle quali al momento non ancora individuate poiché, come tutte le tecnologie rivoluzionarie, le sue reali potenzialità si riveleranno col suo progressivo utilizzo, abilitando quindi ulteriori applicazioni in aggiunta a quelle che già oggi si riesce a prevedere come possibili.

Introduzione

L'interesse verso le tecnologie quantistiche, nasce dal fatto che lo sviluppo tecnologico raggiunto, rende realistico il loro impiego in un contesto di servizio su un orizzonte temporale relativamente prossimo. Le attuali previsioni, che collocano la loro diffusione su larga scala in un periodo variabile tra i 5 – 10 anni a seconda della piattaforma/applicazione quantistica, potrebbero subire un'anticipazione considerando il livello di investimento e l'intensa attività di ricerca che è stato attivato.

La competizione per la leadership tecnologia, che si è innescata a livello mondiale, è spinta soprattutto dai rischi per la security delle comunicazioni e dello storage dei dati, dal momento che queste tecnologie rendono facilmente violabili gli attuali sistemi di cifratura. Nello stesso tempo offrono anche nuovi strumenti per sviluppare soluzioni di security resistenti a queste stesse tecnologie; da qui discende l'interesse ad essere tra i primi a padroneggiarle.

Questa nuova fase della meccanica quantistica è stata definita quantum 2.0. La differenza principale rispetto al periodo in cui venne teorizzata (prime decadi del '900) risiede nella maturità tecnologica raggiunta, grazie alla quale è possibile controllare e manipolare le particelle subatomiche con un'elevata precisione abilitando così lo sviluppo di nuove tecnologie/applicazioni quantistiche.

Nell'ambito delle tecnologie quantistiche si possono facilmente distinguere due principali aree per driver e trend di sviluppo tecnologico e che possono essere rispettivamente denominate quantum computing (per il processing e storage delle informazioni) e quantum commmunication (per i servizi di comunicazione).

Pur essendo la ricerca per queste tecnologie ancora prevalentemente nel campo della fisica, la maturità tecnologica della quantum communication è ad un livello più avanzato, essendo infatti già disponibili prodotti commerciali e installazioni di servizi "pseudo-commerciali".

All'area della quantum communication afferisce l'infrastruttura di rete denominata Quantum Internet, che garantirà le connessioni e comunicazioni quantistiche.

Analogamente alla rete Internet, che costituisce un'infrastruttura globale per interconnettere end-nodes classici (e.g., laptops, smart phones, servers) e realizzare comunicazioni standard, la Quantum Internet costituirà l'infrastruttura globale per collegare i quantum end-nodes, abilitando nuove tipologie di servizi (quantum communication).

Continuando nell'analogia, nelle comunicazioni classiche le informazioni sono codificate in bit e trasmesse sulla rete Internet classica, mentre nelle comunicazioni quantistiche le informazioni sono codificate in qubit (quantum bit) e lo stato di questi qubit viene trasmesso sfruttando i principi fisici alla base del funzionamento della Quantum Internet.

Qubit e Quantum Computing

Il qubit o quantum bit è una grandezza logica che rappresenta l'unità di informazione quantistica, equivalente del bit, unità di informazione classica. I principi che sottendono l'implementazione del qubit, si basano su proprietà delle particelle subatomiche che variano tipicamente tra due livelli, a cui si fanno corrispondere i due valori logici 0 e 1 che qubit e bit possono assumere. A differenza dei bit che possono assumere solo uno dei due valori possibili in maniera esclusiva (0 OR 1), i qubit possono trovarsi in uno stato di:

Superposition: in questo stato (Figura 1) il qubit assume entrambi i valori (0 AND 1) contemporaneamente, in una sovrapposizione che può non essere bilanciata, nella quale cioè la componente del valore 0 incida in maniera diversa rispetto alla componente del valore 1 nella determinazione dello stato del qubit. Lo stato di superposition è molto delicato e viene compromesso a causa di qualunque disturbo esterno (e.g. vibrazione, rumore) ma è fondamentale per ottenere lo speed-up di prestazioni dei computer quantistici.

I computer quantistici per il processing e storage delle informazioni saranno gli end-node della Quantum Internet.

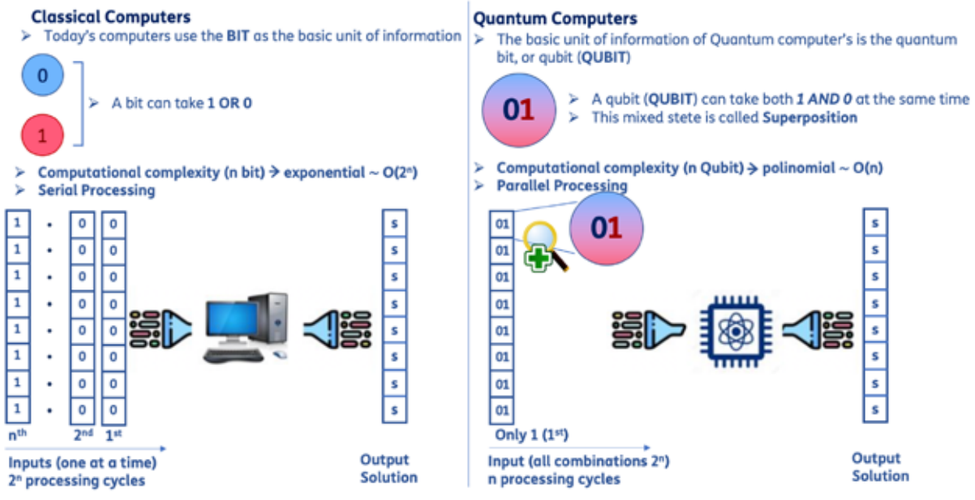
Questi processori operano sui qubit in una corrispondenza analoga a quella che lega computer classici e bit. La differenza rispetto a questi, risiede nel fatto che i primi sfruttano i principi della meccanica quantistica per utilizzare nuove modalità di processing delle informazioni.
In termini semplificativi, grazie alla superposition, un set di N qubit può essere configurato in uno stato in cui tutte le 2N combinazioni sono contemporaneamente presenti e di conseguenza processate in una forma di elaborazione "parallela".

Grazie a questa modalità di processing il computer quantistico risulta esponenzialmente più veloce nel trattare problemi complessi di natura combinatoria, rispetto ad un computer classico che invece opera in modalità seriale, scansionando cioè tutto il set di 2N combinazioni e utilizzandone solo una ad ogni ciclo elaborativo.

Principi della meccanica quantistica alla base della Quantum Internet

Il funzionamento della Quantum Internet si basa su alcuni principi della meccanica quantistica, tra i

1 Classical and Quantum Computing
Il bit, unità di informazione classica, può assumere solo uno dei due possibili valori alla volta (0 OR 1) mentre i qubit, unità di informazione quantistica, possono assumere entrambi i valori (0 AND 1) contemporaneamente (superposition). Questa è uno dei principi della meccanica quantistica che consente ai computer quantistici di avere prestazioni esponenzialmente più elevate rispetto ai computer classici per alcune famiglie di problemi complessi



quali lo stato di Superposition già descritto, che, che costituiscono il fattore differenziante rispetto all'Internet "classica" [1][4]:

Measurement: l'operazione di misura, che si effettua per esempio per una lettura,modifica irreversibilmente lo stato di un qubit, facendogli perdere lo stato di superposition e forzandolo ad assumere uno dei due stati (0 o 1) estremi (collapsing), che manterrà in qualunque misura successiva, rendendolo di fatto uguale ad un bit. L'effetto della misura può essere sfruttato per sviluppare soluzioni di security, per rilevare se l'informazione trasmessa è stata intercettata e quindi letta da un intruso.

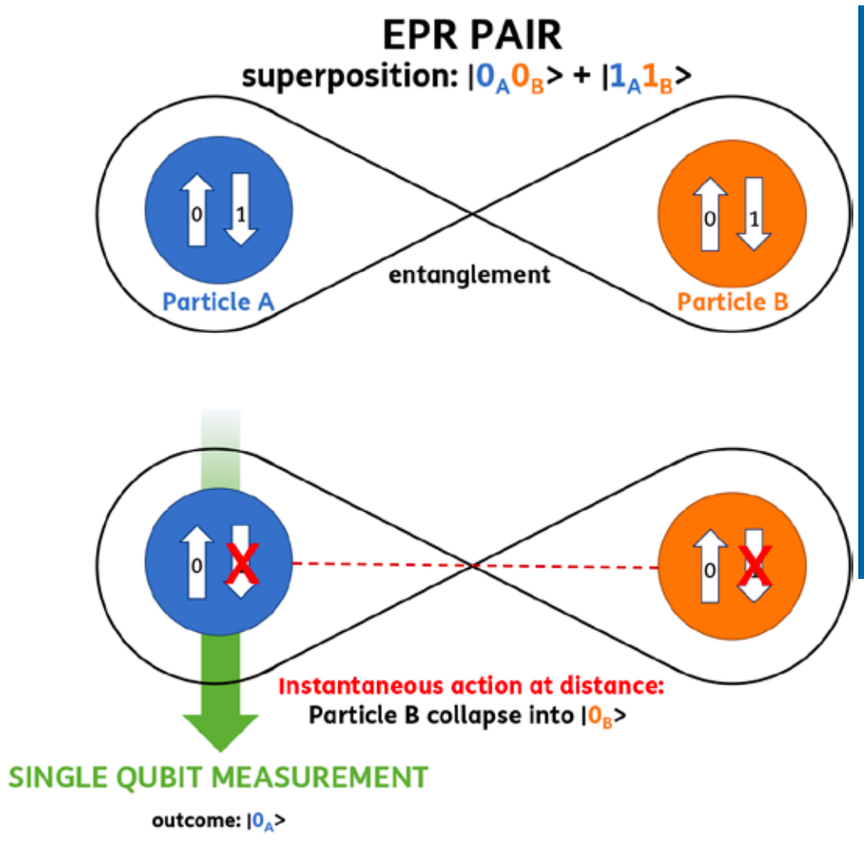
No-Cloning Theorem: per evitare di alterare lo stato del qubit con un'operazione di misura, si potrebbe pensare di effettuarne una copia senza leggerne lo stato. Il no-cloning theorem sancisce l'impossibilità di creare una copia identica di uno stato quantico ignoto.
I due principi di measurement e no-cloning theorem impediscono pertanto di ricorrere agli stessi meccanismi che si utilizzano nelle reti classiche per amplificare e rigenerare il segnale, dal momento che tutti si basano sulla possibilità di effettuare una lettura e/o copia accurata dell'informazione trasmessa (qubit). Fenomeni come attenuazione e rumore introdotti dal canale trasmissivo andranno quindi fronteggiati in maniera diversa con le reti quantistiche.

Entanglement: due oggetti/particelle in entanglement si trovano in una relazione di correlazione così stretta che la misura di uno dei due influenza lo stato dell'altro indipendentemente dalla distanza che li separa. In tale condizione lo stato quantico di ogni oggetto/particella non può essere definito individualmente, ma solo in relazione agli altri oggetti con cui condivide lo stato di entanglement. L'entanglement si genera attraverso un'interazione tra due oggetti vicini, ma una volta creato, lo stato si mantiene anche se gli oggetti vengono separati da grandi distanze. [1][2]

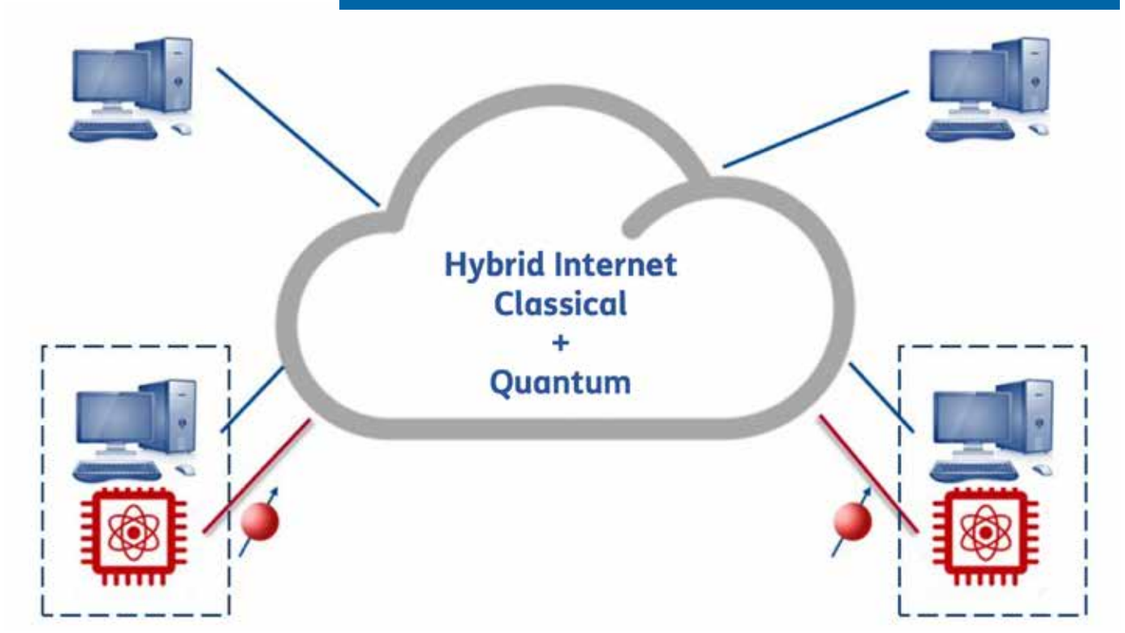
L'Entanglement nelle comunicazioni quantistiche

Nel campo delle reti quantistiche, l'entanglement si contestualizza nella correlazione che si instaura tra due qubit. Così come rappresentato nella Figura 2, la coppia di qubit (denominata EPR pair – Einsten-Podolsky-Rosen) si trova in uno stato di "superposision", in cui le due configurazioni possibili (entrambi i qubit a 0 o entrambi i qubit a 1) sono equamente probabili.

Misurando ogni qubit in forma indipendentemente, il risultato che si ottiene da ognuno può essere 0 o 1 in maniera equiprobabile, ma i due qubit agiscono in maniera coordinata, perché lo stato di entanglement iniziale li forza ad assumere



2 Entanglement tra due qubit (EPR pair)
Misurando uno dei due qubit, si ottiene come risultato 0 o 1 in maniera equiprobabile; istantaneamente e indipendentemente dalla distanza che li separa, lo stato del secondo qubit cambia concordemente alla relazione di entanglement iniziale (entrambi qubit a 0 o entrambi a 1) (Fonte: [1])



3 Hybrid Internet
The quantum Internet will operate in synergy with the classical Internet

lo stesso valore (entrambi a 0 o a 1).
Esistono altre configurazioni di entanglement (e.g. i due qubit hanno valori opposti), nelle quali esiste lo stesso tipo di coordinazione tra qubit, per cui nel momento in cui se ne misura uno, istantaneamente il suo "gemello" assume un valore inequivocabile che deriva dalla relazione di entanglement di partenza.

Più in generale l'entanglement può essere anche realizzato su gruppi costituiti da più di due qubit (multipartite entanglement).

L'entanglement ha due caratteristiche interessanti per lo sviluppo di nuove applicazioni di una rete quantum:

- instaura relazioni di correlazione più strette di quelle classiche, abilitando applicazioni che si basano sul coordinamento di più entità
- non può essere condiviso, nel senso che un qubit diverso da quelli in entanglement non può inserirsi in questa relazione. Quindi l'entanglement permette di realizzare delle connessioni "private" e inaccessibili ad entità esterne.

Quantum Internet

La Quantum Internet costituirà l'infrastruttura per trasmettere i qubit e condividere il loro stato tra gli end-nodes quantistici (quantum computers ecc...).
Per parlare di rete quantistica non è sufficiente che sia costituita da nodi quantum che comunicano in modalità classica, ma è necessario che i nodi si scambino qubits e distribuiscano stati di entanglement tra di loro.

E' bene sottolineare come alla base dello sviluppo della Quantum Internet non ci sia l'obiettivo di sostituire, migliorare o surclassare l'Internet classica.

Al contrario, la Quantum Internet opererà in sinergia con la rete esistente, andando a costituire una rete Internet ibrida, "classica" e "quantistica".
In questa nuova rete ibrida la quantum Internet interverrà per supportare nuove funzionalità che consentiranno di migliorare/arricchire le comunicazioni e applicazioni "classiche".[3]Le nuove applicazioni "quantistiche" a loro volta, per poter funzionare, si appoggeranno alle comunicazioni classiche della rete Internet.[Figura 3]

L'architettura delle reti quantistiche rifletterà quella delle reti classiche, in quanto sarà costituita da elementi che avranno ruoli analoghi ai loro corrispondenti classici, sebbene funzioneranno basandosi sui principi della meccanica quantistica: nodi sede di processori quantistici, switch e router quantistici oltre ai mezzi trasmissivi.

La Quantum Internet sarà il risultato di un grosso sviluppo, che inizialmente partirà con la realizzazione di reti quantistiche "locali", che collegheranno pochi nodi e con connessioni a basse velocità; questi nuclei iniziali verranno progressivamente espansi e connessi fino ad arrivare a costituire una rete globale, la Quantum Internet.

E' presumibile che, in questo scenario di sviluppo, i primi gestori e/o utilizzatori delle reti quantistiche saranno gli enti governativi, i centri accademici, i telecom providers, i fornitori del mondo high tech, gli istituti finanziarie i settori militare e dell'intelligence.
La fase commerciale si aprirà successivamente, con il rilascio "massivo" di servizi per la Quantum Communication economicamente accessibili.

La soluzione al momento più realistica per la trasmissione dei qubit (i cosidetti "flying" qubit per distinguerli dai "matter qubit" residenti negli end-nodes quantum e utilizzati per processare o memorizzare informazioni), consiste nell'utilizzo dei fotoni, in virtù di una serie di ragioni:

- hanno proprietà (e.g. polarizzazione, posizione ecc...) i cui stati possono essere utilizzati per codificare facilmente dei qubit
- interagiscono debolmente con l'ambiente, cosa che li rende maggiormente immuni ai disturbi e quindi "robusti" nel mantenere lo stato quantistico che trasportano
- sono facilmente controllabili e possono essere trasmessi per esempio su fibra, utilizzando la tecnologia ottica di cui esiste già un'ampia e consolidata esperienza
- hanno velocità di trasmissione elevate

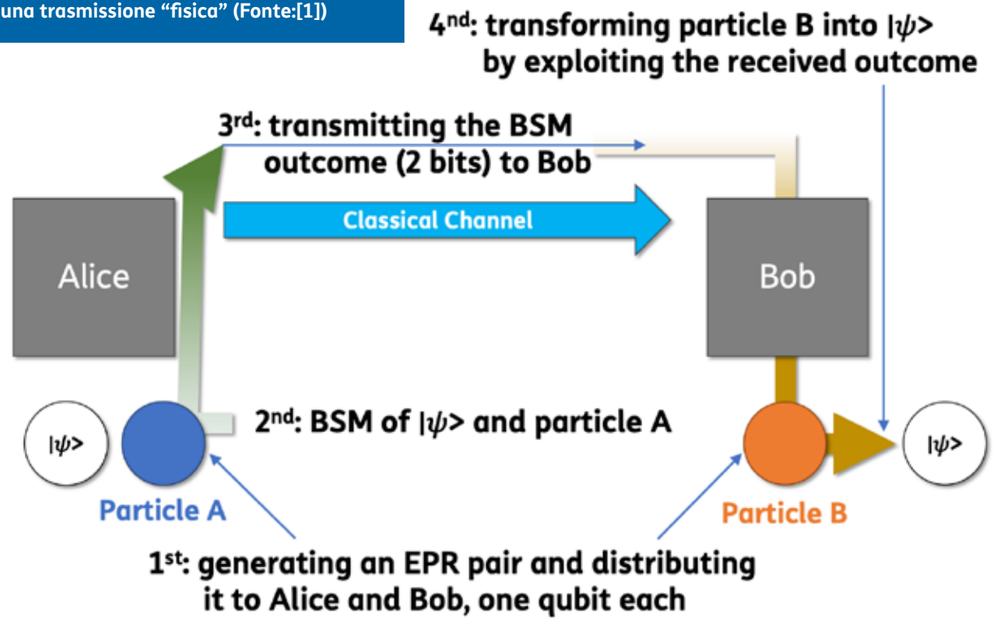
In aggiunta a tutto ciò, occorre considerare il vantaggio di permettere il riutilizzo dell'infrastruttura in fibra ottica esistente, salvaguardandone gli investimenti.[1][2]

In questo scenario occorre considerare che le distanze su cui può avvenire efficacemente la trasmissione dell'informazione quantistica tramite fotoni sono limitate: alcune decine di km per trasmissione su fibra e poche migliaia di km in free space (via satellite).

Questo perché il "quantum" di informazione trasportato da un "flying photon" non può essere amplificato o rigenerato a causa dei principi di quantum measurement e no-cloning theorem. Pertanto al crescere della distanza percorsa, si accumulano gli effetti di attenuazione e rumore, tipici dei canali trasmissivi, sul fotone aumentando il rischio che venga smarrito o corrotto e di conseguenza che si perda l'informazione quantistica che veicola.

Una prima soluzione per ovviare al problema, consiste nel sezionare le distanze lunghe in tratte più brevi, sulle quali i fotoni possono essere trasmessi e ricevuti in maniera sufficientemente affidabile. Questi vari segmenti componenti sono attestati ai cosiddetti "trusted node", nodi nei quali l'informazione da trasmettere viene estratta dai fotoni

4 Quantum Teleportation
Un qubit "informativo" dallo stato ignoto $|\psi\rangle$ è trasportato da nodo origine a destinazione, senza una trasmissione "fisica" (Fonte:[1])



ricevuti e ricodificata nei fotoni che verranno inviati al nodo successivo lungo il cammino che collega i due end-nodes. Una rete costituita da "trusted nodes" non può definirsi propriamente quantum, perché l'informazione trasmessa è classica e viene protetta a livello quantistico solo sui link trasmissivi, mentre nei "trusted node" questi dati sono decodificati e disponibili "in chiaro". La security dell'informazione si basa sul fatto che, se il nodo è "trusted", a livello ambientale sono state applicate una serie di misure atte a prevenire che soggetti non "autorizzati" entrino in possesso delle informazioni.
La trasmissione basata su "trusted node", è quella momento realizzabile su una rete live, per trasportare l'informazione quantistica su lunghe distanze.

La soluzione che permetterà di superare i limiti di massima distanza trasmissiva e che renderà effettivamente "quantistiche" le reti, è la "Quantum Teleportation", tecnologia che si sta attualmente sperimentando in laboratorio.(Figura 4)
Con la "Quantum Teleportation" l'informazione quantistica non viene trasmessa "fisicamente" sui mezzi trasmissivi, ma veicolata attraverso l'entanglement. Per ogni comunicazione origine – destinazione si stabilisce una corrispondente relazione end-to-end di entanglement. L'entanglement viene realizzato utilizzando fotoni, su cui i nodi effettuano operazioni (creazione, trasmissione, ricezione, interazione reciproca, misura) finalizzate a renderlo disponibile come funzionalità e risorsa in rete per il trasporto delle informazioni quantistiche. I fotoni utilizzati per instaurare l'entanglement sono trasmessi sui mezzi trasmissivi, subendone quindi attenuazione e rumore. Una volta stabilita, la connessione end-to-end di entanglement costituirà il substrato su cui l'informazione quantistica verrà trasportata senza interazione "fisica" con i mezzi trasmissivi.
Con la "Quantum Teleportation", i limiti di massima distanza trasmissiva anziché interessare direttamente l'informazione quantistica, intervengono sui fotoni impiegati per realizzare l'entanglement.
Per estendere l'entanglement su lunghe distanze, si stanno studiando soluzioni di suddivisione in tratte più brevi, criterio analogo all'impiego dei "Trusted Node" visti in precedenza. Più nello specifico, gli spezzoni di entanglement delle tratte brevi vengono raccordati iterativamente prolungando progressivamente l'entanglement fino a comporre l'intero cammino tra origine e destinazione. La giunzione tra i segmenti di entanglement di due tratte contigue avviene attraverso un'operazione di entanglement swapping. Questa funzionalità sarà implementata sui futuri "Quantum Repeater", che costituiranno i nodi di sezionamenti e consentirà l'estensione a livello geografico della Quantum Internet. In questo modo l'informazione quantistica verrà trasferita end-to-end senza effettuare le operazioni di decodifica e ricodifica in ogni "Quantum Repeater", come se fosse un livello protocollare superiore all'entanglement. La tecnologia dei "Quantum Repeater" è ancora una tecnologia in fase di ricerca.

