Quantum Technologies and Society

Pietro Massignan · Alejandra Valencia

December 2010

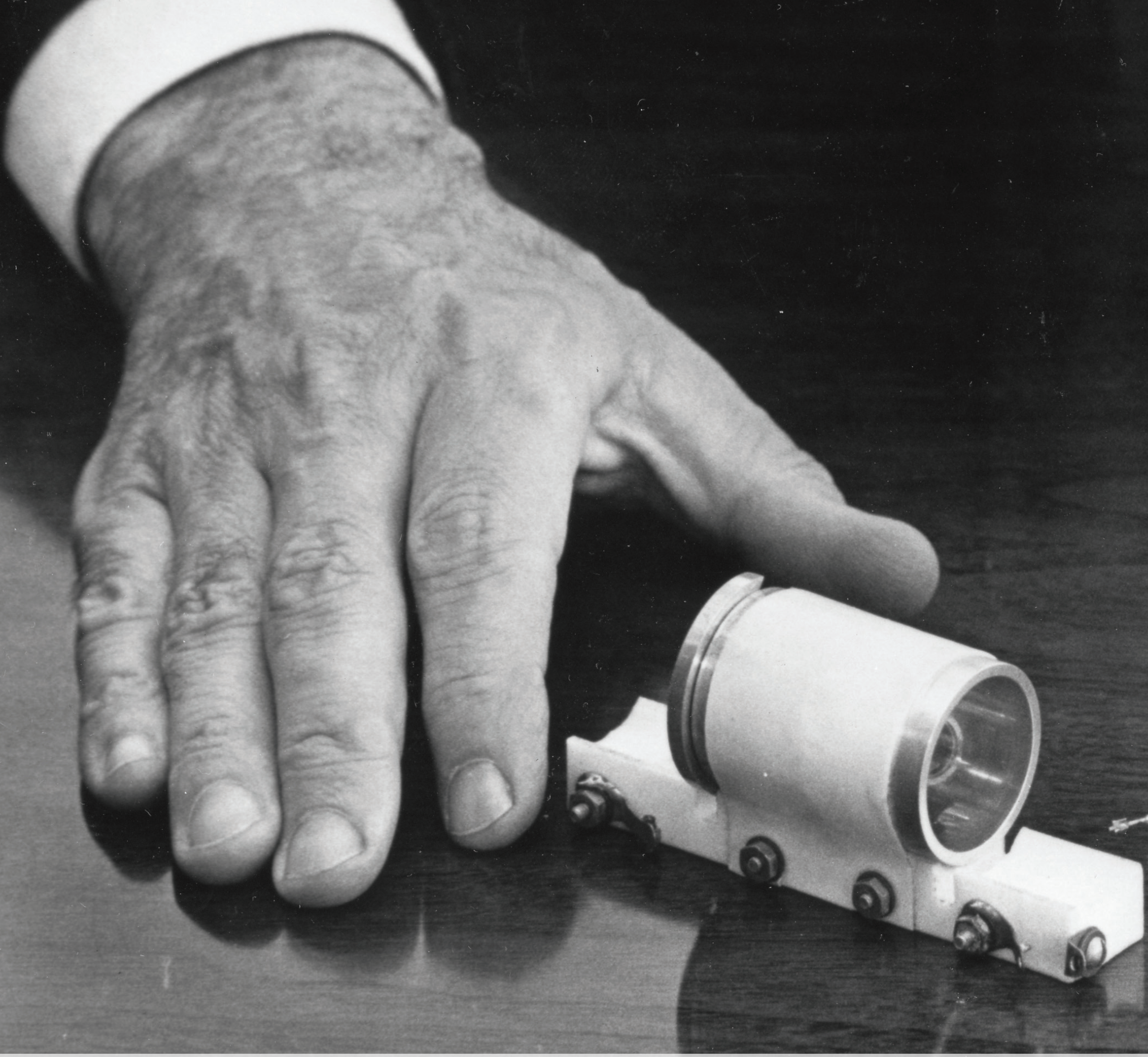
CX CatalunyaCaixa
Obra Social

Ignacio Cirac · CatalunyaCaixa
Chair at ICFO

Index

CatalunyaCaixa
Obra Social

1. Introduction

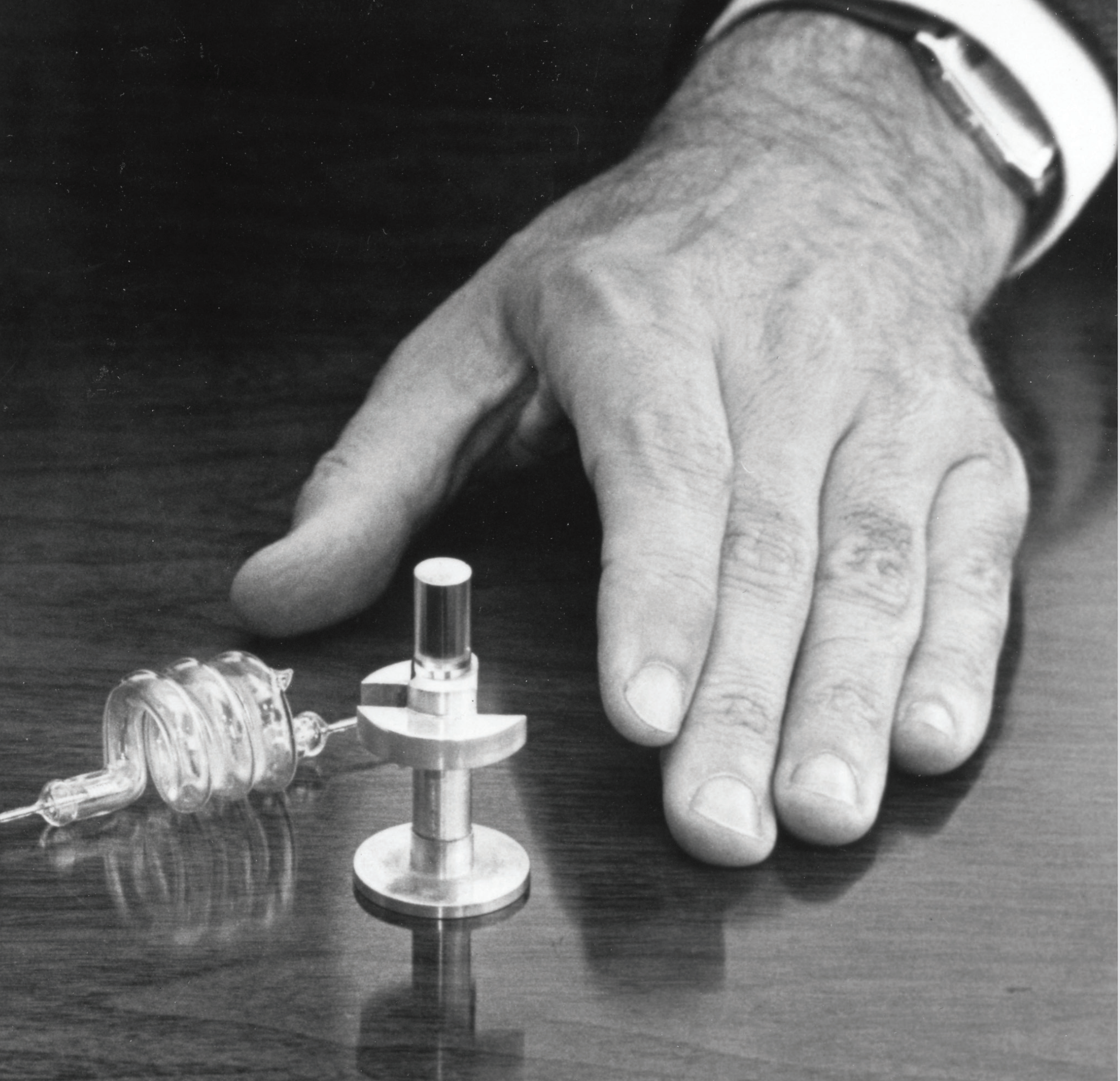


Maiman's first laser, disassembled

LASERFEST

CELEBRATING 50 YEARS OF LASER INNOVATION

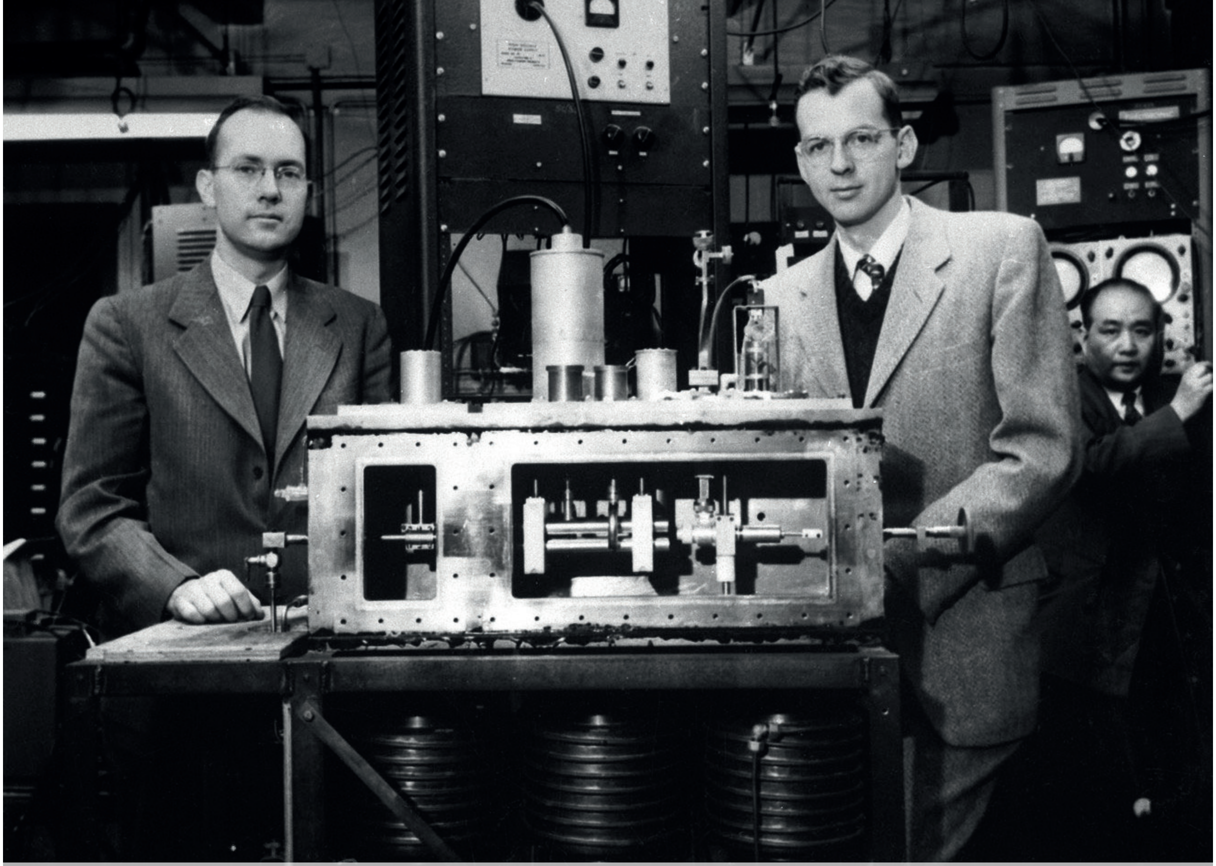
CatalunyaCaixa Obra Social



1. Introduction

When Theodore Maiman built the first **laser** in 1960, hardly anybody could foresee the huge impact this device would have on the lifestyle of the XXI century. A coworker of Maiman described the laser as a “solution searching for a problem”. However, not many years had to pass for the laser to solve a lot of those: in 1961 the first tumor retinal cancer treatment was performed; eight years later, just after the man landed on the moon, laser beams were used to measure the moon-earth distance with unprecedented precision; in 1977, the bar code scanner was introduced; and in 1982, the commercialization of compact disks brought a radical revolution in the way we listen to music and store our data.

Fifty years after its invention, we are constantly surrounded by lasers. The incredibly fast data transmission over the Internet is only possible thanks to the development of diode lasers and optical fibers. On the other hand, thanks to the widespread use of lasers in industry applications, it is almost impossible to think of a commercial product that is not touched by a laser in some way in its production stage. In our everyday life, we can find lasers in cd and dvd drives, barcode



Charles H. Townes (left), winner of the 1964 Nobel Prize for Physics, and associate James P. Gordon in 1955 with the first maser

scanners in shops and airports, laser pointers and lighting devices for entertainment purposes. More generally, lasers find applications in fields as varied as process control, health care, data storage and transmission, and in measuring and sensing tasks.

The theory of **quantum mechanics** was developed at the beginning of the XX century. In just a few years