Applicazioni

Alcune peculiarità della meccanica quantistica sono già state evidenziate lasciando intravvedere come le loro proprietà possano essere sfruttate per arricchire e migliorare gli attuali servizi o crearne di nuovi.
Diverse applicazioni della futura Quantum Internet sono già in fase di studio e, focalizzandosi al settore delle telecomunicazioni, possono essere classificate secondo alcune macrocategorie [5]:

a) Secured communication
Gli attuali sistemi di protezione delle comunicazioni e dei dati utilizzano protocolli crittografici, la cui robustezza deriva dalla difficoltà di risoluzione del problema matematico, che costituisce l'algoritmo alla base del loro funzionamento: tra questi si può citare il problema della fattorizzazione dei numeri interi e il problema logaritmico discreto a curve ellittiche. Si tratta dei cosiddetti sistemi di cifratura a chiave pubblica, che un computer quantistico, utilizzando l'algoritmo di Shor (1994), può risolvere in tempi esponenzialmente più veloci se confrontati anche con quelli del più potente, ad oggi, supercomputer classico.
La soluzione ad eventuali attacchi da parte di hackers, consiste nello sviluppare nuovi sistemi di protezione, che, a seconda della strategia che perseguono, possono essere suddivisi in due aree:
Quantum cryptography: le comunicazioni classiche sono rese "sicure" utilizzando chiavi di cifratura scambiate tra sorgente e destinazione attraverso un canale quantistico parallelo. Sfruttando opportunamente i principi della meccanica quantistica, i tentativi di intercettazione delle chiavi possono essere rilevati e di conseguenza viene interrotto il loro scambio fino al ripristino delle condizioni di sicurezza. L'applicazione più conosciuta e consolidata di quantum cryptography è la quantum key distribution (QKD) per trasmissione delle chiave crittografiche, generate in forma totalmente casuale tramite quantum random number generator (QRNG).
Post-quantum cryptography: termine col quale ci si riferisce a sistemi di cifratura che si basano su algoritmi "sicuri" rispetto ad attacchi da parte di computer quantistici. Proprio per questo si usa anche parlare di classical post-quantum cryptography.

Nella stessa categoria delle secured communication ricadono anche il secured identification e position verification, applicazioni per autenticare i soggetti partecipanti di una comunicazione.

b) Fast coordination/negotiation
Le funzionalità della Quantum Internet possono essere utili nei problemi che richiedono il coordinamento dell'azione di una flotta di entità (e.g. computer, robots...) o l'elezione di un loro leader, per evitare interferenze nel processo decisionale e convergere rapidamente verso una posizione condivisa.

c) Clock timing and synchronization
La quantum clock synchronization è un'altra area di applicazione per aumentare l'accuratezza delle applicazioni che si basano sulla sincronizzazione del timing su oggetti distribuiti (per esempio GPS...)

d) Distributed quantum computing
Per salvaguardare lo stato di superposition, necessario per l'elaborazione "parallela", i qubit devono essere mantenuti in un ambiente protetto (possibilmente isolati e ad una temperatura prossima allo 0 assoluto). Garantire questa condizione, allo stato attuale della tecnologia, risulta più difficile al crescere del numero di qubit equipaggiati; questo limita il trend di espansione della potenza di calcolo dei computer quantistici.
Se questa difficoltà dovesse persistere in futuro, una delle prime applicazioni della Quantum Internet potrebbe essere il distributed quantum computing. Così facendo, si costituirebbero cluster di computer quantistici, la cui potenza di calcolo complessiva sarebbe superiore a quella delle singole macchine: la potenza di calcolo dei cluster scalerebbe in funzione del numero di computer quantistici "fisici" che la quantum internet sarebbe in grado di interconnettere. [1]

e) Secure quantum computing with privacy protection
Quest'area di applicazione si riferisce ai servizi di quantum computing in cloud in cui si mantiene la riservatezza dei dati sorgente (private/blind comoputing) per salvaguardare la natura dell'elaborazione e/o la privacy delle informazioni.

Tutte le potenzialità della Quantum Internet saranno totalmente sfruttabili
Tutte le potenzialità della Quantum Internet saranno totalmente sfruttabili una volta che si raggiungerà il pieno sviluppo delle sue funzionalità ed in particolare l'entanglement sarà disponibile a livello globale e massivo in un contesto commerciale.
Nel frattempo le prime applicazioni si riescono già a realizzare in un contesto di produzione per offrire servizi commerciali. Tra queste rientrano la QKD e la QRNG così come alcuni use case che, in continuità con quanto illustrato finora, verranno descritti nel dettaglio nell'articolo successivo di questo stesso Notiziario ("Quantum Communication in pratica: tecnologie e applicazioni") ■

Bibliografia

1. [1] Cacciapuoti, A. S., Caleffi, M., Cataliotti, F. S., Gherardini, S., Tafuri, F., & Bianchi, G. (s.d.). Tratto da Arxiv: https://arxiv.org/pdf/1810.08421.pdf
2. [2] Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S., & Bianchi, G. (s.d.). Tratto da http://www.quantuminternet.it/files/pub/TechPaper.pdf
3. [3] Dirkse, B. (2019, 10 22). Tratto da https://blog.qutech.nl/index.php/2019/10/22/quantum-internet-at-the-verge-of-an-emerging-technology/#more-1230
4. [4] Kozlowski, W., Wehner, S., Van Meter, R., & Rijsman, B. (s.d.). Tratto da https://github.com/Wojtek242/draft-irtf-qirg-principles/blob/master/draft-irtf-qirg-principles-03.txt
5. [5] Vermaas, P., Nas, D., Vandersypen, L., Coronas, D. E., Asveld, L., Cramer, J., et al. (2019, June). Tratto da https://qutech.nl/quantum-internet-magazine/

Andrea Boella *andrea.boella@telecomitalia.it*

Ingegnere elettronico, è in Telecom Italia dal 1997, dove è entrato nella ex direzione territoriale del Piemonte e Valle d'Aosta iniziando con la pianificazione della rete di trasporto regionale, per passare in qualità di responsabile prima al supporto specialistico trasmissioni e successivamente al secondo livello di assistenza tecnica per la clientela enterprise. Dal 2003 al 2005, come espatriato, è stato responsabile del settore esercizio in Telecom Italia France e al ritorno in Italia entra a far parte del gruppo ex Global Network coordinando, come project manager, attività di supporto verso le partecipate estere inizialmente su tematiche di rete fissa e a partire dal 2008 sulla core network di rete mobile. Da fine 2018 lavora nel gruppo di Service Innovation con attività di ricerca su servizi per l'IOT, blockchain, quantum computing e quantum communication ■

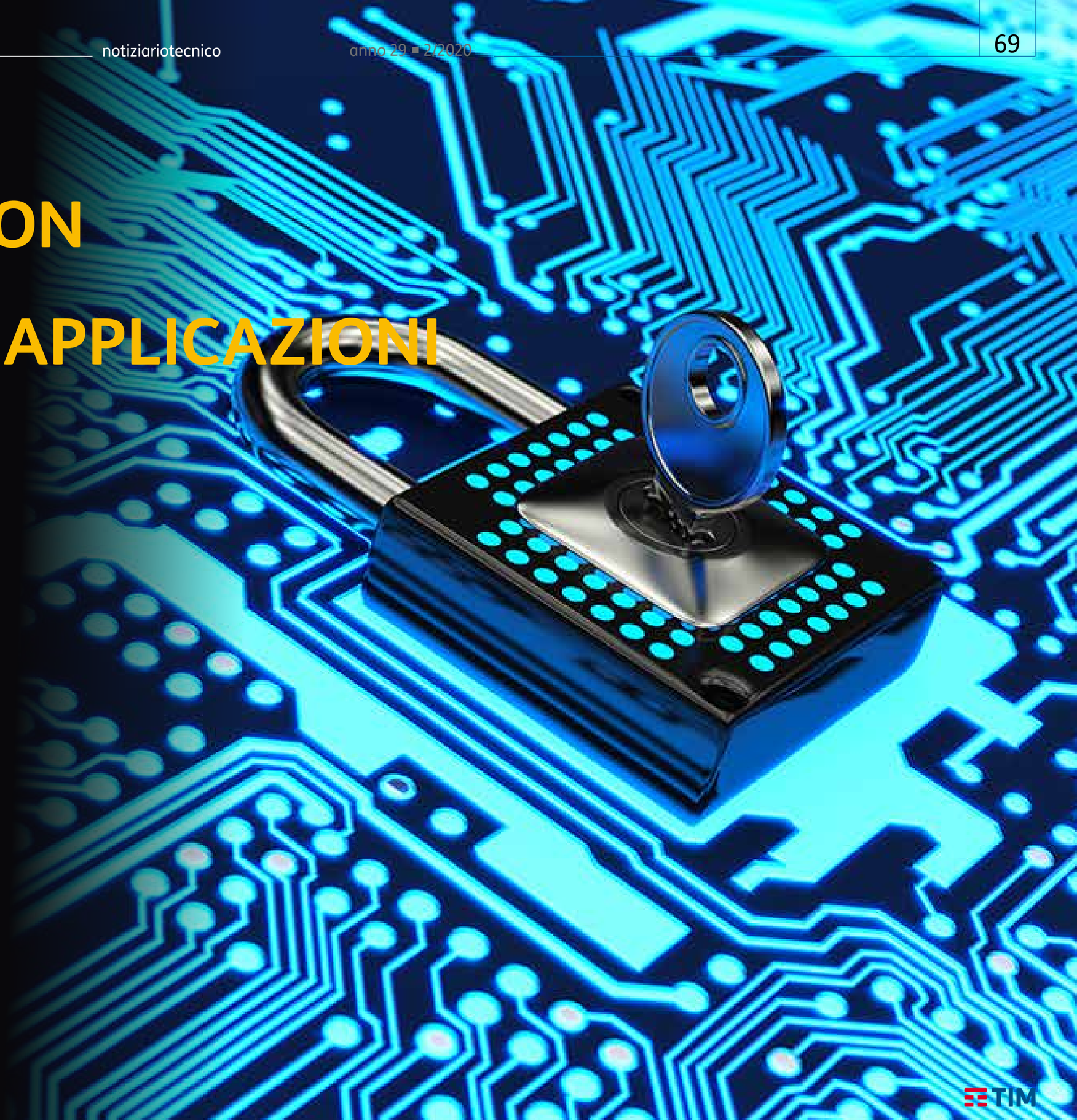
Mauro Alberto Rossotto *mauro.rossotto@telecomitalia.it*

Laureato all'Università di Torino in Informatica con specializzazione Intelligenza Artificiale. Entrato in Telecom Italia nel 1995 ha partecipato a diversi progetti realizzativi legati a Data Mining Lab, analisi dati a scopo Antifrode e Marketing, Push-to-talk, Smart Inclusion. Dal 2012, in Innovation, ha seguito in qualità di responsabile di struttura le attività legate allo sviluppo di servizi innovativi su device connessi, a partire da TIM Vision e TIM Cloud su Smart TV e Game Console. Nel 2014 in Strategy & Innovation sono iniziate le prime attività sul mondo IoT, ed in particolare sui verticali Smart Home, Wellness, Smart City, Smart Retail, Energy e Industry affrontando tutti gli aspetti tecnologici del servizio. Oggi in Service Innovation è responsabile del Program "Internet of Everything" dove vengono seguite tematiche relative a Droni, Robotics, IoT, Blockchain e Quantum Technologies con attività di scouting, prototipazione, sperimentazione e pipeline verso ingegneria ■

QUANTUM COMMUNICATION IN PRATICA: TECNOLOGIE E APPLICAZIONI

Sabrina Guerra, Maurizio Valvo

Negli ultimi anni la meccanica quantistica e' uscita dal ristretto ambito della fisica teorica per conquistarsi uno spazio in campo tecnologico e applicativo. Le comunicazioni quantistiche sono uno dei settori piu' interessanti e promettenti delle tecnologie quantistiche su cui si stanno concentrando esperimenti ed investimenti rilevanti in tutto il mondo. Le innovazioni che la Quantum Internet apporterà e le opportunità di business che ne deriveranno hanno promosso un'intensa attività di ricerca e ci si aspetta che in un futuro non troppo lontano la quantum internet possa uscire dagli ambienti di laboratorio e diventare realtà, affiancandosi e integrandosi alla internet "classica". Fra i servizi di comunicazione quantistica, un posto di riguardo spetta sicuramente alla quantum key distribution (QKD), di cui esistono svariate installazioni, non solo in laboratorio, ma anche su rete live per applicazioni commerciali o pseudo tali relative a use case di interesse per la sicurezza dei dati. La tecnologia dei quantum random number generator (QRNG) garantisce invece la generazione di numeri realmente casuali per svariate applicazioni (crittografia, lotterie, ...). Nel presente articolo verrà presentata una panoramica delle tecnologie abilitanti e degli use case piu' interessanti per gli operatori di TLC.



Quantum Key distribution

Contesto tecnologico e storico di riferimento

La robustezza dei sistemi di crittografia attuali e' basata essenzialmente sui lunghi tempi di calcolo necessari a decodificare le chiavi crittografiche. In linea di principio le informazioni crittate possono essere registrate e decodificate successivamente, il che puo' essere sufficiente p.es. per i numeri delle carte di credito che ogni 2-3 anni vengono cambiate, ma questo puo' essere piu' critico per chiavi che devono essere memorizzate per oltre un decennio.

Nel 1977, Ronald Rivest, Adi Shamir e Leonard Adleman, inventori dell'algoritmo di crittografia asimmetrica che prese il nome dalle loro iniziali (RSA), lanciarono una sfida pubblica: la sfida consisteva nel "craccare" un testo cifrato con un codice di 428 bit. RSA predissero che, con il piu' potente computer disponibile a quei tempi, sarebbero stati necessari 40 quadrillioni (4*10E16) di anni per craccare il codice [1].

Tuttavia, il premio di 100$ venne poi vinto nel 1994 da un gruppo di scienziati che utilizzarono tecniche di calcolo parallelo su internet! La soluzione risultante "The magic words are squeamish ossifrage" (Le parole magiche sono schizzinoso avvoltoio) sono entrate nella storia della crittografia.

Successivamente, nel 2015 la NSA (National Security Agency) emise un annuncio che metteva in risalto il fatto che i computer quantistici potrebbero essere una seria minaccia agli attuali sistemi crittografici [2]. Questo annuncio, rilasciato da un autorevole ente per la sicurezza, ha fatto da ulteriore booster per la promozione della ricerca nel campo della crittografia quantistica.

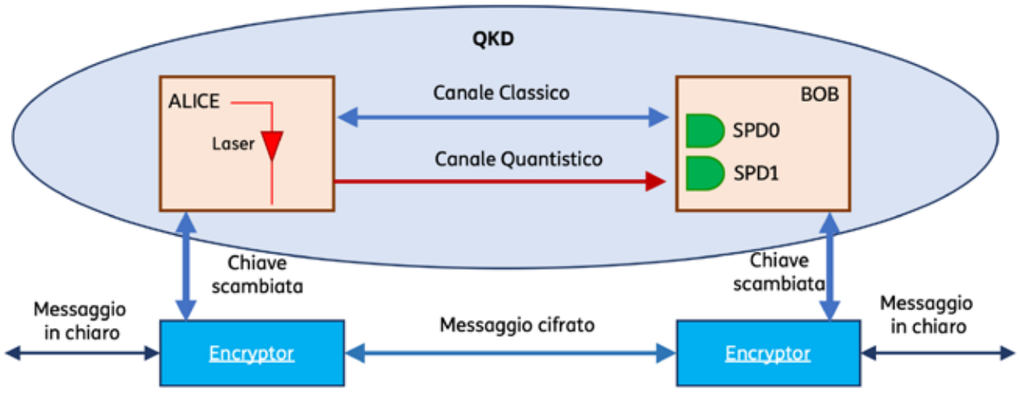
Principi alla base della Quantum Key distribution

Un segnale cifrato inviato su un canale pubblico e' potenzialmente vulnerabile ad essere intercettato e successivamente decodificato (o craccato). A tutt'oggi infatti non esiste alcuna prova matematica che garantisca la sicurezza assoluta dei sistemi crittografici attualmente in uso: la sicurezza di una chiave crittografica e' dunque riposta nel tempo richiesto alla sua crittazione. Per questo e' necessario che le chiavi crittografiche vengano periodicamente rinnovate [3].

In ogni sistema crittografico fra utenti remoti, infatti, uno degli aspetti piu' critici e' lo scambio sicuro delle chiavi crittografiche; in un sistema crittografico "tradizionale", l'invio e lo scambio delle chiavi avviene tramite un sistema potenzialmente insicuro. Con la QKD lo scenario cambia drasticamente in quanto le chiavi possono essere scambiate in modo intrinsecamente sicuro, o meglio, gli utenti finali che si scambiano le chiavi sono in grado di capire se le chiavi sono state intercettate.
Nel caso in cui si scopra che le chiavi sono state intercettate durante la trasmissione e' possibile ritrasmetterle fino a raggiungere la sicurezza che nessun soggetto non autorizzato ne sia entrato in possesso. La QKD si basa su alcuni principi fondamentali della meccanica quantistica, in particolare sul principio di indeterminazione di Heisenberg e sul non-cloning theorem.

Implementazione della Quantum Key distribution

La meccanica quantistica, nata all'inizio del XX secolo, si è affermata come la teoria fondamentale che descrive la fisica delle nanoparticelle e di conseguenza i settori che ne fanno uso (dall'elettronica come nei transistor alle molecole e biomateriali). Nel XX secolo è emerso un altro settore in rapido sviluppo: la tecnologia dell'informazione e della comunicazione (ICT). Di recente, molta attenzione è stata attratta da un nuovo campo di ricerca, la tecnologia dell'informazione e della comunicazione quantistica (QICT),



1
Schema di principio della QKD

che si basa su questi due campi apparentemente poco correlati.

QICT fornisce una comprensione più approfondita della meccanica quantistica attraverso nuovi approcci per la verifica dei suoi principi, nonché funzionalità completamente nuove che non possono essere realizzate dalle ICT "classiche", ad esempio, consentendoci di risolvere problemi estremamente difficili in breve tempo utilizzando i computer quantistici e di avere una comunicazione completamente sicura mediante distribuzione quantistica delle chiavi e certificazione quantistica.
Tra le particelle o fenomeni quantistici utilizzabili nelle QICT, il fotone e' uno dei candidati piu' interessanti, in quanto gia' ampiamente utilizzato nelle comunicazioni in fibra ottica. Mediante proprietà quantistiche legate al fotone (polarizzazione o fase) e' possibile realizzare una distribuzione quantistica delle chiavi (QKD), tecnica che consente la condivisione di chiavi segrete tra due parti remote attraverso l'invio di fotoni con informazioni codificate su di essi.

La caratteristica significativa di questa tecnologia è che i tentativi di intercettazione possono essere rilevati, cosa invece non possibile nelle comunicazioni convenzionali.
Il rischio che i dati digitali scambiati su Internet vengano rubati o intercettati non può essere ridotto a zero e per proteggersi da questi rischi, per esempio quando si inviano password o numeri di carta di credito, si utilizza la crittografia.

Ampiamente usato è il sistema crittografico a chiave pubblica: la sua sicurezza si basa su alcuni difficili problemi matematici. Pertanto, la forza della sua sicurezza dipende dallo dalle prestazioni del computer e dagli algoritmi matematici. Al contrario, il sistema di crittografia tipo OTP (0ne-Time-Pad) è da tempo noto per essere inviolabile, ma le due parti (un mittente chiamato convenzionalmente Alice e un destinatario chiamato Bob) devono condividere chiavi segrete completamente casuali, delle stesse dimensioni del messaggio da inviare e utilizzate una volta sola. QKD può fornire un metodo per distribuire tali chiavi in modo sicuro. Il principio di base di QKD è illustrato nella Fig.1.
Alice prepara un lungo array di bit casuali fatto di 0 e 1 e codifica que-

ste informazioni binarie nello stato di polarizzazione di fotoni, che vengono inviati a Bob attraverso un canale quantico (ad esempio una fibra ottica). Bob ottiene una matrice logica di stati (bit) misurando ogni fotone. Fino a questo punto, lo schema di comunicazione non e' differente dalle comunicazioni classiche, ma la differenza diventa evidente quando un intercettatore (convenzionalmente chiamato Eve, da evesdropper) cerca di intercettare la chiavi scambiate.

Nella comunicazione classica, infatti, l'informazione può essere rubata spillando (leggendo) una parte del segnale. Al contrario, le informazioni quantistiche codificate su una particella elementare o un fotone, non possono più essere divise: le uniche scelte sono prendere tutto o lasciare tutto. I dati intercettati alterano l'informazione (le chiavi) trasmesse e quindi è come se venissero persi; i rimanenti bit casuali possono essere utilizzati come chiave segreta se in seguito Bob ed Alice concordano i sottoinsiemi di bit, all'interno della sequenza trasmessa, che non sono stati intercettati. Un intercettatore intelligente potrebbe inviare fotoni falsi che dipendono dai risultati dei fotoni che è riuscito a misurare ("rubati").

Tuttavia, non è possibile misurare uno stato quantico di un fotone senza modificarlo, introducendo inevitabilmente errori nei bit misurati da Bob. Il non-cloning theorem della meccanica quantistica proibisce all' intercettatore di fare una copia di un fotone non misurato e pertanto ignoto. L'ascoltatore quindi non può ottenere le informazioni chiave senza indurre errori di bit. In altre parole, Alice e Bob possono riconoscere la presenza di un intercettatore controllando gli errori di bit.

Nel primo protocollo QKD proposto nel 1984, chiamato BB84 dai proponenti CH Bennett e G. Brassard, Alice assegna i bit logici 0 e 1 a uno stato di polarizzazione di un fotone usando due insiemi (basi) scelti a caso, vale a dire polarizzazioni circolari (orario o antiorario) o polarizzazioni lineari (orizzontale e verticale). Bob misura il fotone dopo aver scelto la base di misurazione in modo casuale, ma ottiene il risultato corretto solo se ha scelto la stessa base di Alice. Pertanto, dopo la trasmissione dei fotoni, Alice e Bob si scambiano informazioni sulle loro basi e selezionano i bit che sono stati codificati da Alice e misurati da Bob nella stessa base. Confrontano anche parte della chiave "setacciata" (sifted) ottenuta per verificare il tasso di errore.

Se il tasso di errore è inferiore a un determinato valore di soglia, possono concludere che non è presente alcun intercettatore. Infine, viene generata una chiave sicura con il post-processing — correzione degli errori e amplificazione della privacy — per ridurre le informazioni di cui potrebbe entrare in possesso un intercettatore. Le fibre ottiche finora sono state il canale fisico piu' utilizzato per le trasmissioni ottiche e quindi dei fotoni, ma non mancano anche le applicazioni di tipo FSO (Free Space Optics) o satellitare, di cui il caso piu' noto e' il satellite cinese Micius [4].

Attuali limiti della QKD

Va sottolineato che l'uso della QKD non risolve il problema della sicurezza intrinseca delle chiavi, non garantisce cioe' che le chiavi scambiate con la QKD siano robuste ai tentativi di decifratura: la QKD garantisce unicamente la sicurezza delle chiavi durante lo scambio delle medesime. Le chiavi eventualmente intercettate successivamente alla procedura di scambio sono soggette agli stessi rischi di sicurezza delle chiavi scambiate in modalita' classica. Un'altra grande sfida e' l'uso massiccio della QKD in applicazioni quali IoT, big data, cloud, ecc. per i cui utilizzi massivi è necessario che il mercato della QKD si orienti verso costi inferiori rispetto a quelli attuali.
Altro aspetto importante è che i protocolli BB84 e simili sono protocolli concepiti per lo scambio di chiavi point-to-point e le architetture tipo point-to-multipoint devono ancora essere esplorate.

Va anche detto che sono stati proposti e dimostrati un certo numero di possibili attacchi di tipo Denial of Service (DoS) dei sistemi DKD; pertanto la sua vulnerabilita' è ancora oggetto di studio.

Le prestazioni della QKD sono piuttosto limitate in bit-rate e distanza: i dispositivi oggi utilizzati negli esperimenti in campo consentono di coprire distanze di un centinaio di chilometri circa e bit-rate fra le decine e le centinaia di Mbit/s, con un trade-off fra bit-rate e distanza (con un record di 250 km, ma limitato a 16 bit/s) [5]
Ci si aspetta che gli attuali limiti di distanza potranno essere superati in futuro con l'uso dell'entanglement.

Prospettive di sviluppo futuro della QKD

Dati gli attuali limiti tecnologici, le prospettive di sviluppo nell'uso della QKD sono nella direzione della ricerca nel miglioramento delle caratteristiche di rumore di sorgenti e rivelatori sorgenti. Oltre all'uso nelle comunicazioni in fibra ottica, si puo' anche ipotizzare un uso piu' diffuso nelle soluzioni di tipo FSO, dove il canale in aria e' sicuramente piu' vulnerabile a tentativi di intercettazione.

Ma la spinta maggiore ad un utilizzo diffusivo della QKD verra' sicuramente dall'integrazione di tutti i componenti costituenti un trasmettitore o un ricevitore in un unico modulo integrato, verso la realizzazione di un gateway QKD.

La realizzazione di gateway QKD leggeri, compatti ed economici, potra' spingere l'utilizzo della QKD in reti a basso costo e in ambiti dove leggerezza e compattezza sono di importanza prioritaria (p.es. a bordo di droni).

Mercato della QKD - Principali fornitori

La QKD viene gia' considerata sufficientemente matura dal punto di vista tecnologico da stimolare gli interessi di parecchie aziende e soprattutto la nascita di startup che hanno sviluppati prodotti ad hoc.

A tutt'oggi, ufficialmente 4 aziende sono in grado di offrire prodotti chiavi in mano per la QKD [6]: ID Quantique (Svizzera), MagiQ Technologies (USA), Quintessence Labs (Australia) e SeQureNet (Francia).La capostipite di queste e' sicuramente la svizzera ID Quantique [7], nata come spinoff dall'Universita' di Ginevra, che opera nel campo da oltre 10 anni e che ha a catalogo una serie di prodotti specifici, da generatori quantistici di numeri casuali (QRNG) a piattaforme QKD vere a proprie basate sul protocollo BB84 o COW. ID Quantique produce anche soluzioni per photon counting e quantum sensing.

Toshiba Research Europe e' un'altra azienda che ha a catalogo delle piattaforme per la QKD [8]. Allo stato attuale (inizio 2020) la maturita' commerciale di queste piattaforme non e' ancora del tutto chiara.

Vi sono anche produttori di apparati di TLC che integrano nei loro prodotti piattaforme QKD di terze parti. Ad esempio, ADVA, che utilizza prodotti ID Quantique nella piattaforma WDM FSP 3000 [9]. Anche in questo caso, l'effettiva disponibilita' commerciale di questa soluzione e' da provare.

Fra le startup italiane attive nel settore, si puo' ricordare la Micro Photon Devices (MPD), di Bolzano [10], che produce rivelatori single-photon counting.

Principali iniziative di applicazione della QKD

Negli ultimi anni la QKD e' uscita dall'ambito della sperimentazione di laboratorio e innumerevoli sono gli esperimenti effettuati in campo su fibre ottiche posate. Fra gli esperimenti piu' interessanti, si puo' ricordare il trial fra le Universita' di York e di Cambridge in UK [11] (vedere paragrafo use cases).

In Giappone, nel 2010 e' stata inaugurata una rete denominata Tokyo QKD Network, che coinvolge una

quantita' di enti fra cui NICT, NEC, Mitsubishi Electric, NTT, Toshiba Research Europe, the Austrian Institute of Technology ed altri enti di ricerca [12]. La rete si estende su un anello di oltre 90 km e lo scambio di chiavi avviene a circa 400 bps.

In Italia, si possono ricordare un trial effettuato nell'area metropolitana di Firenze, con il laboratorio LENS (European Laboratory for Non-Linear Spectroscopy) utilizzato come end-point per i soggetti Alice e Bob e un datacenter come punto intermedio. Lo scambio delle chiavi e' stato effettuato a vari bit-rate intorno a 3.4 kbit/s [13].

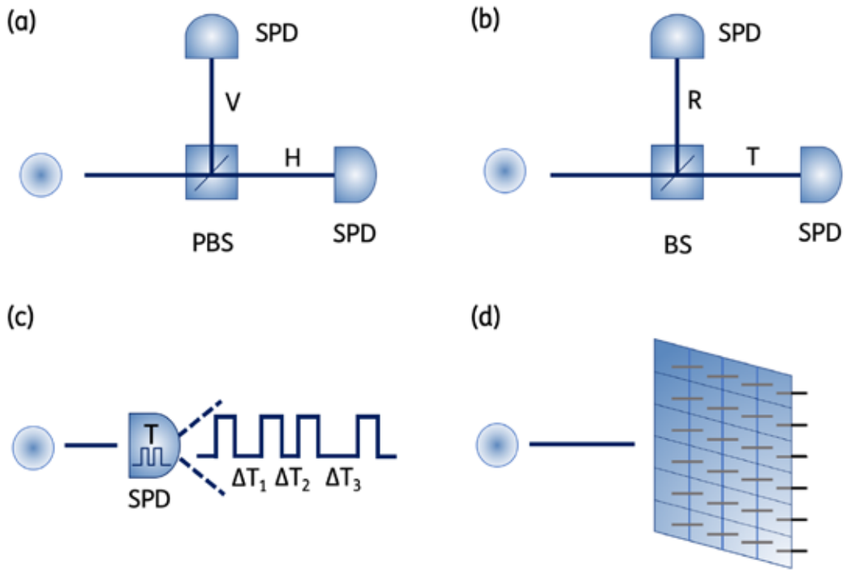
Un altro esperimento di rilievo e' stato effettuato su 96 km di cavo in fibra sottomarino fra Malta e la Sicilia. La rilevanza di questo esperimento e' data dal fatto che e' stato dimostrato l'entanglement quantistico in uno scenario in campo e non solo in laboratorio [14].

Quantum Random Number Generators

In diversi campi della scienza, della tecnica e anche della vita quotidiana (simulazioni e test scientifici, crittografia, giochi, lotterie e concorsi a premi, ecc.) è richiesta la generazione di numeri casuali, il cui requisito fondamentale è la non predicibilità.

Questo requisito non può essere garantito con assoluta certezza utilizzando metodi classici, basati per esempio su algoritmi di calcolo deterministici (generatori software o hardware di numeri pseudocasuali), per quanto si possano utilizzare tecniche di aumento dell'entropia (p.es. sfruttando gli istanti di tempo in cui accadono determinati eventi, i movimenti del mouse di un utente al computer, ecc. per generare il seme da introdurre nel generatore di numeri pseudocasuali).

2
principio di funzionamento di un QRNG fotonico basato su: a) polarizzazione del fotone; b) riflessione/ trasmissione del fotone attraverso una superficie semi-riflettente; c) tempo di interarrivo dei fotoni; d) rivelazione della posizione del fotone tramite matrice di rivelatori (fonte: [25])



La parvenza di casualità di questi metodi è in realtà basata su una elevata complessità che rende difficile, sebbene non impossibile, una predizione.
Anche per i generatori fisici di numeri casuali, basati su fenomeni fisici caotici (p.es. la corrente di rumore di un resistore o di un diodo), non è possibile garantire che non siano soggetti a interazioni con l'ambiente che potrebbero inficiare la qualità del risultato.

Tra i pochi fenomeni fisici in cui è garantita l'assoluta casualità ci sono quelli descritti dalla fisica quantistica, grazie alla natura inerentemente statistica del comportamento delle particelle subatomiche.
Su questi fenomeni si basa lo sviluppo dei generatori quantistici di numeri casuali (Quantum Random Number Generators – QRNGs), costituiti da una sorgente casuale e da un rivelatore, le cui tipologie dipendono dal fenomeno fisico quantistico che si intende sfruttare. Molti generatori odierni si basano su sistemi fotonici perché realizzabili con relativa semplicità, a basso costo e con dimensioni che ne permettono l'inserimento in dispositivi pratici.

Questi dispositivi sono anche facilmente modellabili e consentono di verificarne il corretto funzionamento. La sorgente è costituita tipicamente da un diodo LED o laser; a seconda della tipologia di QRNG, i fotoni emessi attraversano un dispositivo separatore di polarizzazione o una superficie semiriflettente; sui due rami di uscita sono posti dei rivelatori a singolo fotone [Fig.2, a) e b)].
Con eguale probabilità, ogni fotone emesso dalla sorgente può essere rilevato da uno dei due rivelatori (ovvero essere caratterizzato da uno dei due stati di polarizzazione o venire riflesso oppure trasmesso) e la sequenza di detezioni osservate gode della proprietà di perfetta casualità per il processo quantistico che ne è alla base.

Altre tecniche, che permettono di raggiungere frequenze di generazione più elevate, si basano sul tempo di interarrivo dei fotoni [Fig.2, c)] oppure sul punto di arrivo all'interno di una superficie costituita da un insieme di rivelatori a singolo fotone [Fig.2, d)] oppure ancora sul numero di fotoni ricevuti. Altre ancora, basate sul rumore di fase di laser o amplificatori ottici, consentono di utilizzare fotorivelatori comuni (cioè non a singolo fotone) e di raggiungere frequenze di generazione molto più elevate (fino a 68Gbps negli esperimenti più recenti [26]).

Nella pratica, i dispositivi sorgente e rivelatore sono imperfetti (cioè si discostano dal modello teorico) e introducono rumore dipendente da variabili classiche; ciò può inficiare, o essere utilizzato malevolmente per inficiare la perfetta casualità del risultato, introducendo una polarizzazione (ovvero riducendo l'entropia). Tale effetto può essere rimosso, quindi l'entropia può essere massimizzata, tramite metodi di randomness extraction se è noto un modello teorico sufficientemente accurato dei dispositivi.
In alternativa, esistono realizzazioni di QRNG self-testing, che sono in grado di garantire la perfetta casualità dei numeri generati indipendentemente dai dispositivi utilizzati sfruttando protocolli basati su test di disuguaglianza tra quantità facilmente calcolabili (ovvero misurando l'entropia) e applicando tecniche di massimizzazione dell'entropia; purtroppo queste tecniche riducono la frequenza di generazione a valori estremamente bassi, praticamente inutilizzabili.
Una via di mezzo è costituita dalle soluzioni semi self-testing, in cui è noto con sufficiente accuratezza il modello di uno solo dei due dispositivi (sorgente o rivelatore), che consentono di raggiungere frequenze di generazione sufficienti per molte applicazioni pratiche.
Un esempio di dispositivo QRNG commerciale (Quantis), basato sul principio della riflessione o trasmissione di fotoni attraverso una superficie semi-riflettente e in grado di generare bit casuali a una frequenza di 4-16Mbit/s, è prodotto dall'azienda svizzera IDQuantique [Fig.3], [28].

Overview sulle attività degli enti di standardizzazione, mercato e investimenti sulla Quantum Communication

La vulnerabilità del QKD con tecniche di Injection Locking

Le comunicazioni quantistiche sembrano promettere modalità perfettamente sicure (e.g., attraverso QKD) di trasmissione e scambio di informazioni e dati. Recenti studi e sperimentazioni, in realtà, dimostrano la possibile vulnerabilità anche dei sistemi QKD.

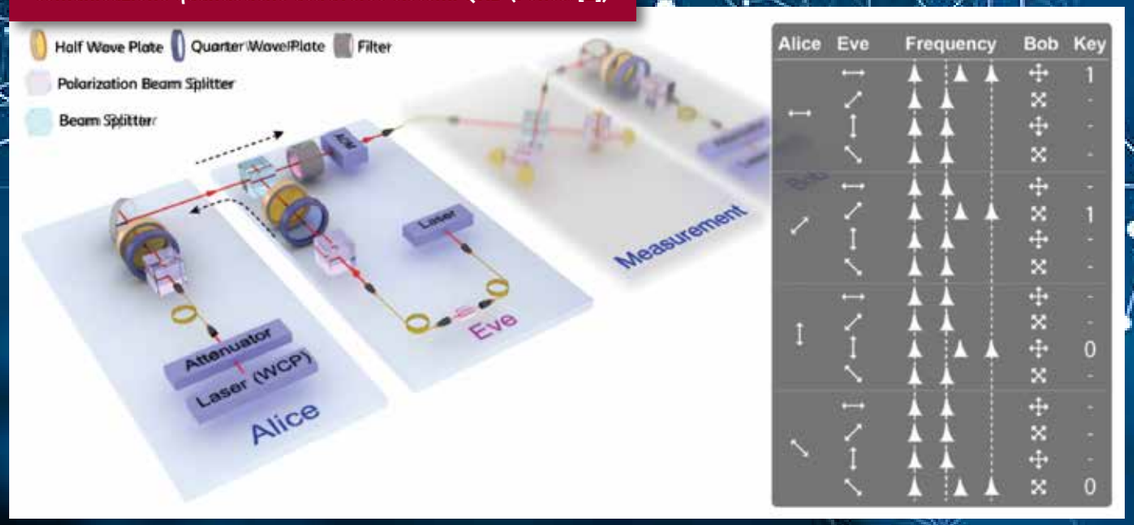
Questo è quanto riportato in [1], [2], dove si illustra l'utilizzo di tecniche di Injection Locking per lo sviluppo di strategie di hacking di comunicazione quantistiche attraverso sistemi QKD.

Si ricorda che il fenomeno di Injection Locking si verifica quando un oscillatore armonico subisce l'interferenza di un secondo oscillatore operante ad una frequenza sufficientemente vicina. In particolare, quando l'accoppiamento tra i due oscillatori è abbastanza forte e le frequenze relativamente vicine, il secondo oscillatore può catturare il primo oscillatore, portandolo ad oscillare ad una frequenza sostanzialmente identica alla seconda.

Nello studio e sperimentazione presentato in [2] è stato sviluppato un sistema (vedi figura A) dove Eve (un possibile hacker che inserisce nella comunicazione tra Alice e Bob) utilizza una tecnica di Injection Locking per forzare il laser di Alice a produrre quei fotoni che hanno lo stesso stato di polarizzazione di quelli iniettati da Eve alla stessa frequenza del laser di Eve. I successivi passi di filtraggio e riconversione di frequenza e il monitoraggio della fase di post-selezione (protocollo BB84), consentono a Eve di ricostruire la chiave crittografica con buona probabilità di successo, all'insaputa di Bob e Alice.

Nella sperimentazione l'utilizzo di un laser a semiconduttore (distante in frequenza 251 MHz da quello di Alice) ha permesso di ottenere una percentuale di successo nell'operazione di hacking del 60%, con un tasso di errore del 6% circa per livelli di potenza dei 110 nW, nonostante l'impiego di un isolatore (che idealmente blocca i segnali in ingresso) sul laser di Alice.

A
Utilizzo di tecniche di Injection Locking per hacking di comunicazione quantistiche attraverso sistemi QKD (Fonte: [2])



Riferimenti

[1] MIT – Technical Review "There's a new way to break quantum cryptography" https://www.technologyreview.com/2019/03/06/136765/theres-a-new-way-to-break-quantum-cryptography/

[2] Pang, X. L., Yang, A. L., Zhang, C. N., Dou, J. P., Li, H., Gao, J., & Jin, X. M. (2020). "x". Physical Review Applied, 13(3), 034008

antonio.manzalini@telecomitalia.it

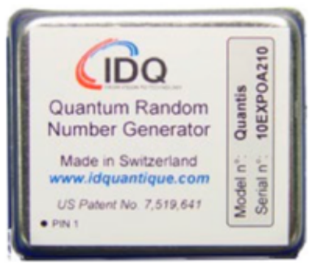
Da qualche tempo anche i principali enti di standardizzazione hanno cominciato ad occuparsi concretamente di QKD.
Ad esempio, l'ETSI (European Telecommunication Standard Institute), che gia' nel 2010 pubblico' un documento che identifica e definisce i principali use case [15].

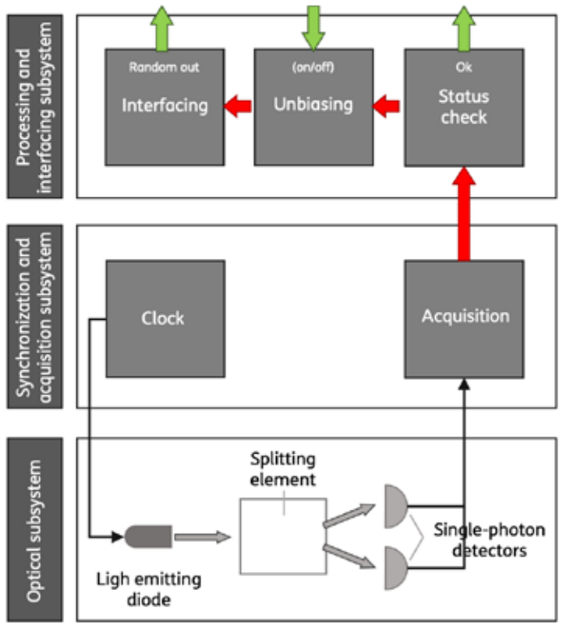
Successivamente, ETSI ha pubblicato altre specifiche relative a vari aspetti della QKD, fra cui Application Interfaces, Module Security Specification, Components, etc. [16].
Successivamente anche ITU-T ha iniziato ad occuparsi di QKD nell'ambito dello Study Group 13, che ha per mandato la standardizzazione delle reti di prossima generazione e l'evoluzione della NGN (Next Generation Network): nel giugno 2019 ITU-T ha pubblicato la prima raccomandazione sulle tecnologie quantistiche, la Y.3800 ("Framework for Networks supporting Quantum Key Distribution"), mentre attualmente (gennaio 2020) altre raccomandazioni sono allo stato di draft, fra cui: Y.QKDN_KM ("key management") e Y.QKDN_Arch. ("Functional Architectures") [17-18] .

Successivamente, nel settembre 2019 ITU-T ha istituito un Focus Group specificamente dedicato alle tecnologie quantistiche: FG-QIT4N [19]
Fra gli altri enti di standardizzazione attivi in questo settore si possono ricordare l'IETF (Internet Engineering Task Force), che ha istituito un Research Group su Quantum Internet [20], il NIST (National Institute of Standard and Technology) [21] e ISO (International Organization for Standardization) [22].

Le tecnologie quantistiche sono considerate come uno dei settori piu' promettenti delle tecnologie innovative per i prossimi anni e stanno raccogliendo investimenti rilevanti.
Nel 2018 l'Unione Europea ha lanciato lo European Quantum Flagship [23], un ambizioso programma articolato su 10 anni per il finanziamento di un gran numero di progetti di ricerca su aree:

3
il componente "Quantis" di IDQuantique e la sua architettura interna (fonte: [28])





1) Quantum Communication,
2) Quantum Simulation,
3) Quantum Computing,
4) Quantum Metrology & Sensing.
Il budget complessivo del progetto e' di 1 miliardo di €.

Tra i progetti più rilevanti del Quantum Flagship si può annoverare l'OPENQKD, un progetto che vede la partecipazione di enti europei appartenenti a vari settori (fornitori di soluzioni per le telecomunicazioni, telco operators, fornitori di soluzioni QKD, esperti di sicurezza, enti accademici ecc...).

L'OPENQKD ha l'ambizione di portare l'Europa a giocare un ruolo di primo piano nell'ambito delle tecnologie per la quantum communication. Il raggiungimento di questo obiettivo si fonda su alcune iniziative messe in campo dall'OPENQKD:

- realizzare alcuni testbeds per la QKD con l'obiettivo di promuovere e dimostrare verso potenziali utilizzatori e stakeholders del campo della ricerca e dell'industry, le funzionalità della tecnologia e la realizzabilità di use cases per la quantum communication
- incentivare lo sviluppo dell'ecosistema, promuovere la formazione, supportare l'evoluzione tecnologica e lo sviluppo della supply chain delle tecnologie e servizi per la quantum communication

Nel 2018 il Presidente degli USA Trump ha firmato una proposta di legge per il finanziamento del programma Quantum National Initiative Program per 1.2 MLD$ [24] su un periodo iniziale di 5 anni.
Nel 2017 la Cina ha dichiarato di voler aprire un centro di ricerca specificamente dedicato alle tecnologie quantistiche con un investimento di 10 MLD$ [24]

Use Cases

TIM sta valutando il probabile impatto della tecnologia Quantum Communication (QC) nel settore delle telecomunicazioni, identificando alcuni use case.

Negli ultimi anni, in questo contesto, si è osservata una crescita di interesse in campo internazionale, maggiori investimenti sia a livello di ricerca che a livello sperimentale, da parte di un intero ecosistema (Operatori, Università, Fornitori, Verticals, Amministrazioni) nell'ottica di familiarizzare con le nuove tecnologie, partendo dall'attuale livello tecnologico, e verificando

Fonte 29
ADVA Quantum-safe encryption deployment

la reale disponibilità di nuove applicazioni inerenti a nuovi spazi di mercato.

In particolare per gli operatori telco, come TIM, i benefici concretizzabili sono duplici sia per la clientela che internamente:

- lato End-user:
  - Crittografia quantistica sicura di dati critici
  - Applicazioni time-critical e coordinazione di applicazioni dislocate in siti remoti con l'utilizzo della distribuzione quantica di segnali di sincronizzazione temporale (via entanglement)
- lato Mobile Network Operator:
  - Internamente: rendere Quantum-safe parti critiche della rete e/o infrastrutture dei data center
  - Verso la clientela: offrire una comunicazione quantistica sicura as a service

Si sta studiando la fattibilità di applicazione delle QC su due fronti:

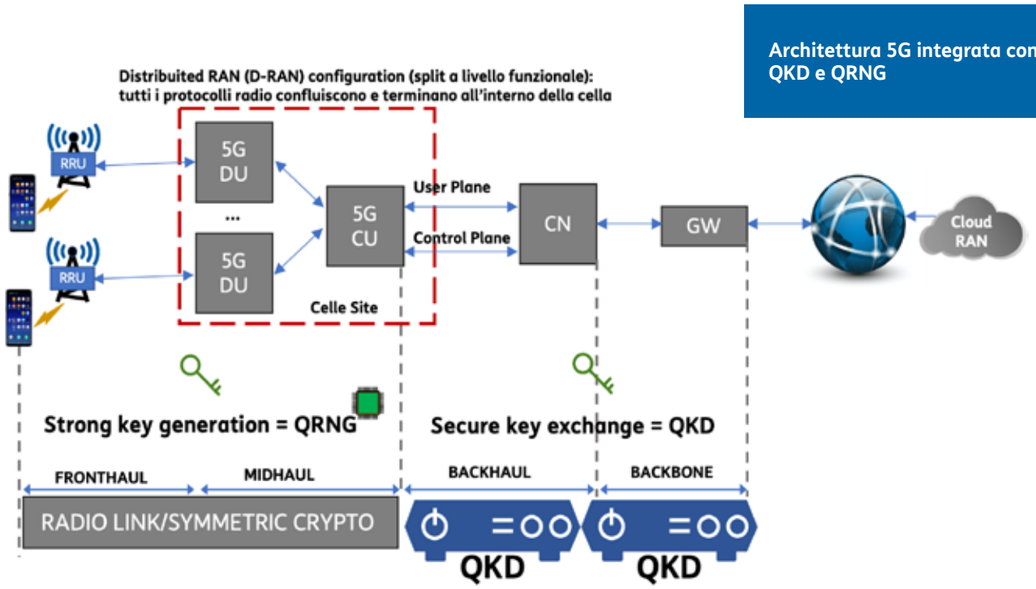
- l'integrazione di tali tecnologie nella propria infrastruttura legacy in fibra ottica, sfruttando anche le nuove potenzialità del 5G
- l'abilitazione di servizi che potrebbero avere una ricaduta nel breve e medio termine anche nel settore Industry 4.0

Nel seguito vengono riportati alcuni casi d'uso scelti tra i molti proposti ed in fase di studio e realizzazione.

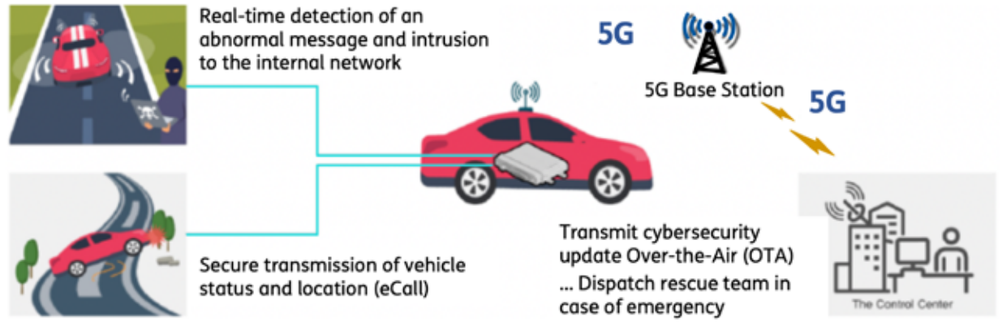
Comunicazione sicura, tramite QKD, tra due Customer data center (peer2peer)

Trattasi di un collegamento in grado di trasportare canali classici e quantistici sulla stessa infrastruttura, per inviare dati crittografati e per distribuire le relative chiavi crittografiche quantiche.

Una sperimentazione analoga è stata finanziata dal governo UK



Architettura 5G integrata con QKD e QRNG



Fonte 30
SKT: V2X Secure Central Gateway demonstration

e realizzata (a marzo 2019) da Quantum Communications Hub (QComm Hub): una partnership tra ADVA, BT, ID Quantique e le università di Cambridge e York.

La soluzione include un sistema di ID Quantique per la distribuzione delle chiavi crittografiche su canale quantistico e un sistema di trasporto ottico di ADVA per il trasporto dei dati su una distanza di 120 km tra l'hub tecnologico di BT (Adastral Park) e l'Università di Cambridge.

In ambito amministrativo risulta interessante anche l'esperienza svizzera, durante le elezioni nazionali, in cui è stata usata la crittografia quantica per proteggere la rete tra il centro raccolta dei voti e quello governativo in cui sono archiviati.

Utilizzare la QC per proteggere la comunicazione all'interno della rete oppure tra utente e rete nell'architettura 5G

La maggior parte dei link di Backhaul e di Backbone di una rete sono realizzati su fibra ottica. La QKD (Quantum Key Distribution) può esser aggiunta logicamente come un layer con un livello di distribuzione di chiavi, per esempio per proteggere in un'architettura di rete radiomobile:

- le connessioni di controllo (Control Plane)
- le connessioni radio (User Plane) tramite crittografia simmetrica combinata con QRNG

Security Industry 4.0

L'impiego delle QC (in particolare delle tecniche QKD e QRNG) può garantire la sicurezza anche nel settore Industry 4.0, cioè essere esteso ai sistemi di produzione come quelli dell' automotive e dell'industria manifatturiera e di processo, tenendo conto dei requisiti specifici del dominio in termini di criticità temporale, sicurezza e protezione.

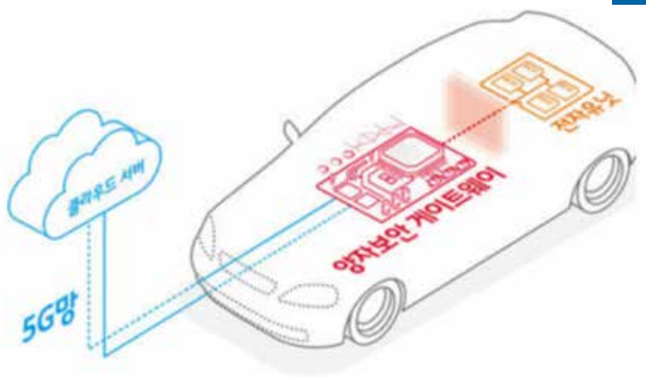
Sicurezza quantica per “connected vehicles”

In previsione di una maggiore diffusione di veicoli connessi e a guida autonoma diventa fondamentale l’ambito della sicurezza. Infatti bisogna assicurare che il controllo di un veicolo a guida autonoma non sia assunto da un malintenzionato, tramite l’installazione di software malicious.

Due, sono le fasi principali potenzialmente a rischio hacking, in cui ha senso l’adozione di QKD e QRNG:

- comunicazione intra-veicolo: all’interno dell’autoveicolo tra i vari moduli ospitanti una logica intelligente
- comunicazione extra-veicolare: fra veicolo e stazione di ricarica (ad esempio durante l’aggiornamento del firmware del modulo intelligente sul veicolo)

Interessante l’iniziativa di SK Telecom (2018): in un contesto 5G, lancia un gateway QKD per Vehicle-2-Everything (V2X) per un sistema di assistenza alla guida.
E’ un dispositivo che monitora le reti a bordo per rilevare intrusioni/anomalie quasi in real-time grazie al 5G (notifica, eventuali tentativi di hacking, al conducente e a qualsiasi centro di monitoraggio collegato,). La sicurezza applicativa è garantita da un QRNG, che produce una chiave quantistica rendendo più sicuri i messaggi applicativi inviati via rete mobile.



Fonte 31
SKT launch a Quantum gateway for connected vehicles

Sicurezza quantica in una micro-fabbrica

Un riferimento applicativo, può essere quello della micro-fabbrica, in particolare un ambiente di prototipazione di auto elettriche e dei relativi impianti produttivi. In tale dominio, si sta studiando la fattibilità di inserire un “gateway QKD” in alcuni punti/parti del processo di produzione, quali:

- le “isole” lungo la catena di montaggio/fabbricazione dell’autoveicolo;
- la supply chain con i fornitori

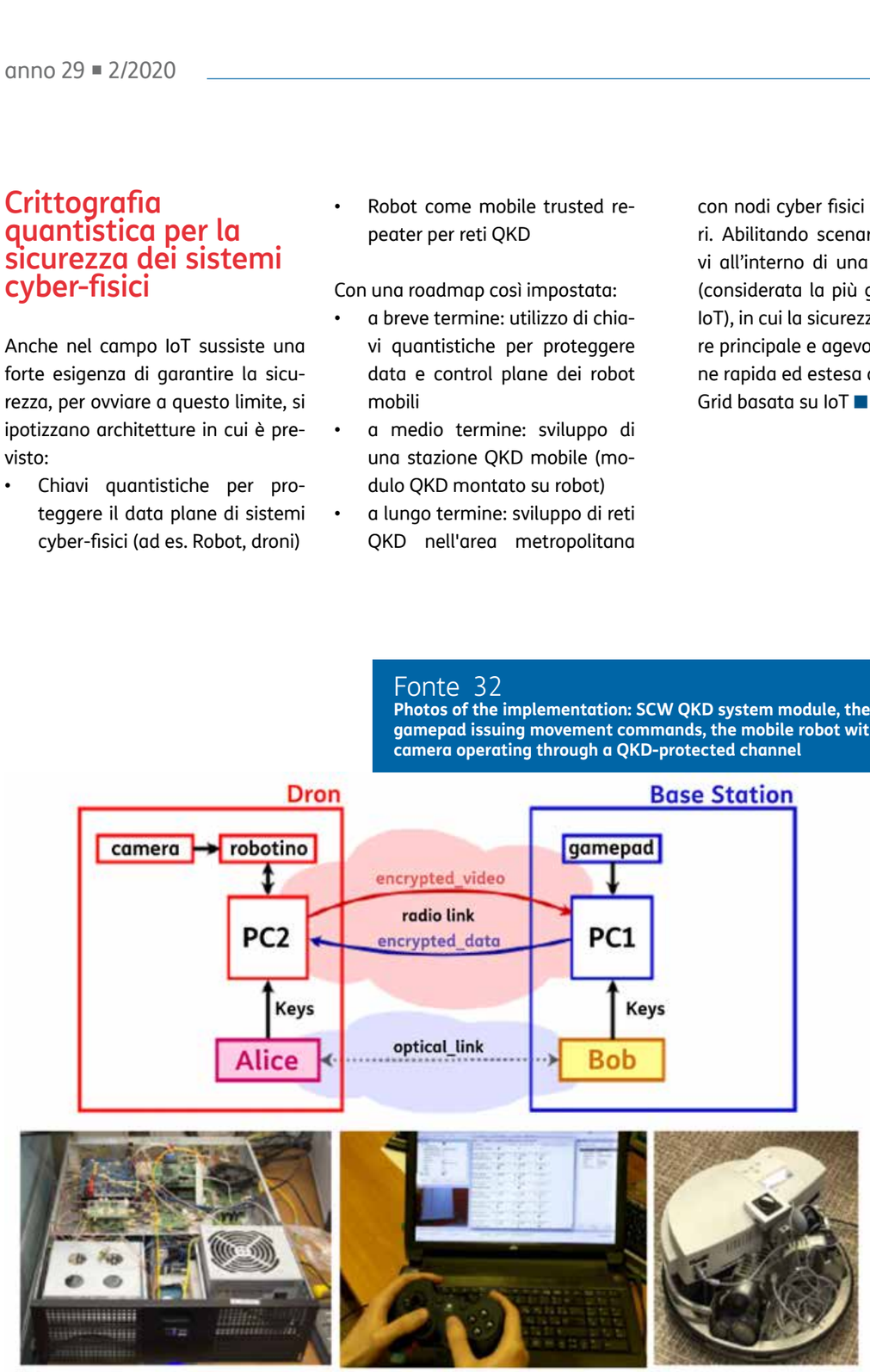
Crittografia quantistica per la sicurezza dei sistemi cyber-fisici

Anche nel campo IoT sussiste una forte esigenza di garantire la sicurezza, per ovviare a questo limite, si ipotizzano architetture in cui è previsto:

- Chiavi quantistiche per proteggere il data plane di sistemi cyber-fisici (ad es. Robot, droni)
- Robot come mobile trusted repeater per reti QKD

Con una roadmap così impostata:

- a breve termine: utilizzo di chiavi quantistiche per proteggere data e control plane dei robot mobili
- a medio termine: sviluppo di una stazione QKD mobile (modulo QKD montato su robot)
- a lungo termine: sviluppo di reti QKD nell'area metropolitana con nodi cyber fisici e stazionari. Abilitando scenari applicativi all’interno di una smart city (considerata la più grande rete IoT), in cui la sicurezza è il fattore principale e agevola l'adozione rapida ed estesa della Smart Grid basata su IoT ■



Fonte 32
Photos of the implementation: SCW QKD system module, the gamepad issuing movement commands, the mobile robot with a camera operating through a QKD-protected channel

Bibliografia

1. http://en.wikipedia.org/wiki/The_Magic_Words_are_Squeamish_Ossifrage
2. http://futurism.com/nsa-warns-dangers-quantum-computing
3. http://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201109fa6.html
4. https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html
5. V.Ojha, A.Sharma, V.Goar et Al., Limitation of Practical Quantum Cryptography, Intl. J. of Computer Trends and Technolo., Mar-Apr. 2011
6. http://en.wikipedia.org/wiki/Quantum_key_distribution
7. http://www.idquantique.com
8. http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/
9. http://www.adva.com/en/newsroom/press-releases/20190326-adva-plays-key-role-in-development-of-uks-quantum-secured-transport-network
10. http://www.micro-photon-devices.com/
11. https://www.york.ac.uk/news-and-events/news/2019/research/ultra-secure-quantum-network-link/
12. http://www.uqcc.org/QKDnetwork/
13. Aa.Vv, Field Trial of a finite-key quantum key distribution system in the Florence metropolitan area, Quantum Proceeding, March 2019
14. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6452733/
15. Quantum Key Distribution: Use Cases – ETSI GS QKD 002 v1.1.1 (2010-06)
16. http://www.etsi.org/committee/1430-qkd#
17. http://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx
18. http://www.itu.int/md/T17-SG13-200313-TD-WP3-0350/en
19. http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15059
20. http://www.ietf.org/live/previous-ietf-live-sessions/live104/ietf104-qirg/
21. http://www.nist.gov/topics/quantum-communications
22. http://www.iso.org/standard/77097.html
23. http://ec.europa.eu/digital-single-market/en/quantum-technologies
24. http://www.wired.co.uk/article/quantum-computing-china-us
25. Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, Zhen Zhang, “Quantum random number generation”, arXiv:1510.08957v2 [quant-ph]
26. You-Qi Nie, Leilei Huang, Yang Liu, Frank Payne, Jun Zhang, Jian-Wei Pan, “68 Gbps quantum random number generation by measuring laser phase fluctuations”, Rev. Sci. Instrum. 86, 063105 (2015), arXiv:1506.00720v1 [quant-ph]
27. ITU-T Rec. X.1702 “Quantum noise random number generator architecture”, Approved on 2019-11-13
28. White Paper “What is the Q in QRNG?”, Jan. 2019, IDQuantique
29. – ADVA: Quantum-safe Encryption https://www.redimadrid.es/files/2019-8-QuantumSafeDCI-Elbers.pdf
30. – SKT at MWC2019: security Mobility (post by Michael A. Lesniak - True Innovation Program)
31. – SKT launches a quantum gateway for self-driving car security https://www.zdnet.com/article/sk-telecom-to-launch-quantum-gateway-for-self-driving-car-security/
32. – ITU Workshop on Quantum Information Technology for Networks (Shanghai, China, 5-7 June 2019) https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Vladimir%20_Egorov_Presentation.pdf

Sabrina Guerra *sabrina.guerra@telecomitalia.it*

Laureata in Scienze dell’informazione a Torino, è in TIM dal 2001. Ha lavorato in diversi ambiti sempre nel campo dell’innovazione ed, in particolare nella definizione di servizi innovativi nel contesto delle telecomunicazioni. In questi ultimi anni ha maturato anche esperienze in progetti finanziati (europei e nazionali) e ha seguito diversi trial. Inoltre, ha approfondito alcune tematiche applicative quali: domotica, energy management, IoT (Internet of Things) e QS (Quantified Self). Attualmente, lavora nella funzione Chief Innovation & Partnership Office ove approfondisce aspetti della E2E (End -to-End) security e segue le evoluzioni degli standard sul 5G a supporto di ambiti applicativi per droni. Inoltre partecipa a una fase di studio e valutazione delle tecnologie Quantum nell’ottica di abilitare nuovi servizi che potrebbero avere una potenziale ricaduta a breve e medio termine sul business aziendale ■

Maurizio Valvo *maurizio.valvo@telecomitalia.it*

Ingegnere elettronico, Ë in Azienda (prima CSELT) dal 1991, dove si Ë inizialmente occupato di sistemi Passive Optical Network, partecipando a progetti di ricerca e sviluppo europei. Ha proseguito la sua attivit‡ nellíambito della ricerca sui sistemi di accesso innovativi (PON, xDSL, GbE, HFC), occupandosi dellíintegrazione delle reti di accesso broadband in architetture di rete triple-play, contribuendo alla definizione delle specifiche IPTV nellíambito del gruppo Full Service Access Network (FSAN) e coordinando le sperimentazioni in campo di sistemi PON, Free Space Optics, Fixed Wireless Access e di architetture Fibre To The Cabinet. Nell'Area Technology Innovation, coordina nel ruolo di Project Manager le attivit‡ di scouting, specifica, standardizzazione e testing relative allíevoluzione delle tecnologie ottiche di accesso e di raccolta dei siti radiomobili ed Ë responsabile dei laboratori "Access Network Innovation" e "Innovation Lab ñ Next Generation Access Network". È titolare di 6 brevetti, coautore di 3 libri e di numerose memorie presentate a conferenze internazionali. ■

TECNOLOGIE QUANTISTICHE: QUANTUM METROLOGY & SENSING ALL'INRIM

Davide Calonico

L'INRiM dedica rilevanti attività all'uso di tecnologie quantistiche per migliorare le capacità di misura a livello nazionale e internazionale. Il paradigma metrologico con cui si declinano le tecnologie quantistiche è duplice: da un lato effetti quantistici consolidati e altri innovativi concorrono a migliorare le nostre capacità di misura; dall'altro il rigore della metrologia vuole garantire alle tecnologie livelli quantitativi propri di una proposta standardizzata alla società, che rispetti la qualità scientifica e le realtà del mercato.

Introduzione

Nel secolo scorso, a partire dagli anni Trenta e fino alla fine degli anni Novanta, la scoperta e il consolidamento del corpus imponente della Meccanica Quantistica (MQ) ha avuto immediatamente un impatto tra i più significativi nella storia umana.

Fisica atomica, laser, fisica dei semiconduttori, transistor, nanodispositivi sono stati rami della scienza che si sono immediatamente tradotti in tecnologie rivoluzionarie. Ma già alla fine del secolo, e ancora di più oggi, alcuni principi della Meccanica Quantistica ci riservano brillanti innovazioni di cui oggi riusciamo a vedere anche l'utilizzo tecnologico: sviluppi quali il raffreddamento laser, l'entanglement, il principio di sovrapposizione, la coerenza quantistica ci garantiscono capacità tecniche e scientifiche ancora superiori. Computer e simulatori quantistici, comunicazione e crittografia quantistica, una nuova generazione di orologi atomici, sensori quantistici con applicazioni in svariati campi, imaging quantistico: sono alcuni dei temi che riservano l'impatto più significativo.

Nel Quantum Manifesto [1] la Comunità Europea riconosce tutte le potenzialità di questi ulteriori sviluppi, tanto da produrre nella Commissione uno sforzo considerevole, anche e soprattutto economico, per accelerare il passaggio dalle realtà accademiche e dei centri di ricerca a più consolidate tecnologie industriali. Esiti concreti di questo sforzo sono oggi il programma di ricerca "Quantum Technologies Flagship" [2], lanciato dalla Commissione Europea nel 2018 con investimento iniziale di 1 miliardo di euro in dieci anni, destinati a crescere e la "European Quantum Communication Infrastructure" [3], iniziativa lanciata nel 2019, già sostenuta da 25 paesi dell'Unione, con l'ambizioso obiettivo di finanziare e costruire un'infrastruttura per le comunicazioni quantistiche che in dieci anni porti a servizi per la società, infrastruttura fondata su una componente di terra in fibra ottica e una spaziale (da cui una forte sinergia con l'Agenzia Spaziale Europea).

La metrologia, la scienza delle misure e della loro armonizzazione a livello mondiale, ha qui un ruolo duplice. Da un lato, continua a sviluppare dispositivi che le sono propri dalla prima rivoluzione e che sono cardine anche del Quantum Manifesto, come gli orologi atomici, o i sensori che usano proprietà quantistiche, continuando a sviluppare capacità di misura sempre migliori. In questo senso, la metrologia sviluppa il pilastro del Manifesto noto come "Quantum Metrology and Sensing".
D'altro canto però, la metrologia offre la propria specificità interdisciplinare – uso della meccanica quantistica, attenzione rigorosa alle misure, compiti istituzionali di standardizzazione mondiale - e la applica anche su altri pilastri, in particolare sulla comunicazione quantistica e sulla simulazione.
Vedremo quindi brevemente come si declina il ruolo metrologico, e come lo sta interpretando l'Istituto Nazionale di Ricerca Metrologica (INRiM), espressione scientifica per l'Italia nella Convenzione Internazionale del Metro [4,5].

L'attenzione alle Tecnologie Quantistiche della comunità metrologica si è concretizzata nella creazione di un apposito European Metrology Network on Quantum Technologies (EMN-Q) promosso dall'Associazione Europea di Metrologia, Euramet, nell'attuazione di un programma europeo di investimenti per la ricerca, lo European Metrology Program for Innovation and Reasearch (EMPIR) [6]. L'attenzione di INRiM è testimoniata dal Coordinamento dell'EMN-Q, e dalla creazione di una Divisione interamente dedicata alla Metrologia Quantistica.

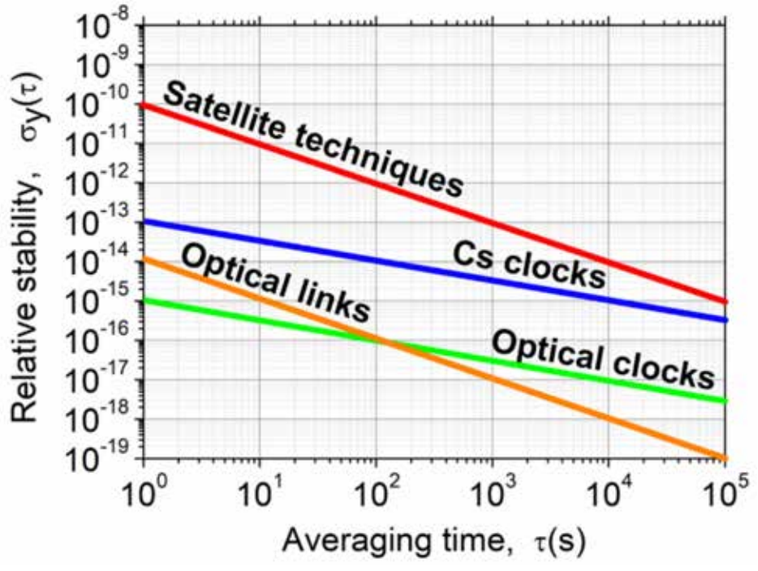
Tecnologie quantistiche basate su Orologi Atomici

Tra le tecnologie quantistiche, gli orologi atomici rivestono un ruolo di cerniera: protagonisti della prima rivoluzione quantistica a partire dagli anni Cinquanta del secolo scorso, compiono un'importante evoluzione con l'utilizzo dell'interazione collettiva tra laser e atomo (raffreddamento laser) e il confinamento laser in reticolo di atomi neutri e di ioni carichi in trappole elettromagnetiche. Lo sviluppo definitivo che li colloca nella seconda rivoluzione quantistica è il passaggio da orologi nel regime delle microonde ad orologi atomici nel regime ottico, detti appunto orologi ottici [7-11].

In un orologio atomico, un sistema quantistico a due livelli funge da riferimento di frequenza per una radiazione in grado di eccitare gli atomi tra due stati di una transizione quantistica detta di orologio.

Negli orologi ottici, la radiazione ha una frequenza nel visibile. Il passaggio agli orologi ottici ha aperto un salto importante nell'accuratezza e nella stabilità di questi sistemi, che hanno migliorato di almeno due ordini di grandezza l'accuratezza ultima di misura, arrivando a parti in 1e18 in termini di frequenza relativa, e di tre ordini di grandezza la cosiddetta stabilità, che identifica anche il rumore statistico esibito da questi dispositivi.

Il miglioramento della stabilità è legato alla velocità con cui gli orologi raggiungono la loro migliore accuratezza; inoltre, il tempo di misura migliora in modo proporzionale al quadrato della stabilità, per cui tre ordini di grandezza di stabilità significa raggiungere la stessa incertezza di misura in un milionesimo del tempo necessario, come si vede in Figura 1.



1
Stabilità degli orologi atomici al Cesio e ottici. Sono riportate le incertezze introdotte dai sistemi di distribuzione dei segnali degli orologi in remoto, con tecniche satellitari e in fibra ottica. La combinazione di orologi ottici e fibra ottica permette la migliore accuratezza in remoto per metrologia quantistica di frequenza e sensing

Dal punto di vista delle tecnologie quantistiche, abbiamo quattro rami principali a cui gli orologi ottici sono interessati. In primis, l'accuratezza a cui sono giunti li rendono dei sensori quantistici molto spinti.

Un esempio è il loro utilizzo in nuove forme di misure geodetiche, note come geodesia relativistica, dimostrato per la prima volta all'INRiM con il suo orologio al Cesio e ad atomi di Itterbio ultrafreddi e un orologio trasportabile tedesco allo Stronzio [12].

Grazie alle nuove accuratezze e alla sensibilità degli orologi dal campo gravitazionale, dato dalla teoria della relatività, due orologi ottici riescono a misurare la differenza di

potenziale gravitazionale locale a livello centimetrico. Analoghe possibilità si offrono per la misura di campi magnetici.

Una secondo filone di sviluppo è legato al quantum computing e a alla simulazione quantistica. L'enorme accuratezza con cui si determina l'energia dei livelli energetici di un sistema atomico o a ione per un orologio, li rende candidati ideali per identificare celle di qubit, il cuore di un computer quantistico, dove due stati quantistici sono sovrapposti per creare un quantum-bit, una sovrapposizione di due stati analogo a una base binaria, che evolve secondo le leggi quantistiche e permette una computazione più potente dell'analogo classico.

Gli orologi a ioni sono in questo caso più indicati, perchè i "qubit" realizzati con questi dispositivi sono manipolabili con maggiore sensibilità – gli orologi a ione sono capaci di disporre singoli ioni in array, che determinano quindi array di qubit.

Gli orologi ad atomi neutri invece sono archetipi per la simulazione quantistica: sono in grado cioè di usare questi sistemi manipolabili e misurabili con grande precisione per simulare la fisica quantistica che descrive i comportamenti di altri stati, come quelli tipici della fisica dello stato solido e del magnetismo [13].

Un terzo filone di ricerca invece usa al contrario il paradigma della seconda rivoluzione quantistica: usare fenomeni più complessi per migliorare gli orologi – il cosiddetto enhancement quantistico. In questo caso la ricerca si concentra sul fenomeno dell'entanglement e ancor di più dello squeezing quantistico. Lo squeezing sfrutta una proprietà fondamentale del principio di indeterminazione di Heisenberg.

Due variabili (ovvero due grandezze fisiche) tra loro coniugate non possono essere determinate con incertezza simultaneamente migliorabile a piacere. Il prodotto delle loro incertezze sarà sempre maggiore o al massimo uguale a una quantità proporzionale alla costante di Planck. Nel caso degli orologi, le grandezze coniugate sono alcune funzioni del momento angolare quantistico dell'atomo: la sua proiezione sull'asse di quantizzazione (ottenuto attraverso un campo magnetico) porta l'informazione di orologio, mentre una data combinazione delle componenti su un piano ortogonale all'asse sono la grandezza coniugata.

Lo squeezing consiste nel ridurre significativamente l'incertezza sulla componente di orologio a scapito dell'incertezza sull'altra grandezza. Nel sistema sperimentale, questo viene fatto con accoppiamenti del sistema atomico a luce laser su determinate frequenze. Ne risulta un sistema che sfrutta proprietà avanzate della fisica quantistica per produrre orologi ancora più veloci nelle loro capacità di misura. All'INRiM, quest'ambito di ricerca si svolge su un orologio ad atomi di Stronzio ultrafreddi [14].

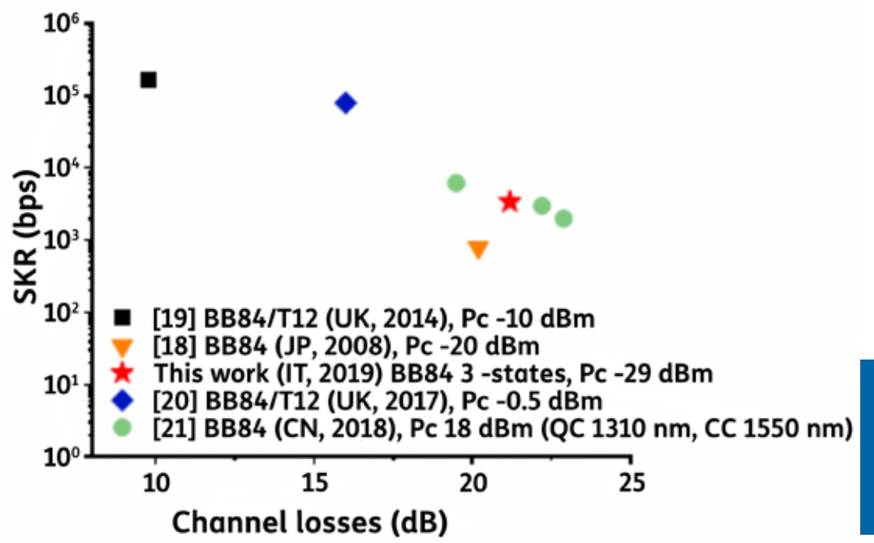
L'ultimo filone di ricerca è la miniaturizzazione degli orologi ottici, che permetterà di trasferire le conquiste delle nuove tecnologie quantistiche su sistemi reali come satelliti e sistemi di telecomunicazione, permettendo così un balzo in avanti nel geoposizionamento e nelle comunicazioni avanzate come quelle del 5G.

Metrologia quantistica e Quantum Key Distribution

La comunicazione quantistica è uno dei pilastri del Quantum Manifesto: si fonda sui principi dell'entanglement e della sovrapposizione quantistica per trasportare maggiori informazioni di quanto possa la comunicazione classica.

É plausibile che questo tipo di comunicazione sosterrà meglio in futuro le reti di computer quantistico, permettendo di evitare un passaggio quantistico-classico-quantistico qualora due computer quantistici dovessero parlare tra loro con protocolli classici.

In realtà un sottoinsieme delle comunicazioni quantistiche si rivela già oggi una tecnologia pronta per l'utilizzo nella società: lo scambio quantistico delle chiavi crittografiche, ovvero la Quantum Key Distribution (QKD).



2
Test di QKD in campo reale sulla dorsale quantistica dell'INRiM [16]

Il protocollo QKD si basa su un fenomeno noto anche come collasso della funzione d'onda. I sistemi quantistici sono caratterizzati da una serie di stati cosiddetti puri, ma uno stato generico è dato da una sovrapposizione di tutti o alcuni stati puri del sistema.

Questo vale anche per i fotoni, i quanti di luce, che sono alla base dei protocolli di comunicazione. I fotoni che viaggiano su una fibra ottica possono essere descritti da una combinazione lineare di stati puri, per esempio in polarizzazione, con una miscela quantistica di stati verticali e orizzontali.

Se passiamo dal mondo macroscopico a molti fotoni a una situazione di singolo fotone, questo continua a essere descritto da una sovrapposizione di stati fino alla misura, ovvero fino a quando non interagisce con un fotorivelatore, dove il suo stato collassa ovvero si presenterà con uno stato definito di polarizzazione, per esempio o verticale o orizzontale.

Tuttavia, preparando diversi fotoni singoli nello stesso modo, in una sovrapposizione identica di stati, all'interazione con il fotorivelatore questi collasseranno in modo casuale in uno dei due stati, seguendo però una ben nota statistica.

L'idea della QKD è di codificare sui singoli fotoni i bit di una chiave crittografica e di lanciare nel canale di comunicazione i bit sotto forma di singoli fotoni. Il vantaggio rispetto

Il protocollo QKD si basa su un fenomeno noto anche come collasso della funzione d'onda. I sistemi quantistici sono caratterizzati da una serie di stati cosiddetti puri, ma uno stato generico è dato da una sovrapposizione di tutti o alcuni stati puri del sistema.

Questo vale anche per i fotoni, i quanti di luce, che sono alla base dei protocolli di comunicazione. I fotoni che viaggiano su una fibra ottica possono essere descritti da una combinazione lineare di stati puri, per esempio in polarizzazione, con una miscela quantistica di stati verticali e orizzontali.

Se passiamo dal mondo macroscopico a molti fotoni a una situazione di singolo fotone, questo continua a essere descritto da una sovrapposizione di stati fino alla misura, ovvero fino a quando non interagisce con un fotorivelatore, dove il suo stato collassa ovvero si presenterà con uno stato definito di polarizzazione, per esempio o verticale o orizzontale.

Tuttavia, preparando diversi fotoni singoli nello stesso modo, in una sovrapposizione identica di stati, all'interazione con il fotorivelatore questi collasseranno in modo casuale in uno dei due stati, seguendo però una ben nota statistica.

L'idea della QKD è di codificare sui singoli fotoni i bit di una chiave crittografica e di lanciare nel canale di comunicazione i bit sotto forma di singoli fotoni. Il vantaggio rispetto

a una comunicazione classica è che se la chiave viene intercettata sul canale di comunicazione, il collasso della funzione d'onda avviene ad opera di chi intercetta.

Il collasso è irreversibile: il destinatario della chiave si accorgerà dell'intercettazione perché la statistica di conteggi non è più compatibile con singoli fotoni in una sovrapposizione di stati, ma soltanto con fotoni "collassati". In altre parole, abbiamo una legge irreversibile di natura che garantisce di conoscere la violazione della chiave.

La metrologia della QKD si concentra su tre filoni di ricerca. Innanzitutto, per la creazione di un protocollo di QKD sono indispensabili sorgenti di singolo fotone, codificatori di bit su questi fotoni, e infine rivelatore di singolo fotone.

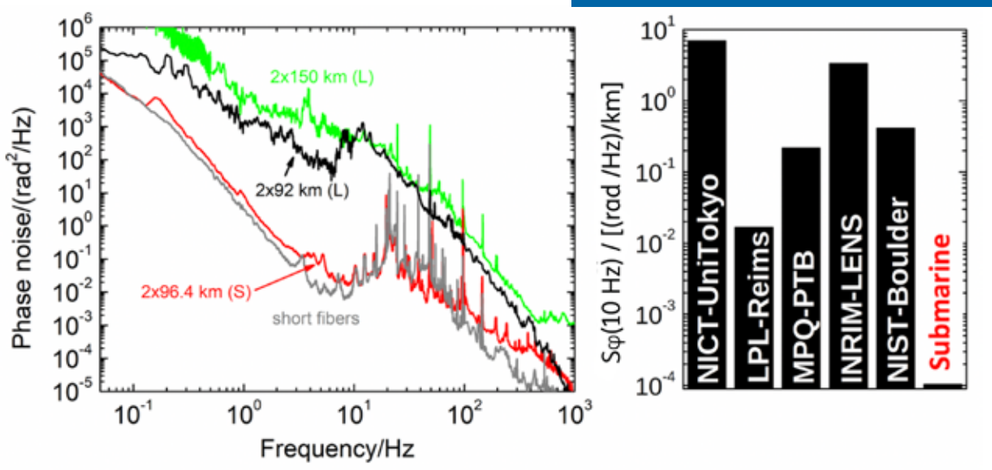
Le capacità di questi elementi devono essere certificate e standardizzate per garantire l'efficienza del protocollo quantistico, su cui INRiM è attivo da diversi anni [15].

Un secondo filone è la realizzazione in campo. Qui la comunicazione quantistica si avvarrà dell'esperienza su fibra ottica che proviene dalla metrologia di tempo e frequenza: INRiM ha già dato diversi contributi con la propria esperienza sulla propria dorsale in fibra ottica (vedi paragrafo 5) [16-19].

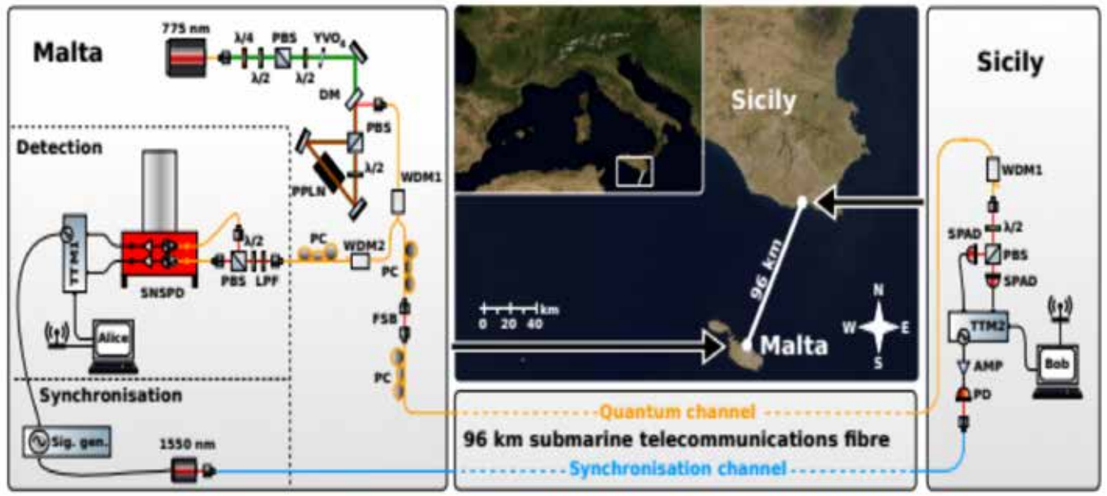
Infatti, la conoscenza di alcune proprietà della fibra, non tanto l'attenuazione, ma il rumore di fase e di polarizzazione sono componenti cruciali per realizzazioni in campo efficaci [17].

Negli anni e per altri motivi, la metrologia ha sviluppato tecniche di misura e di controllo di queste priorità che ora si rivelano importanti per capire il sistema QKD in ambiente reale, soprattutto quando si parla di tragitti maggiori di distanze di pochi chilometri.

In figura 2,3 si mostrano i risultati delle misure di rate QKD e del rumore di fase in due diversi esperimenti.



3
Rumore di fase della fibra ottica in applicazioni di tecnologie quantistiche. Confronto tra tratti terrestri e tratti sottomarini [17]



4
Esperimento sottomarino di entanglement a singolo fotone. Set up sperimentale [18,19]

Figura 4 riporta il set-up sperimentale di una distribuzione di entanglement su cavo sottomarino [18]

Imaging: a super-risoluzione quantistica

Un ambito di ricerca del sensing quantistico di grande rilevanza è l'imaging quantistico [20].

L'imaging è ovviamente un settore di notevoli investimenti da sempre, in particolare per quanto riguarda la microscopia: gli avanzamenti nella risoluzione dell'indagine del microcosmo hanno portato sempre a notevoli sviluppi nelle scienze, soprattutto biologiche e dei materiali [21].

L'illuminazione di oggetti con luce quantistica, ovvero usando emettitori di singolo fotone, permette di estrarre informazioni dalle correlazioni misurate dai fotorivelatori che catturano i singoli fotoni diffusi dal target illuminato.

Le proprietà di diffrazione e le limitazioni di risoluzione legate alla diffrazione classica possono essere superate, sfruttando effetti quantistici come l'antibunching, tecniche esotiche note come ghost imaging e che hanno tutte due obiettivi primari: da un lato, l'imaging di sorgenti debolissime, dove il rumore ottico di fondo impedisce la risoluzione dell'immagine; da un altro, il superamento dei limiti di risoluzione dati dalla diffrazione.

Il Ghost imaging fu proposto e realizzato negli anni Novanta del secolo scorso, usando correlazioni quantistiche generate da sorgenti di luce note come spontaneous parametric down conversion (SPDC).

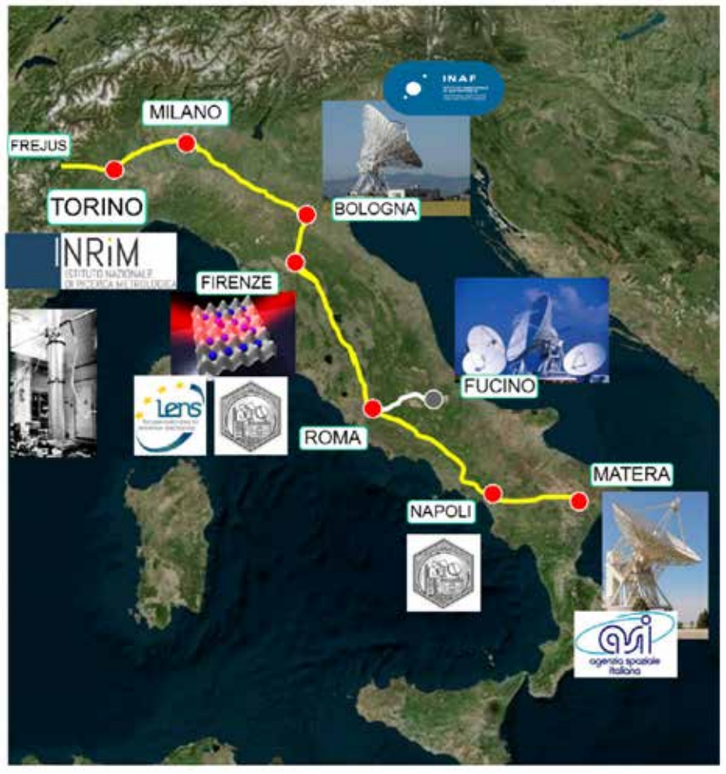
In realtà, questo tipo di tecnica si trovò inizialmente a definire il dibattito scientifico nel confine tra effetti classici ed effetti quantistici, ma successivamente ottenne maggiore attenzione perché si dimostrò utile in svariati casi del mondo reale, in cui per esempio il fondo ambientale

sovrasta l'oggetto da vedere, come per esempio nei casi di turbolenza atmosferica e sorgenti a bassa intensità, utilizzando le correlazioni del numero di singoli fotoni.
D'altro canto, la sensibilità nell'imaging ottico classico è limitata dal rumore di tipo shot, che è inversamente proporzionale alla radice quadrata del numero di fotoni usati.

Andare oltre questo limite è uno dei temi classici del sensing quantistico, specialmente quando il caso concreto in esame ha dei limiti nella potenza ottica utilizzabile, per esempio perché c'è un limite di danneggiamento o di degradazione del campione da visualizzare.
Luce non classica si rivela particolarmente interessante nell'imaging sub-shot noise [22, 23].
In questo caso, diversi sono le sorgenti possibili, ma meritano menzione le coppie di fotoni entangled che accoppiate a rivelatori di singolo fotone permettono un sensing quantum enhanced fino a raggiungere anche qui il limite fondamentale di Heisenberg in microscopia.
Anche in questo settore, INRiM ha dato contributi rilevanti per avanzare le capacità di microscopia e quest'area di ricerca rimane strategica per l'Istituto.

Infrastrutture per le tecnologie quantistiche all'INRiM: Italian quantum Backbone e Laboratorio Piquet

Nel quadro descritto, INRiM ha dedicato particolare attenzione alle infrastrutture di ricerca, realizzando due rilevanti sistemi, aperti anche ad altri istituti e collaborazioni.



5
Dorsale Italiana in Fibra Ottica dell'INRiM per le tecnologie quantistiche

La prima infrastruttura è l'Italian Quantum Backbone [24], una dorsale in fibra ottica di 1800 km dedicata alla distribuzione dei riferimenti degli orologi ottici e allo sviluppo in campo di tecnologie quantistiche come la QKD (la Figura 5 mostra lo sviluppo geografico della dorsale). La dorsale collega tutte le principali città italiane, i principali centri di ricerca nazionali (CNR, INAF, ASI) e si collega a reti analoghe europee.

La struttura è aperta alle collaborazioni di ricerca anche con l'industria, come sta avvenendo con le principali aziende nel settore dell'aerospazio e della difesa.

La seconda infrastruttura di ricerca è il laboratorio Piemonte Quantum Enhanced Techonologies (Piquet) [25], finanziato da fondi europei POR-FESR sul bando Infra-P della Regione Piemonte, coordinato da INRiM in collaborazione con Politecnico e Università di Torino.

Piquet è un laboratorio in camera pulita (500 metri quadri) che accoglie macchine di nanofabbricazione per le nanotecnologie, le tecnologie quantistiche e i dispositivi, in particolare quelli della comunicazione e del sensing quantistico descritti in precedenza.
Anche Piquet vuole essere un'infrastruttura di ricerca aperta, per collaborazioni soprattutto industriali.

Conclusioni

La metrologia quantistica, come quella tradizionale, si presenta con sfumature diverse.

Da ogni punto di vista, un approccio metrologico alle tecnologie quantistiche si caratterizza per una grande attenzione al rigore della qualità delle misure, al percorso più opportuno per la certificazione e la standardizzazione e infine a un rapporto molto stretto con l'industria e al servizio del tessuto produttivo nazionale e internazionale.

Un aspetto caratteristico è invece dato dalla vicinanza tra innovazione tecnologica e tentativo di standardizzazione, che trova sintesi nell'accelerazione della presa di beneficio da parte delle aziende.

In questo senso, le iniziative della Commissione Europea spingono molto a questa convergenza rapida tra risultati dei centri di ricerca e il loro recepimento da parte del tessuto produttivo, con una forte incentivazione di natura economica già in atto e che vede un rafforzamento nei prossimi anni.

Dal punto di vista meramente tecnico-scientifico, le tecnologie quantistiche di seconda generazione mostrano già una maturità di rilievo in alcuni dispositivi (sensing, QKD, metrologia di frequenza), ma hanno potenzialità ancora forti e soprattutto vedono nel processo di micro e nanofabbricazione una convergenza rispetto a quelle piattaforme che sono state dominanti nella prima rivoluzione quantistica ■

Bibliografia

1. http://qurope.eu/manifesto
2. https://qt.eu/
3. https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network
4. https://www.bipm.org/en/worldwide-metrology/national/
5. https://www.inrim.it/lente/chi-siamo/missione
6. https://www.euramet.org/european-metrology-networks/quantum-technologies/
7. Nicholson, T. L. et al. Systematic evaluation of an atomic clock at 2× 10−18 total uncertainty. Nat. Commun. 6, 6896 (2015).
8. Ushijima, I., Takamoto, M., Das, M., Ohkubo, T. & Katori, H. Cryogenic optical lattice clocks. Nat. Photon. 9, 185–189 (2015).
9. Huntemann, N., Sanner, C., Lipphardt, B., Tamm, C. & Peik, E. Single-ion atomic clock with 3× 10−18 systematic uncertainty. Phys. Rev. Lett. 116, 063001 (2016).
10. Margolis, H. Timekeepers of the future. Nat. Phys. 10, 82–83 (2014).
11. Pizzocaro, M. et al. Absolute frequency measurement of the 1S0–3P0 transition of 171Yb with a link to international atomic time, Metrologia 57 035007 (2020)
12. Grotti, J. et al., Geodesy and metrology with a transportable optical clock, Nature Physics, 14, 437 (2018)
13. Livi, L. F. et al., Synthetic Dimensions and Spin-Orbit Coupling with an Optical Clock, Physical Review Letters, 117, 220401 (2016)
14. http://rime.inrim.it/labafs/
15. Meda, A. et al. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution, Light-Science & Applications, 6, e16261 (2017)
16. Bacco, D. et al. Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area, Epj Quantum Technology, 6, 5 (2019)
17. Clivati et al., Optical frequency transfer over submarine fiber links Optica 5, 893-901 (2018)
18. Wengerowsky, S. et al. Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre Npj Quantum Information 6, 5 (2020)
19. Wengerowsky, S. et al Entanglement distribution over a 96-km-long submarine optical fiber, Pnas, 116, 6684-6688 (2019)
20. Berchera Ruo, I. et al. Quantum imaging with sub-Poissonian light: challenges and perspectives in optical metrology Metrologia, 5,6, 024001 (2019)
21. https://www.nature.com/collections/gypbyxmrcq
22. Samantaray, N. et al. Realization of the first sub-shot-noise wide field microscope Light-Science & Applications 6, e17005 (2017)
23. Brida, G.et al., Experimental realization of sub-shot-noise quantum imaging Nature Photonics, 4, 227-230 (2010)
24. Calonico, D.et al., Light and the distribution of time, EPL,110, 40001 (2015)
25. http://www.piquetlab.it/

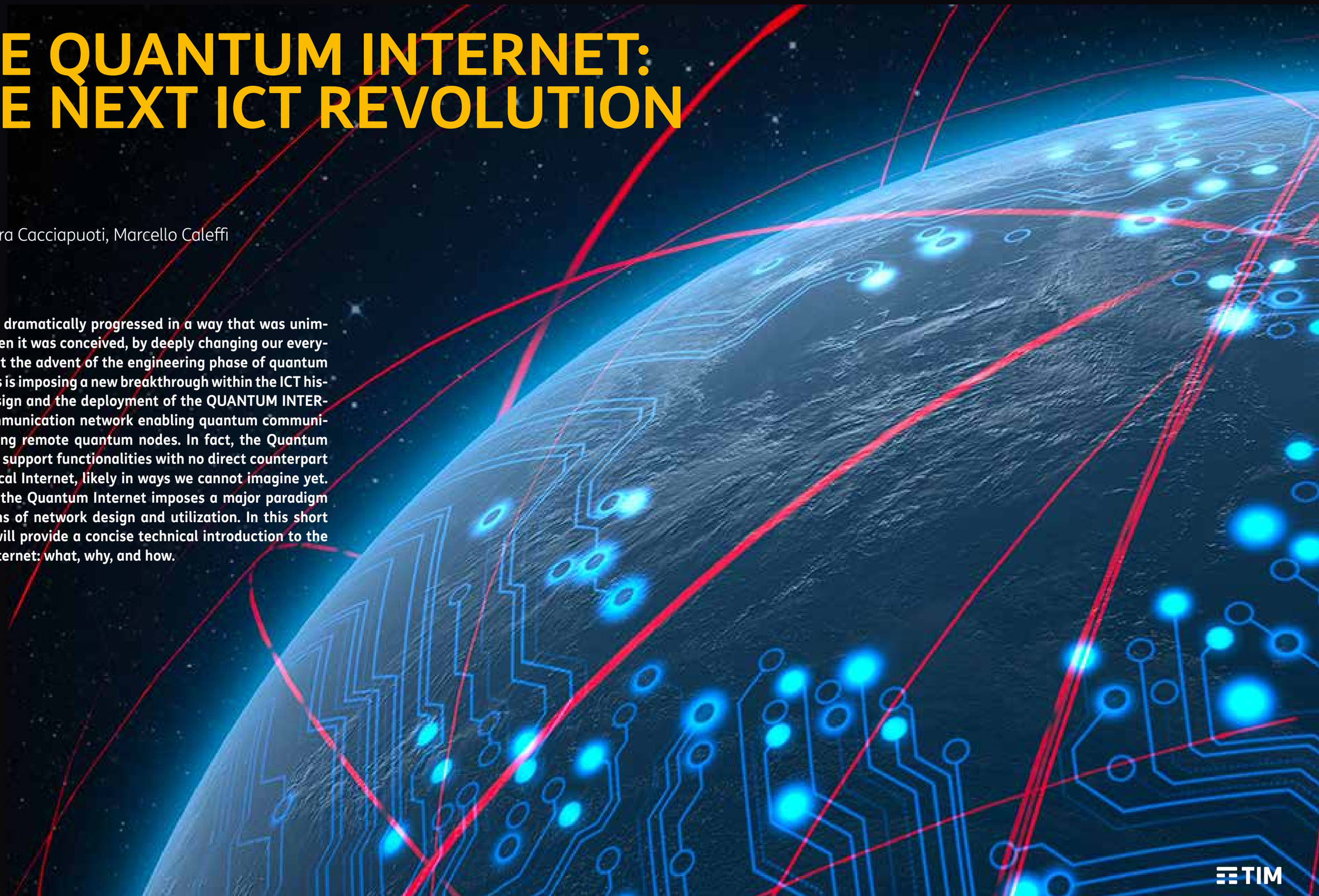
Davide Calonico *d.calonico@inrim.it*

Davide Calonico è fisico, PhD in metrologia presso il Politecnico di Torino.
Responsabile della Divisione "Metrologia e nanotecnologie quantistiche" presso INRIM, l'Istituto metrologico nazionale italiano, si occupa principalmente di tecnologie quantistiche, metrologia del tempo e della frequenza, orologi atomici raffreddati a laser e distribuzione di tempo certificato in fibra ottica. DC è anche Presidente del Consorzio Top-IX, una delle più grandi infrastrutture di Internet Exchange in Italia. Le sue attività di sviluppo di Tecnologie Quantistiche comprendono la realizzazione di un backbone nazionale di 1800 km, per testare nuove tecnologie legate alla comunicazione quantistica, al quantum sensing e in particolare alla QKD. DC è anche coinvolto nell'iniziativa European Quantum Communication Infrastructure, per costruire un'infrastruttura europea di comunicazione quantistica della Commissione Europea ■

THE QUANTUM INTERNET: THE NEXT ICT REVOLUTION

Angela Sara Cacciapuoti, Marcello Caleffi

Internet has dramatically progressed in a way that was unimaginable when it was conceived, by deeply changing our everyday lives. But the advent of the engineering phase of quantum technologies is imposing a new breakthrough within the ICT history: the design and the deployment of the QUANTUM INTERNET – a communication network enabling quantum communications among remote quantum nodes. In fact, the Quantum Internet will support functionalities with no direct counterpart in the classical Internet, likely in ways we cannot imagine yet. To this aim, the Quantum Internet imposes a major paradigm shift in terms of network design and utilization. In this short article, we will provide a concise technical introduction to the Quantum Internet: what, why, and how.



The Quantum Internet

In the realm of computing, probably the most commonly referred quantum algorithm is the pioneering Shor's factoring algorithm, which proved the disruptive potential of quantum computation for integer factorization [1].

The hardness of the integer factorization problem constitutes the essence of the most widely adopted method for securing our communications over the modern Internet. Cracking a 2048-bit RSA encryption key with a classical supercomputer takes billions of years – more than the age of the universe – but it would take only a few minutes (or hours) by using a quantum computer [2]. This implies that our online banking system, encrypted so far with 1024-bit keys, can be almost instantaneously decrypted when a fully functioning quantum computer is available.
A quantum computer inherits its computing power owing to the unique features of its building blocks – aka the quantum bits (qubits), describing a discrete two-level quantum state – to be in unconventional states such as superposition and entanglement. To elaborate a little further, in classical domain, the unit of information is conveyed by the binary digit (bit), which can only hold the value "0" or "1" at a certain time. By contrast, the unit of quantum information – the so-called qubit – can be used to convey "0", "1", or the superposition of both of them at the same time. Meanwhile, entanglement – the most distinguishing quantum phenomenon with no counterpart in the classical world – is a special case of superposition of multiple qubits in which the quantum states of the particles become inextricably linked.

And any action experienced by one particle will immediately influence the others even if they are separated at a great distance [3]–[5].

Thanks to these marvels – and by grossly oversimplifying – the computing power of a quantum computer scales exponentially with the number of qubits that can be embedded and interconnected within [4]–[6].
The greater is the number of qubits, the harder is the problem that can be solved by a quantum computer.

Unfortunately, qubits are very fragile and easily corrupted by interactions with the outside world, via a noise process known as decoherence [3], [7]. And the challenges for controlling, interconnecting, and preserving the qubits get harder as the number of qubits within the quantum processor increases.

A very promising approach to address the challenges arising in the realization of large-scale quantum processors is to realize a quantum communication network – aka the Quantum Internet – to mimic modern high-performance computing infrastructures –where thousands of processors, memories and storage units are inter-connected, and the computational tasks are solved by adopting a distributed computing approach [5].

In fact, with the availability of this communication infrastructure and by adopting the distributed paradigm, the Quantum Internet can be regarded as a virtual quantum machine constituted by a high number of qubits, scaling with the number of interconnected devices. This, in turn, implies the possibility of an exponential speed-up of the quantum computing power, with just a linear amount of the physical resources [6], i.e., the quantum processors.

More in detail, the Quantum Internet is a global quantum network, able to transmit qubits and to distribute entangled quantum states among remote quantum devices through quantum links, in synergy with classical links.

Such a quantum network constitutes a breakthrough, since it will provide unparalleled capabilities [8]–[10] – by exploiting its exponentially larger state space – ranging from blind computing through secure communications to noiseless communications, which have already been theorized or even experimentally verified [3], [5], [6], as recently overviewed by an IETF Quantum Internet Draft [11].

The Road Towards the Quantum Internet

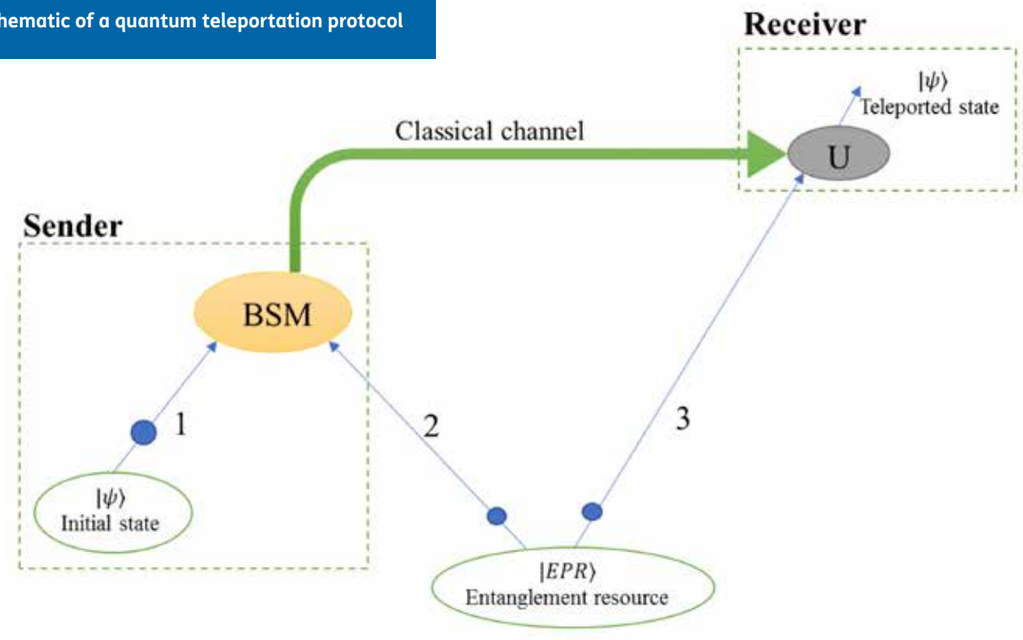
As mentioned before, the gravest challenge of quantum information technologies is mitigating the deleterious effects of quantum decoherence, a type of noise with no counterpart in classical networks.
An immeasurable amount of efforts has been invested for perfecting the physical implementation of quantum processors and quantum links as well as for composing various error control protocols on the upper layers for circumventing the unavoidable imperfection.

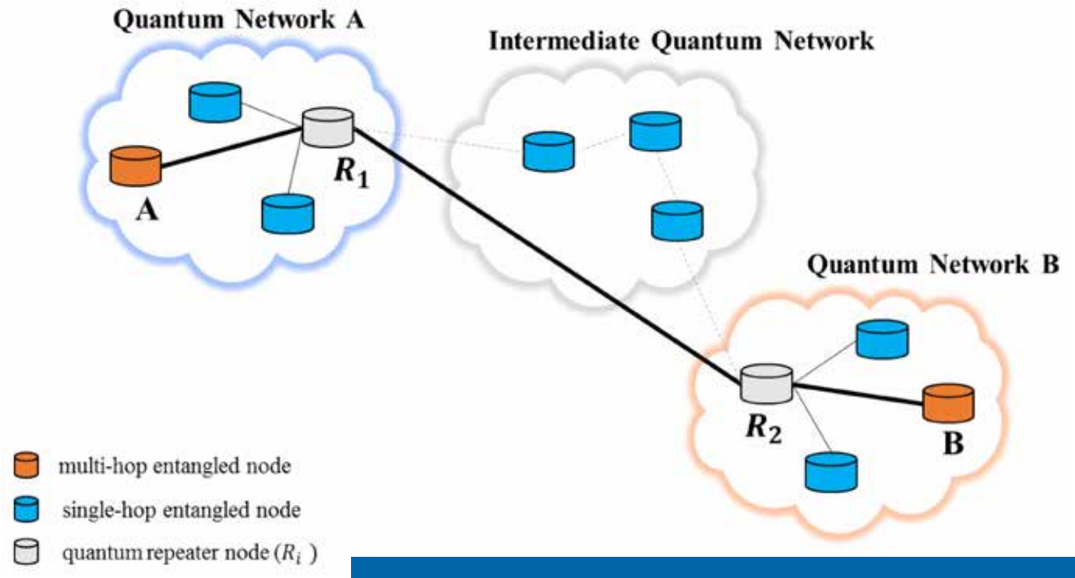
In the classical domain, several methods of error-control or congestion are invoked to guarantee the successful transmission of information, such as forward error-correction in the physical layer as well as automatic request protocol (ARQ) in the data-link and network layer within the classical TPC/IP network stack.

And they have been proven to be effective solutions for the classical Internet during the last decades. However, these techniques rely on the capability of extensively reading and copying information.

Bits are duplicated among the different components of a network and among different nodes.

1
The schematic of a quantum teleportation protocol





2
The stylized topology of entanglement distribution in the Quantum Internet. The initial network consists of a transmitter node (A), a distant target node (B) and intermediate repeater nodes (Ri)

Unfortunately, this does not hold in the Quantum Internet as a consequence of the no-cloning theorem – which forbids any possibility of duplicating an unknow qubit.

Furthermore, the simple act of measuring – i.e., reading – a qubit irremediably alters the encoded quantum information due to the quantum measurement postulate.

Due to the aforementioned quantum principles, it results that – although one can transmit directly a qubit to a remote node via a fiber link by encoding the quantum information within an inner state of a photon – if the traveling photon is lost due to attenuation or it is corrupted by noise, the associated quantum information cannot be recovered via a measuring process or a copy of the original information.

As a consequence, the direct transmission of qubits via photons is not readily feasible, unless the network applications can tolerate the loss of information and/or low transmission success rates, as in Quantum Key Distribution (QKD) networks [3].

If the quantum links are inevitably noisy and direct transmission of qubits is not feasible, how can we possibly conceive a reliable connection between two remote quantum processors? Luckily, the wonderful properties of quantum mechanics equip the Quantum Internet for transferring quantum information without actually sending any qubit through the quantum channel by the virtue of quantum teleportation [3], [12].
The quantum teleportation process of a single qubit is illustrated in Fig. 1.

Specifically, to realize the marvel of quantum teleportation, two resources are needed.

One resource is classic: two classical bits must be transmitted from the source to the destination.

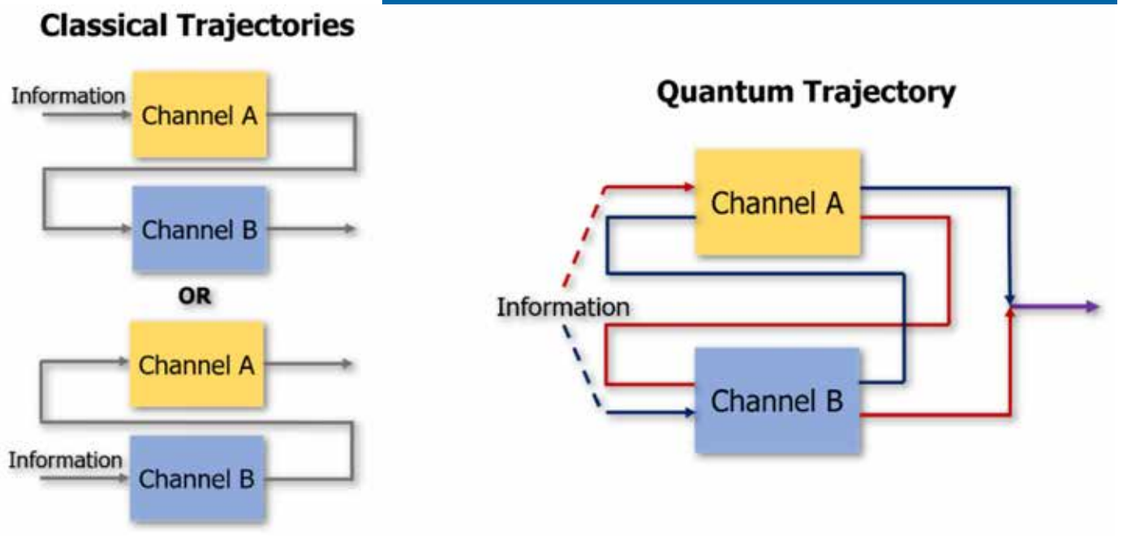
The other resource is quantum: a maximally entangled pair of qubits, also known as EPR pair, must be generated and shared between the source and the destination.
As a consequence, quantum teleportation requires two communication links, a classical link for transmitting the pair of classical bits and a quantum link for entanglement generation and distribution.

From this, it results that the integration of classical and quantum resources is a crucial aspect for the Quantum Internet. In particular, the classical communication resources – i.e., the classical links for transmitting classical bits – will be likely provided by integrating classical networks such as the current Internet with the Quantum Internet [7].

Regarding the quantum communication resources, it seems attractive to utilize existing optical fiber networks. However, efficient ways to interface photons with the hardware implementing the qubits within a quantum processor are yet to be found.

Furthermore, the heterogeneity of the hardware underlying computa-

3
Classical trajectories versus Quantum Trajectories [16]: (left plot) a message traversing two channels in a well-defined causal order; (right plot) a message traversing two channels in a superposition of different orders



tional/memory qubits – atoms, ion traps, superconducting circuits, etc. – within and among the quantum network nodes must be seamlessly handled by the network functionalities [4].
This constitutes a distinctive challenge for the Quantum Internet design with respect to classical networks.

Furthermore, the notion of connectivity in the Quantum Internet will be highly determined by the availability of EPR pairs amongst the quantum nodes across the network.

Consequently, one of the fundamental requirements of the Quantum Internet is the reliable distribution of EPR pairs amongst quantum nodes as depicted in Fig 2. Similar to the classical network, entanglement distribution is accomplished via a quantum repeater [13].

In contrast to a classical repeater, where it relies on the decode-and-forward mechanism, a quantum repeater hinges on the capability of performing entanglement swapping [11] for extending the connectivity within the quantum networks.

On the Noise Mitigation: Some more Perspectives

Obviously, we are facing similar challenges in both classical and quantum communications, namely mitigating the effects of noise introduced by the communication channels.

Borrowing the idea of classical error control, we can have the quantum version of classical error correction.

However, the major drawback of this direct approach is that error correction in the quantum domain requires a massive overhead in terms of physical qubits needed to implement a fault-tolerant logical qubit [14].

In our research group, we approach this problem in a different light. As previously mentioned, quantum information can be in the superposition of multiple states. Interestingly, the concept of superposition state can be extended to the superposition of quantum channels.

Specifically, quantum particles can propagate simultaneously among multiple space-time trajectories – aka quantum trajectories – as illustrated in Fig. 3.

By exploiting this unconventional capability, quantum superpositions of noisy channels can behave as perfect noiseless quantum communication channels, even if no quantum information can be successfully transmitted throughout either of the noisy component channels individually [15], [16].

This phenomenon has no classical counterparts and potentially opens new unexplored possibilities to achieve transmission rates exceeding the fundamental limits of conventional (quantum) Shannon theory [15], [16], with the Quantum Internet providing the underlying infrastructure.

Conclusions

The marvel of quantum technology soon will embrace the world of Internet. The Quantum Internet will enable various alluring applications without classical counterparts. Ultimately, the journey towards the Quantum Internet is a multi-disciplinary and collaborative endeavor.

The communications engineer community with both its academic and industrial components can and should play a fundamental role in this journey. Indeed, with this intent, the “Emerging Technical Committee on Quantum Communications and Information Technology (QCIT- ETC)”, where our Quantum Internet group actively participates, has been established within the IEEE Communications Society.
There are also already significant on-going efforts toward quantum network design and standardization. In this regard, we would like to mention the working group within the Internet Engineering Task Force (IETF), where researchers, including our groups, are trying to conceptualize the architectural principles of the Quantum Internet [11].

Acknowledgement

The authors thank Dr. Daryus Chandra, Daniele Cuomo and Shima Hassanpour – members of the www.QuantumInternet.it research group at the University of Naples Federico II – for their contribution in writing this article ■

References

1. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Review, vol. 41, no. 2, pp. 303–332, 1999.
2. R. Van Meter, K. M. Itoh, and T. D. Ladd, “Architecture-Dependent Execution Time of Shor’s Algorithm,” in Controllable Quantum States: Mesoscopic Superconductivity and Spintronics, World Scientific, 2008, pp. 183–188.
3. A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, “When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet,” IEEE Transactions on Communications (Invited Paper), 2020.
4. M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, “The Rise of the Quantum Internet,” Computer, vol. 53, no. 6, pp. 67–72, 2020.
5. D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, “Towards a Distributed Quantum Computing Ecosystem,” IET Quantum Communication (Invited Paper), 2020.
6. M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, “Quantum Internet: From Communication to Distributed Computing!,” in Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication (Invited Paper), 2018, pp. 1–4.
7. A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, “Quantum Internet: Networking Challenges in Distributed Quantum Computing,” IEEE Network, vol. 34, no. 1, pp. 137–143, 2019.
8. K. Bourzac, “4 Tough Chemistry Problems that Quantum Computers Will Solve,” IEEE Spectrum, vol. 54, no. 11, pp. 7–9, 2017.
9. J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum Machine Learning,” Nature, vol. 549, no. 7671, pp. 195–202, 2017.
10. P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, “Quantum Search Algorithms for Wireless Communications,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1209–1242, 2019.
11. W. Kozlowski, S. Wehner, R. Van Meter, B. Rijsman, A. S. Cacciapuoti, and M. Caleffi, “Architectural Principles for a Quantum Internet,” Internet Engineering Task Force (Work in Progress), Mar. 2020.
12. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels,” Physical Review Letters, vol. 70, no. 13, pp. 1895–1899, 1993.
13. R. Van Meter and J. Touch, “Designing Quantum Repeater Networks,” IEEE Communications Magazine, vol. 51, no. 8, pp. 64–71, 2013.
14. Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, “Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 970–1010, 2019.
15. A. S. Cacciapuoti and M. Caleffi, “Capacity Bounds for Quantum Communications through Quantum Trajectories,” arXiv preprint arXiv:1912.08575, 2019.
16. M. Caleffi and A. S. Cacciapuoti, “Quantum Switch for the Quantum Internet: Noiseless Communications through Noisy Channels,” IEEE Journal on Selected Areas in Communications, vol. 38, no. 3, pp. 575–588, 2020.

Angela Sara Cacciapuoti *angelasara.cacciapuoti@unina.it*

Angela Sara Cacciapuoti is a faculty at the University of Naples Federico II, Italy. Since July 2018, she held the national habilitation as "Full Professor" in Telecommunications Engineering. Currently, Angela Sara serves as Area Editor for IEEE Communications Letters, and as Editor/Associate Editor for the journals: IEEE Trans. on Communications, IEEE Trans. on Wireless Communications, IEEE Trans. on Quantum Engineering and IEEE Open Journal of Communications Society. In 2016 she has been an appointed member of the IEEE ComSoc Young Professionals Standing Committee. Since 2017, she has been the elected Treasurer of the IEEE Women in Engineering (WIE) Affinity Group of the IEEE Italy Section. Since 2018, she has been appointed as Publicity Chair of the IEEE ComSoc Women in Communications Engineering (WICE) Standing Committee and then in 2020 as Vice-Chair of WICE. Her current research interests are mainly in Quantum Communications and Quantum Information Processing. ■

Marcello Caleffi *marcello.caleffi@unina.it*

Marcello Caleffi is with the DIETI Department, University of Naples Federico II, and with the National Laboratory of Multimedia Communications, National Inter-University Consortium for Telecommunications (CNIT). From 2010 to 2011, he was with the Broadband Wireless Networking Laboratory at Georgia Institute of Technology and with the NaNoNetworking Center in Catalunya (N3Cat) at the Universitat Politecnica de Catalunya (UPC), as visiting researcher. Since July 2018, he held the Italian national habilitation as Full Professor in Telecommunications Engineering. His work appeared in several premier IEEE Transactions and Journals, and he received multiple awards Currently, he serves as editor/associate technical editor for IEEE Trans. on Quantum Engineering, IEEE Communications Magazine and IEEE Communications Letters. He has served as Chair, TPC Chair, and TPC Member for several premier IEEE conferences. In 2017, he has been appointed Distinguished Lecturer from the IEEE Computer Society. In 2019, he has been appointed member of the IEEE New Initiatives Committee from IEEE Board of Directors. ■

QUANTUM SOFTWARE

Michele Amoretti

Current progress in the field of quantum computer hardware makes it credible that, in just a few years, quantum computers will outperform classical ones. Many research groups and companies are working on the hardware, but the key questions of what a realistically-sized quantum computer can achieve, how to do this, and how to verify the results refer to quantum software. In this article, we stress the importance of quantum software and illustrate a few meaningful examples.

The importance of quantum software

A quantum computer is a device that harnesses the laws of quantum mechanics to solve certain tasks using fewer computational resources than classical computers. The fundamental information-carrying components of a quantum computer are the quantum bits (qubits). A qubit is a quantum-mechanical system (e.g., a particle) whose state can be the superposition of 0 and 1 at the same time.

At least as important as building quantum computers is the quest to establish which problems are prone to quantum speed-ups and to develop quantum algorithms that can achieve such speed-ups.

Quantum software addresses the key questions of what a realistically-sized quantum computer can achieve, how to do this, and how to verify the results [QSManifesto]. The broad and multidisciplinary field of quantum software includes a wide range of topics, such as quantum algorithms and protocols, quantum information theory and verification of quantum devices.

In this article, we present our research activity on quantum software, encompassing the design and development of highly efficient quantum compilers, quantum algorithms and quantum protocols. Our code is usually released under an open source license and published on GitHub (https://github.com/qis-unipr).

Quantum Compiling

Current quantum computers are noisy intermediate-scale quantum (NISQ) devices [Preskill2018], characterized by a reduced number of qubits (5-50) with non-uniform quality and highly constrained connectivity. Such devices may be able to perform tasks which surpass the capabilities of today's most powerful classical digital computers, but noise in quantum gates limits the size of quantum circuits that can be executed reliably.

Quantum compilation, i.e., device-aware implementation of quantum algorithms, is a challenging problem. A good quantum compiler must translate an input quantum algorithm, defined as a quantum circuit, into the most efficient equivalent of itself, getting the most out of the available hardware. In general, the quantum compilation problem is NP-Hard [Botea2018].

On NISQ devices, quantum compilation is declined in the following tasks: gate synthesis, which is the decomposition of an arbitrary unitary operation into a sequence of gates from a discrete set; compliance with the hardware architecture; and noise awareness. Quality indicators of the compiled quantum algorithm are, for example, circuit depth, gate count and fidelity of quantum states.

Recently, some noteworthy quantum compiling techniques have been proposed. For example, Zulehner et al. [Zulehner2019] proposed a strategy based on the A* search algorithm [Hart1968] for mapping the logical qubits (of the quantum circuit) to the physical qubits (of the device). The proposed approach is efficient in terms of running time and output depth, but may not be scalable because of the exponential space complexity of A*. SABRE by Li et al. [Li2019] is apparently more efficient, but its code has not been released.

In general, most compiling approaches have two common features: 1) they rely on randomized algorithms and 2) they are general purpose, but they are not able to make assumptions on circuit structure or characteristics. These kind of solutions, although effective in many cases, are not as much efficient when facing circuits characterized by well-defined peculiar sequences, i.e., patterns, of two-qubit operators. This is particularly true if those patterns repeat themselves many times in a circuit and are not compliant with the quantum device connectivity.

In a research work with Davide Ferrari [Ferrari2018], we started the investigation of deterministic algorithms for compiling recurrent quantum circuit patterns.

The proposed strategy focused on quantum circuits for generating Greenberger–Horne–Zeilinger (GHZ) entangled states. It is well known that GHZ states have several practical applications, including quantum machine learning.

We integrated the resulting compiler with Qiskit, IBM's open source software development kit for working with OpenQASM and the IBM Q quantum processors.

Later, with Davide Ferrari and Ivano Tavernelli [Ferrari2019], we developed ChainSwap, a software tool implementing new deterministic algorithms that cope with a larger set of quantum circuit patterns.

In particular, such patterns appear in quantum circuits that are used to compute the ground state properties of molecular systems using the VQE algorithm together with a wavefunction Ansätz like the Coupled-Cluster expansion.

Some experimental results are illustrated in Table 1, where ChainSwap is compared to IBM Qiskit's Basic, Stochastic and Lookahead compilers. Ideally, the depth of the compiled circuit should be less or equal to the depth of the input circuit.

	Circuit Depth				
Circuit Name	Input Circuit	ChainSwap	Basic	Stochastic	Lookahead
H2_UCCSD	82	71	71	71	71
LiH_UCCSD	8845	8065	10989	10820	n.a.
H2O_UCCSD	15388	18397	16143	18116	n.a.
Random20_UCCSD	125683	154185	163516	n.a.	n.a.
H2_RyRz	73	56	161	108	n.a.
Li2_RyRz	233	216	n.a.	666	n.a.
H2O_RyRz	273	256	1517	851	n.a.
Random20_RyRz	393	376	3558	1624	n.a.

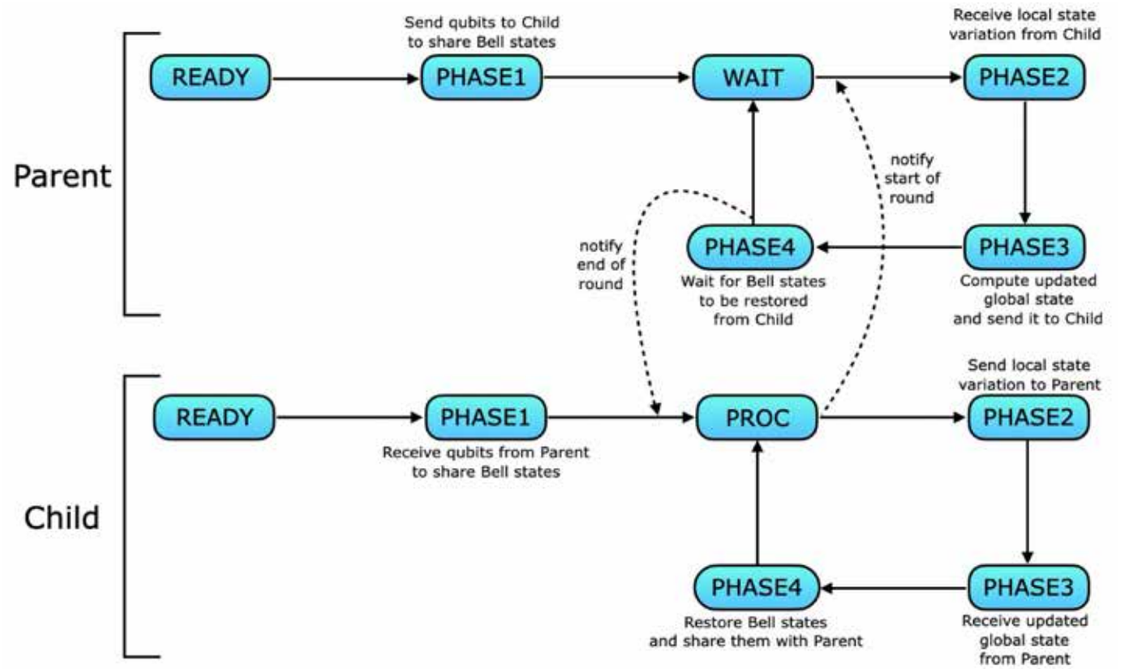
Table 1
Depth of different quantum circuits compiled with ChainSwap and IBM Qiskit's compilers

In practice, this is quite unlikely. ChainSwap produces circuits whose depth is generally very good, and in some cases is ideal.

Enhancing distributed functional monitoring with quantum protocols

Scalability concerns are motivating distributed quantum computing architectures, and experimental efforts have demonstrated some of the building blocks for such a design [VanMeter2016].

With the network and communications functionalities provided by the



1
QGM protocol: state machines of parent and child nodes

Quantum Internet [Wehner2018], remote quantum processing units can communicate and cooperate for executing computational tasks that each NISQ device cannot handle by itself.

The main idea of the Quantum Internet is to enable quantum communication between any two points on Earth, in synergy with the "classical" Internet, in order to achieve unmatched capabilities, as well as levels of resiliency and trustworthiness that are impossible by using only classical information.

Over long distances, the primary method of operating the Quantum Internet is to leverage optical networks (re-using existing optical fiber) and photon-based qubits.

In a joint work with Mattia Pizzoni and Stefano Carretta [Amoretti2019], we proposed the quantum geometric monitoring (QGM) protocol to solve threshold monitoring problems, where N players are located at different sites, each observing a stream of items and communicating with one coordinator, whose goal is to know when a function of the union of the streams exceeds a given threshold.

QGM enhances the classical geometric monitoring (GM) protocol [Giatrakos2016] with quantum communication and entanglement.

An entangled state is a special state of a group of qubits, such that the state of each qubit cannot be described independently of the state of the others. For example, Bell states are maximally entangled states of two qubits.

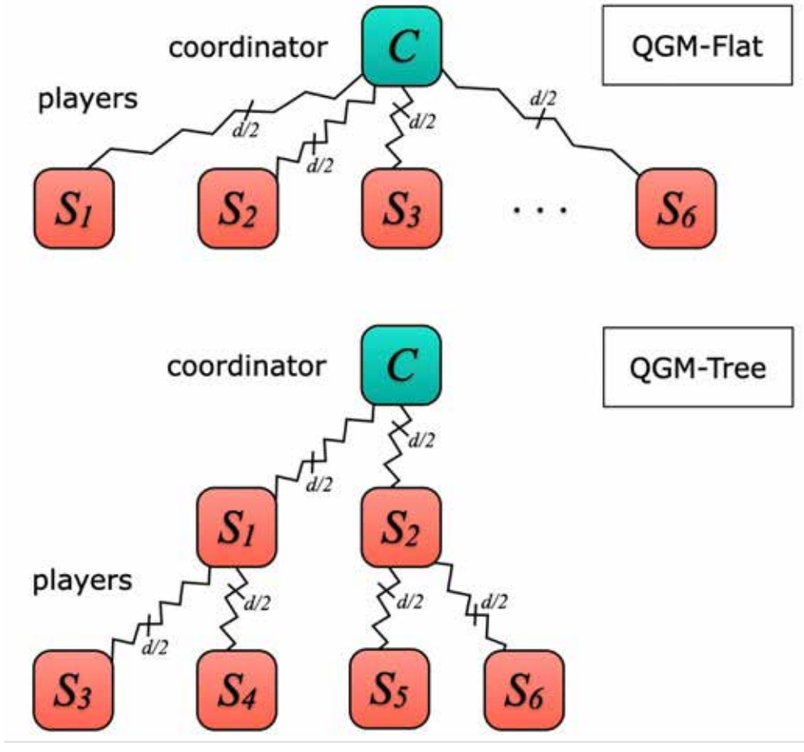
In QGM, Bell states are used to encode bit pairs and the supporting qubits are moved back and forth between the coordinator and the N players. The QGM protocol leverages the special properties of Bell states to reduce the communication cost, with respect to the GM protocol.

Generally speaking, the QGM protocol defines two roles: Parent and Child (Figure 1).

Then, there are two specializations of QGM, namely QGM-Flat, where the coordinator interacts with all the N players, and QGM-Tree, where the N players assume a tree structure (Figure 2).

In QGM-flat, the coordinator is the Parent and the N players are its Children. In QGM-Tree, the N players are both Children and Parents (with the exception of those corresponding to the leaves of the tree, which are just Children).

We implemented the QGM protocol with SimulaQron [Dahlberg2019], a



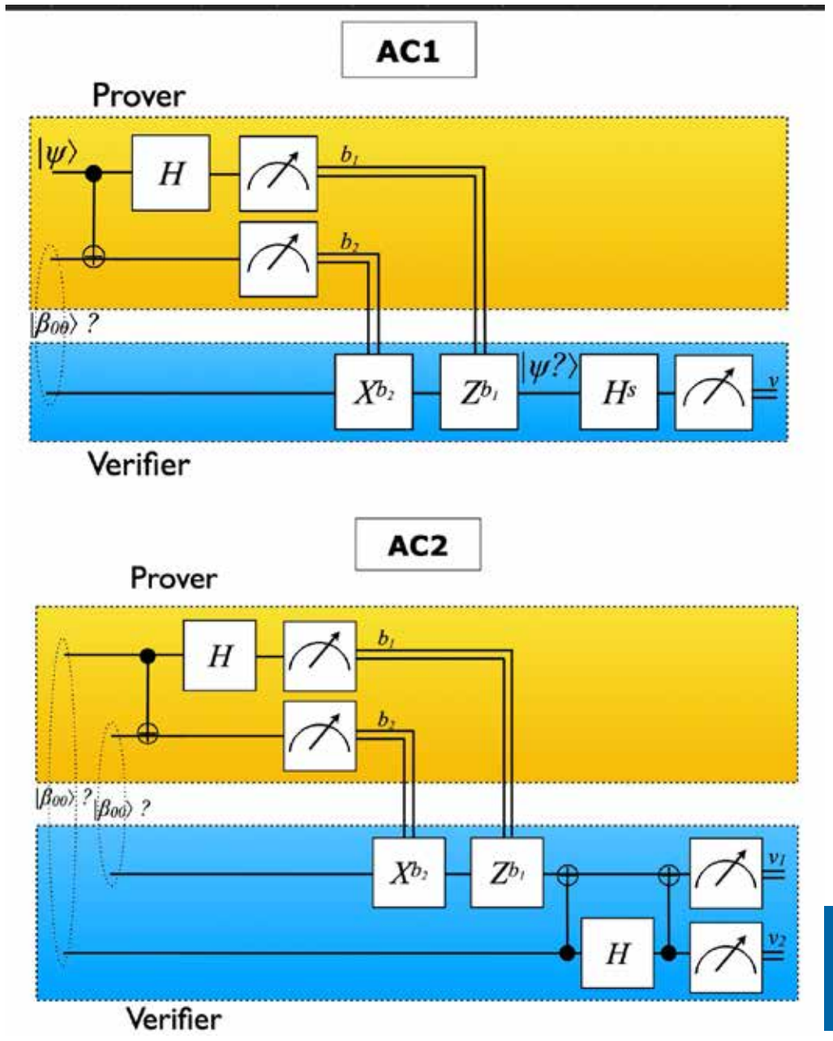
2
Examples of QGM system configurations for solving the threshold monitoring problem

Python library for the development and simulation of quantum networking applications.
Simulation results confirmed that the average communication cost in QGM-based systems is lower than in GM-based ones, with the same error rate.

Entanglement verification in quantum networks with tampered nodes

In general, entanglement is a precious resource in quantum networks.

Entangled states exhibit correlations that have no classical analog and may be used, e.g., to solve leader election problems, to perform distributed computing tasks, to share secrets, or to perform remote synchronization of clocks.



3
Quantum circuits of the AC1 and AC2 protocols

Recently, in a joint work with Stefano Carretta [Amoretti2020], we proposed two protocols for entanglement verification across the quantum memories of any two nodes of a quantum network.

The proposed protocols (denoted as AC1 and AC2) cope with the highly disruptive attack scenario where an attacker physically captures a node and takes full control of its operations. Interacting with the local quantum memory, the attacker reconfigures the states of the qubits (e.g., breaking entangled states shared with other nodes, by measuring local qubits) either to make a denial-of-service attack or to reprogram the node to a behavior in accordance with her own plans.

Both AC1 and AC2 rely on local operations and classical communication (LOCC), with simple quantum circuits characterized by only a few H, Z, X and CNOT quantum gates (Figure 3). The execution of the protocols requires that some of the Bell states $|\beta_{00}\rangle$ shared by the Verifier and the Prover are sacrificed. Both protocols are randomized, reason why the Prover, challenged by the Verifier, cannot trick.

We proved that AC1 is $(3/4)^m$-robust on any set of m Bell states sacrificed by the Verifier and the Prover, assuming that the Prover is controlled by an attacker that performs measurements either in the computational or diagonal basis. Moreover, we proved that AC2 is $(3/8)^m$-robust on any set of 2m Bell states sacrificed by the Verifier and the Prover, with the same assumption as above.

Here, ε-robustness means that the probability that the protocol aborts is at most ⍰. Furthermore, by means of simulations, we observed that the probability to detect the attacker in one round of the AC2 protocol, is greater than or equal to 1/2 for any possible choice of the measurement basis by the attacker.

Conclusions

Our current research on quantum compilers follows two main directions. On the one hand, we need to take into account not only the architecture of the hardware but also its noise profile.

On the other hand, we are working on highly innovative quantum compilers for mapping any quantum algorithm to any distributed quantum computing architecture, in order to achieve high-quality distributed quantum computations.

Regarding QGM, we plan to integrate complementary protocols, such as quantum leader election ones, in order to cope with dynamic scenarios where the role of coordinator may not be assigned in advance.

Finally, we will investigate the possibility to extend our entanglement verification protocols to quantum systems that involve more than two qubits, to cope for example with GHZ states, W states and graph states ■

References

1. [QSManifesto] Quantum Software EU Platform, Quantum Software Manifesto (2017)
2. [QIS] Quantum Software, University of Parma, http://www.qis.unipr.it/quantumsoftware.html
3. [Preskill2018] Preskill, J.: Quantum Computing in the NISQ era and beyond. Quantum 2(79) (2018)
4. [Botea2018] Botea, A., Kishimoto, A., Marinescu, R.: On the Complexity of Quantum Circuit Compilation. The Eleventh International Symposium on Combinatorial Search (SOCS 2018) (2018)
5. [Zulehner2019] Zulehner, A., Paler, A., Wille, R.: An ecient methodology for mapping quantum circuits to the IBM QX architectures. IEEE Trans. on CAD of Integrated Circuits and Systems 38(7), 1226-1236 (2019)
6. [Hart1968] Hart, P. E., Nilsson, N. J. and Raphael, B.: A formal basis for the heuristic determination of minimum cost paths. IEEE Transactions on Systems Science and Cybernetics, vol. 4, no. 2, pp. 100–107 (1968)
7. [Li2019] Li, G., Ding, Y., Xie, Y.: Tackling the qubit mapping problem for NISQ-era quantum devices. Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS '19, pp. 1001-1014 (2019)
8. [Ferrari2018] Ferrari, D., Amoretti, M., Efficient and effective quantum compiling for entanglement-based machine learning on IBM Q devices. International Journal of Quantum Information 16(08), 1840006 (2018)
9. [Ferrari2019] Ferrari, D., Tavernelli, I., Amoretti, M., Efficient Quantum Compiling for Quantum Chemistry Simulation on IBM Q. 1st European Quantum Technology Conference (EQTC), Grenoble, France (2019)
10. [VanMeter2016] Van Meter, R., Devitt, S.J.: The Path to Scalable Distributed Quantum Computing. Computer 49(9), pp. 31-42 (2016)
11. [Wehner2018] Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: A vision for the road ahead. Science 362(6412) (2018)
12. [Amoretti2019] Amoretti, M., Pizzoni, M., Carretta, S: Enhancing distributed functional monitoring with quantum protocols. Quantum Information Processing 18(21), 371 (2019)
13. [Giatrakos2016] Giatrakos, N., Deligiannakis, A., Garofalakis, M.: Scalable approximate query tracking over highly distributed data streams. ACM SIGMOD ‘16. ACM (2016)
14. [Dahlberg2019] Dahlberg, A.,Wehner, S.: Simulaqron—A simulator for developing quantum internet software. Quantum Science and Technology 4, 015001 (2019)
15. [Amoretti2020] Amoretti, M., Carretta, S.: Entanglement Verification in Quantum Networks With Tampered Nodes. IEEE Journal on Selected Areas in Communications 38 (3), pp. 598-604 (2020)

Michele Amoretti *michele.amoretti@unipr.it*

Professore Associato presso il Dipartimento di Ingegneria e Architettura dell’Università di Parma, dove insegna "High Performance Computing" (con un modulo di “Quantum Computing”) e "Sistemi Orientati ad Internet". Nel 2013 è stato Visiting Researcher presso il LIG Lab, a Grenoble, Francia.
E’ autore di oltre 100 articoli di ricerca su riviste internazionali, atti di conferenze e libri. Si occupa di algoritmi paralleli e distribuiti, per computer classici e quantistici. Contribuisce all’iniziativa Quantum Information Science dell’Università di Parma, guidando il gruppo di ricerca sul Quantum Software (http://www.qis.unipr.it/quantumsoftware.html) ■

QUANTUM COMPUTING E HPC IN EUROPA

Daniele Ottaviani

Da qualche anno, la comunità HPC è chiamata a risolvere una sfida molto difficile. Se da una parte la crescente domanda di risorse computazionali di alto livello da parte di un mondo sempre più digitalizzato è ben compensata dalle altrettanto avanzate competenze di coloro che si occupano di High Performance Computing, dall'altra c'è l'annoso problema dell'evoluzione dei supercalcolatori. Da qualche anno si sta assistendo ad un forte rallentamento nell'evoluzione dei computer classici: l'aumento di potenza si è slegato dal semplice aumento di prestazioni del processore, il fattore discriminante è sempre di più diventato l'utilizzo di più processori in parallelo che collaborano con acceleratori esterni. Il Quantum Computing è un concetto rivoluzionario per il calcolo ad alte prestazioni: si basa sulla realizzazione di un nuovo tipo di calcolatore in grado di sfruttare le leggi della meccanica quantistica per aumentare enormemente la propria potenza di calcolo. Anche se ancora in stato prototipale, questa nuova tecnologia sta già attirando l'attenzione della comunità HPC, che la vede come una possibile soluzione al problema dell'evoluzione dei computer attuali. In questo articolo, dopo avervi brevemente spiegato i concetti di HPC e Quantum Computing, parlerò dello stretto rapporto tra le due tecnologie e l'importanza che esse stesse stanno sempre più acquisendo in Italia e in Europa.

Introduzione

Con il termine High Performance Computing (HPC) si intende l'insieme di tecnologie necessarie per l'assemblaggio di supercomputer e per la loro programmazione, per la quale vengono sfruttate avanzate tecniche di parallelizzazione.

Per supercomputer, invece, si intende un calcolatore con una potenza di calcolo di diversi ordini maggiore rispetto ai computer che normalmente possiamo trovare sul mercato.

Al fine di comprendere meglio quest'ultima informazione, spieghiamo come viene misurata la potenza di un computer: per quantificarla normalmente si utilizza il concetto di FLOPS ("Floating Point Operations Per Second"), unità di misura che registra il numero di operazioni in virgola mobile che un computer può effettuare nell'arco di un secondo; ad esempio, un computer che monta un processore di mercato di fascia intermedia come un Intel(R) Core(TM) i5-5675R CPU @ 3.10GHz può sviluppare una potenza di calcolo media pari a 25.45 GFLOPS (25.45 miliardi di operazioni in virgola mobile al secondo), mentre una macchina equipaggiata con un potente AMD Ryzen Threadripper 3960X 24-Core Processor può arrivare anche a 10 volte tanto (254 GFLOPS).

I supercomputer, per essere definiti tali, devono avere potenze di calcolo superiori di qualche ordine di grandezza rispetto a quelle dei comuni computers.

Sfogliando la classifica "Top500"[1], la lista periodicamente aggiornata (e pubblicamente disponibile online) che riporta la potenza di calcolo di tutti i supercomputer del mondo, si legge che ad esempio Summit, il primo classificato, ha una potenza di calcolo media pari a circa 150 PFLOPS, ovvero circa 150 milioni di miliardi di operazioni al secondo. Per poter raggiungere tali impressionanti velocità ogni macchina ha bisogno di utilizzare tutto quello che l'attuale tecnologia mette a disposizione per aumentarne la potenza.

Oltre ad aver bisogno di moltissimi processori (si parla, in media, di milioni di cores per ogni macchina, suddivisi in svariati nodi), esso deve essere in grado di sfruttare efficientemente anche tutti i validi acceleratori disponibili sul mercato, come le Graphic Processing Units (GPU).
Inoltre, ha bisogno di girare codice scritto utilizzando particolari accorgimenti, che normalmente non rientrano nella pura implementazione di un algoritmo: i programmi scritti per essere eseguiti da un supercomputer devono essere in grado di suddividere e orchestrare il lavoro tra i moltissimi processori, oltre ad essere in grado di accedere e sfruttare eventuali acceleratori presenti sulla macchina, in modo da poter veramente utilizzare appieno tutta la potenza di calcolo disponibile.

Il ruolo di un programmatore HPC è proprio questo, permettere ad un codice di sfruttare al meglio la potenza delle macchine, in modo da riuscire a compiere i propri calcoli nel più breve tempo possibile. Negli ultimi 70 anni l'HPC è diventato sempre più parte integrante delle realtà aziendali e universitarie del mondo intero: l'introduzione del calcolo parallelo ha reso possibile l'esecuzione di simulazioni che fino a poco tempo prima risultavano semplicemente impensabili.

Oggi l'HPC è una realtà insostituibile nel panorama scientifico mondiale; oltre alla presenza sul terreno mondiale di diversi centri di supercalcolo a livello nazionale anche moltissime aziende private hanno istituito dei rami di ricerca HPC. Basti pensare, come esempio, alla gigantesca mole di ore calcolo utilizzate dalle case farmaceutiche (e ancora in utilizzo) per cercare una cura contro il coronavirus.

La simulazione computazionale dell'interazione tra molecole, infatti, oltre a rappresentare uno strumento ormai insostituibile in mano alla ricerca medica rappresenta anche un problema computazionale molto difficile da risolvere in tempi sufficientemente rapidi.

1
Il supercomputer "Marconi", primo computer pubblico italiano e cuore pulsante dell'HPC in CINECA

L'HPC in Italia e la legge di Moore

In Italia l'HPC è gestito da diversi centri di supercalcolo e da molte aziende, esattamente come accade nel resto del mondo. In particolare, vale la pena menzionare CINECA[2], consorzio inter-universitario italiano con sede nel bolognese, che oltre ad occuparsi di programmazione HPC gestisce e mantiene il più potente supercomputer pubblico italiano, Marconi (vedi figura 1), recentemente aggiornato con partizioni dotate di NVIDIA Volta V100GPUs[3].

CINECA si occupa di fornire soluzioni HPC alle industrie e alle università italiane da più di 50 anni, offrendo ore calcolo su supercomputer aggiornati periodicamente (la cui potenza è sempre stata testimoniata dalla costante presenza delle macchine CINECA nei primi posti nella lista Top500) e personale altamente qualificato, in grado di guidare l'utente sia nella conversione del suo codice, ottimizzandolo per l'utilizzo sulle macchine HPC, sia di mantenere un supporto attivo per tutta la durata dei progetti intrapresi.

Sin dalla sua fondazione, il consorzio CINECA si è sempre impegnato per fornire ai suoi utenti le soluzioni HPC più all'avanguardia, collaborando sia con lo Stato Italiano sia con la Comunità Europea, partecipando attivamente a tutte le iniziative su tema. Sappiamo bene che per continuare a soddisfare

le esigenze computazionali della comunità HPC è sempre più necessario rivolgere lo sguardo alle nuove tecnologie che in qualche modo riescono ad aumentare la potenza di calcolo degli attuali supercalcolatori, accelerandone le prestazioni.

Tale accorgimento, una volta praticamente impensabile, è ormai diventato necessario: nel corso degli anni, infatti, si è assistito ad un forte rallentamento dell'aumento della potenza computazionale prodotta dall'industria dei supercomputer.

Qualche decina di anni fa il mondo dell'HPC poteva fare affidamento sulle previsioni di crescita conosciute con il nome di "legge di Moore"[4]: tale legge affermava, empiricamente, che la potenza di calcolo dei computer sarebbe raddoppiata ogni anno e mezzo.

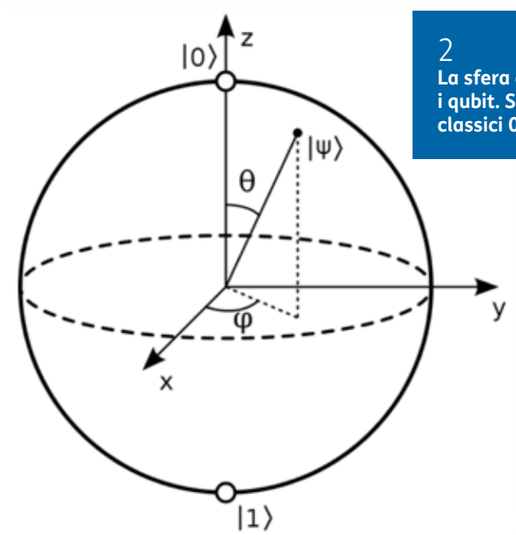
Le previsioni di Moore si rivelarono esatte per un lungo periodo dell'evoluzione dei calcolatori classici.

All'inizio del nuovo millennio, però, le maggiori case produttrici di processori si resero conto di aver raggiunto un limite fisico nella realizzazione di CPU sempre più potenti.

Tale limite, che riguarda la miniaturizzazione dei circuiti, risulta ancora oggi molto difficile da superare; questo fenomeno ha sancito un inevitabile rallentamento nell'evoluzione della potenza computazionale, rendendo obsoleta la legge di Moore.

Per ovviare ai limiti di costruzione delle CPU, vennero prese in considerazione diverse idee. Inizialmente nacque il concetto di multicore e di calcolo parallelo: ovvero cercare di superare il limite fisico imposto alla realizzazione di nuove CPU creando dei sistemi di elaborazione composti da molti processori che lavorano insieme.

Questo approccio, ancora oggi utilizzato, nasce nei primi anni del 2000: esso inizialmente riuscì a compensare la perdita di potenza delle singole CPU, trainando ancora una volta il grafico della potenza computazionale a disposizione dell'HPC verso l'alto, senza però riuscire a dare nuova vita alla legge di Moore.



2
La sfera di Bloch, "mondo matematico" dove vivono i qubit. Si noti come i poli siano costituiti dagli stati classici 0 e 1

Il Quantum Computing

La nascita dell'idea di computer quantistico è attribuita ad una famosa frase del professor Feynman, fisico statunitense, il quale nel 1982 disse:
"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy".

In sostanza, Feynman immaginava un nuovo concetto di calcolatore[5], in grado di simulare le interazioni fisiche tra particelle manipolando unità logiche di informazione di base quantistiche, anziché macroscopiche.

Il bit, l'unità logica di base del computer classico, costituito sostanzialmente da un flusso di corrente che lo rende acceso o spento, doveva essere sostituito con un'entità atomica in grado di manifestare stati normalmente impossibili, "vie di mezzo" tra l'acceso e lo spento, generabili grazie allo sfruttamento del principio di sovrapposizione quantistica. La caratteristica chiave di questa nuova unità logica di base, detta qubit, è proprio quella di poter assumere infiniti stati di sovrapposizione tra l'acceso e lo spento, rendendo possibili operazioni intrinsecamente parallele irrealizzabili utilizzando le architetture dei computer classici (vedi figura 2).

Nel 1982 l'idea di Feynman era un'idea destinata a rimanere sulla carta: molti scienziati, però, animati da uno spirito pionieristico e visionario, credettero sin da subito nel nuovo futuristico calcolatore, dando vita molto precocemente alla branca che oggi è conosciuta come Quantum Computing.

È proprio lo studio precoce del quantum computing che ha attirato sin da subito l'attenzione di moltissimi scienziati: la possibilità di poter sfruttare a proprio vantaggio i comportamenti quantistici dei qubit si dimostrò un potentissimo mezzo a disposizione degli scienziati.

Ci si rese immediatamente conto che gli algoritmi scritti con questo nuovo approccio, spesso e volentieri, superavano di gran lunga le controparti classiche, dando vita a nuovi metodi molto più efficienti e rapidi.
Tutto il lavoro svolto prima della comparsa dei primi computer quantistici ha generato una gran moltitudine di algoritmi quantistici pronti per essere usati, che aspettano solo un computer sufficientemente evoluto per poterli implementare.

I primi prototipi funzionanti di computer quantistico comparvero nei primi anni 2000 ma ci vollero almeno 10 anni per realizzare dei calcolatori effettivamente programmabili ed utilizzabili. Nel frattempo, molte grandi case produttrici come IBM, Google e Microsoft, deviarono parte della loro ricerca scientifica per la realizzazione di computer quantistici sempre più potenti; contemporaneamente, in giro per il mondo nacquero start-up con lo stesso scopo, come D-Wave o Rigetti.

Ad oggi, inizio 2020, possiamo affermare che lo stato dell'arte dei computer quantistici è un passo sopra al livello di prototipo, ma non ancora sufficientemente evoluto per rappresentare una vera e propria rivoluzione nel campo dell'HPC.

Le ridotte dimensioni dei chipset e le tecnologie di realizzazione ancora un po' acerbe non permettono alle macchine attualmente disponibili sul mercato di implementare i complessi algoritmi pensati anni prima al pieno delle loro potenzialità, seppur siano perfettamente in grado di dimostrare di poterlo fare in piccolo (al massimo delle loro attuali capacità computazionali).

Eppure, come dimostrato recentemente da un esperimento condotto da Google, è già possibile realizzare computer quantistici in grado di dimostrare la cosidetta "supre-

mazia quantistica", seppur limitatamente ad uno specifico algoritmo di campionamento. Secondo alcune proiezioni fatte da tecnici e scienziati vicini all'argomento, potremo osservare nuovamente evidenze di supremazia quantistica applicata ad algoritmi di uso comune tra poco, ovvero quando i computer quantistici avranno rotto la barriera dei 100 qubit.

Si stima, infatti, che superata tale soglia i computer saranno in grado di implementare un'intera categoria di algoritmi quantistici, soprattutto riguardanti simulazioni chimiche, cominciando ad ottenere risultati ineguagliabili dai supercomputer attuali.

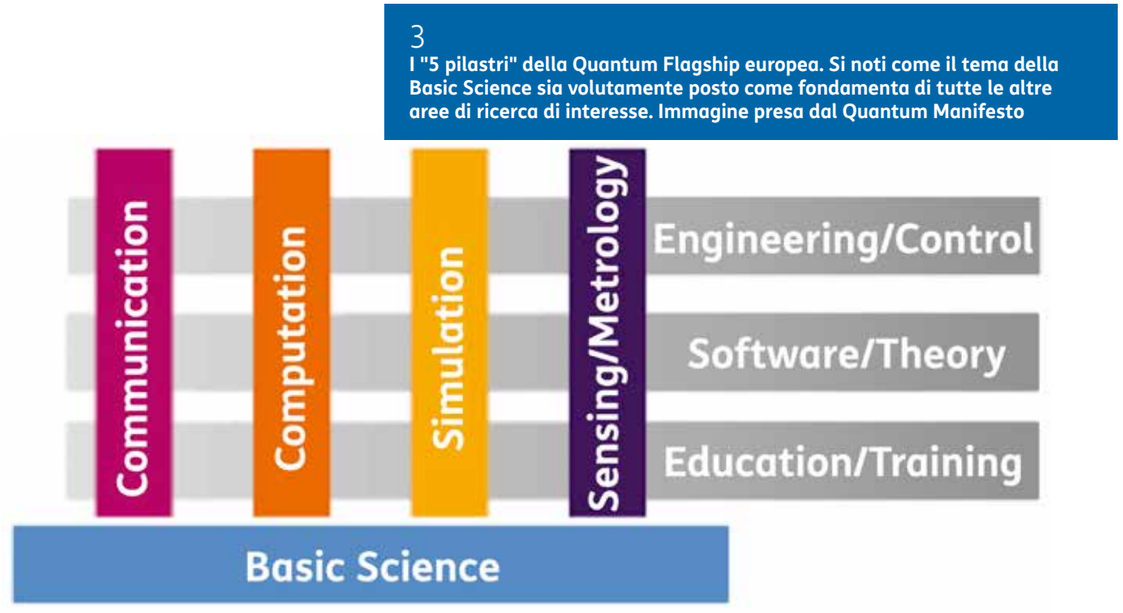
Anche se la tecnologia quantistica attuale è ancora lontana dal computer universale, è pericoloso e controproducente aspettare di vederla evolvere per iniziare a tenerla in considerazione.

Questo per diversi motivi: come prima cosa, le conoscenze per utilizzare un computer di questa nuova generazione sono tutt'altro che scontate; i computer quantistici seguono logiche completamente diverse, per poterli utilizzare al meglio è necessario conoscere il quantum computing.

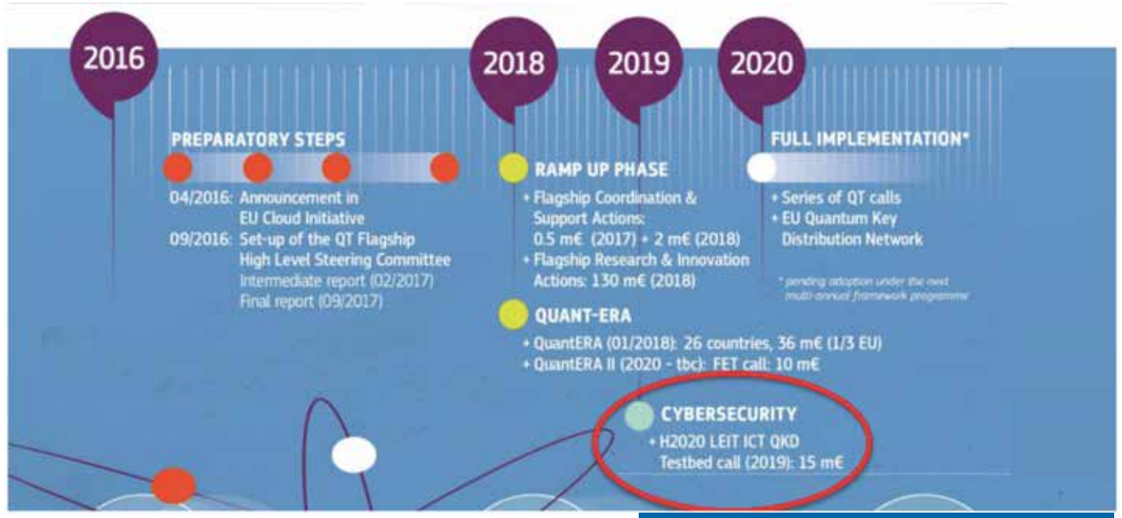
In secondo luogo, anche al livello attuale i computer quantistici potranno presto essere sfruttati per migliorare la potenza computazionale dei supercomputer attuali.

Al momento, infatti, stiamo per entrare nella fase dei "NISQ" Computers[6]: per NISQ Computers (Noisy Intermediate-Scale Quantum), si intendono computer quantistici di modeste dimensioni, con tecnologie di realizzazione qubits non proprio perfette, ma comunque in grado di compiere calcoli molto complessi per computer digitali, anche se limitati dalla rumorosità e dalle dimensioni del chipset.

Menti lungimiranti, hanno già previsto la possibilità di utilizzare



3
I "5 pilastri" della Quantum Flagship europea. Si noti come il tema della Basic Science sia volutamente posto come fondamenta di tutte le altre aree di ricerca di interesse. Immagine presa dal Quantum Manifesto



4
Timeline delle fasi della Quantum Flagship

i computer quantistici di prossima generazione come acceleratori per i supercomputer, affiancando la QPU (Quantum Processing Unit) alle già presenti CPU e GPU al fine di ottimizzare le prestazioni totali.

HPC e Quantum Computing in Europa

Anche se lo stato dell'arte delle tecnologie quantistiche non permette ancora applicazioni a livello industriale, il loro immenso potenziale e la necessità di familiarizzare sin da subito con quella che è a tutti gli effetti una rivoluzione nel campo dell'HPC hanno spinto l'Europa, al pari di molti altri governi mondiali, ad intraprendere sin da subito ingenti azioni di finanziamento.

Il 17 maggio 2016 è stato annunciato dalla comunità europea nell'ambito del Programma Quadro di ricerca Horizon 2020 il lancio della nuova FET Flagship in Quantum Technologies[7], ovvero un programma di ricerca decennale finanziato con 1.3 miliardi di euro che vede il coinvolgimento di tutti gli Stati Membri al fine di creare un network europeo quantistico in grado di padroneggiare ogni aspetto delle nuove tecnologie emergenti, dalla loro costruzione al loro utilizzo.

Nell'ambito della Quantum Flagship, partita ufficialmente due anni dopo, il 29 ottobre 2018 (in occasione di un congresso tenutosi a Vienna), sono stati finanziati moltissimi progetti.

Gli autori del Quantum Manifesto[8], ovvero il whitepaper che ha dato il via all'iniziativa della Quantum Flagship, identificano 5 aree di ricerca "Quantum" di interesse per la comunità europea: Communication, Computation, Simulation, Metrology e Basic Science.

Quest'ultima, che racchiude lo sviluppo di tutta la matematica che sta alla base di qualsiasi implementazione, è vista come un pila-

stro fondamentale su cui tutte le altre scienze si basano (vedi figura 3).
Dopo una prima fase preliminare di due anni (2016-2018), La "ramp-up phase" della Quantum Flagship (2018-2020) ha previsto un investimento iniziale di 132 milioni di euro (Flagship Research and Innovation Actions) da suddividere per circa 20 progetti approvati (su circa 140 valutati).

I 20 progetti approvati sono così suddivisi: 7 progetti di ricerca di base, 4 nell'ambito dei sensori quantistici (e metrologia), 4 progetti sulla comunicazione quantistica, 2 per la simulazione quantistica ed infine 2 nell'ambito del quantum computing.

Ora stiamo per entrare nella cosidetta "Full Implementation Phase", dove si prevede il finanziamento di ulteriori progetti operativi, sfruttando la maggiore potenza computazionale quantistica a disposizione (in particolare la realizzazione dei primi computer quantistici NISQ, in grado di poter essere davvero affiancati a dei supercomputer per svolgere in particolare simulazioni di chimica computazionale in maniera più efficiente rispetto ai calcolatori classici).

Il progetto della Quantum Flagship fa parte di una visione di insieme più grande, che da qualche anno la comunità europea sta cercando di perseguire. Uno dei grandi problemi che l'Europa sta cercando di risolvere nel campo dell'HPC è quello dell'indipendenza tecnologia: se da una parte è vero che la comunità HPC europea può contare su diversi supercomputer e su una ampia schiera di centri di calcolo ben nutriti di competenze specifiche, è anche vero che la costruzione dei supercalcolatori è spesso affidata ad aziende extraeuropee, in particolare cinesi o americane.

La fondazione "EuroHPC Joint Undertaking"[9], divenuta operativa il 6 novembre 2018, nasce come azione di partnership tra soggetti pubblici e privati, raccogliendo risorse dagli Stati Membri e dagli stakeholders impegnati nell'ambito del programma europeo Horizon 2020 al fine di realizzare un'infrastruttura di high performance computing completamente europea.

La fondazione vuole approfittare della corsa all'Exascale (ovvero la corsa alla realizzazione di un supercomputer in grado di raggiungere una potenza computazionale misurabile in ExaFLOPS) per finanziare progetti europei in grado di realizzare tali tecnologie. Già nel giugno del 2019 EuroHPC ha selezionato 8 siti adeguati per accogliere un supercomputer "pre-exascale", ovvero la generazione immediatamente precedente ai computer exascale; tra i siti selezionati vale la pena menzionare il sito italiano, identificato nel CINECA, che gestirà un supercomputer da 240 milioni di euro chiamato Leonardo.

Quest'ultimo, una volta connesso con gli altri supercomputer della rete, darà vita alla base del network HPC europeo, il quale verrà poi man mano implementato con ulteriori infrastrutture.

È proprio in quest'ottica che il futuro dell'HPC europeo e il futuro delle tecnologie quantistiche si intersecano: la rete europea costituita dagli otto supercomputer pre-exascale potrà disporre, nel prossimo futuro, anche di risorse computazionali quantistiche da integrare alle proprie.

Altro obiettivo della comunità europea è anche quello di estendere il concetto di indipendenza tecnologica anche alla nascente industria della costruzione di computer quantistici: per questo si vuole si da subito includere la realizzazione di una rete di computer quantistici sparsi per l'europa in connessione alla rete HPC.

Il progetto, che fa parte della call EuroHPC 2020, precisamente denominato "EuroHPC-2020-01-b: Pilot on quantum simulator", partirà già quest'anno: la call prevede l'installazione di un primo computer quantistico in un centro di calcolo europeo, la sua connessione ad un supercomputer di ultima generazione e l'istituzione di una task force di esperti in grado di gestire la nuova rete e di formare altro personale a farlo.

In Italia il CINECA ha cominciato a monitorare l'evoluzione del nuovo panorama HPC mondiale in concomitanza con le iniziative europee, istituendo un team responsabile del monitoraggio e dello studio delle nuove tecnologie quantistiche.

Nel corso degli anni, dopo aver collaborato con industrie e università italiane su ricerche relative al quantum computing, il team di quantum computing del CINECA ha consolidato le proprie conoscenze sul tema, rendendo il centro di calcolo perfettamente allineato con gli sviluppi europei della nuova tecnologia.

Oltre ad aver fornito consulenza specialistica e supporto tecnico CINECA ha anche organizzato eventi di divulgazione annuale a tema "Quantum Computing and HPC", che hanno raccolto un grande successo in tutte le edizioni. Ormai la connessione tra quantum computing e HPC si sta facendo sempre più chiara agli occhi di tutta la comunità europea: conformemente alla sua missione nel campo dell'HPC, dal punto di vista quantum lo scopo del CINECA è quello di fornire mezzi, competenze e formazione per aiutare industrie e enti di ricerca italiani ad affrontare serenamente quest'imminente seconda rivoluzione quantistica ■

Bibliografia

1. https://www.top500.org/ Top500 list
2. https://www.cineca.it/ CINECA
3. http://www.hpc.cineca.it/content/hardware Infrastruttura HPC CINECA
4. Cramming more components onto integrated circuits Gordon E. Moore, Electronics, Volume 38, Number 8, April 19, 1965
5. Simulating physics with computers Richard P. Feynman International Journal of Theoretical Physics volume 21, pages467–488(1982)
6. Quantum Computing in the NISQ era and beyond John Preskill Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology, Pasadena CA 91125, USA 30 July 2018
7. Quantum Flagship https://qt.eu/
8. Quantum Manifesto Whitepaper https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf
9. EuroHPC JU website https://eurohpc-ju.europa.eu/

Daniele Ottaviani *d.ottaviani@cineca.it*

Matematico di formazione, sin dalla sua tesi magistrale si è appassionato alla modellistica matematica e alle sue applicazioni. Ha perfezionato i suoi studi con un Master di II livello in “Calcolo Scientifico”, dove ha approfondito l’High Performance Computing (HPC), e con un Ph.D. in “Matematica e Modelli”. Dal 2013 ha lavorato presso l’Osservatorio Astronomico di Roma “Monte Porzio Catone”, dove ha svolto il ruolo di assegnista di ricerca con mansioni relative alla realizzazione “from scratch” (dalla teorizzazione all’implementazione ottimizzata) di algoritmi matematici per il denoising di immagini astronomiche (prese, in particolare, dal telescopio Hubble). Dal 2018 lavora in CINECA come HPC Software Developer, con mansione speciale di monitoraggio attivo per le nascenti tecnologie quantum. Nel corso di questi ultimi due anni ha partecipato a diversi progetti relativi al quantum computing (di cui due diventati articoli scientifici), supportando università e aziende nelle loro ricerche di interesse nel campo ■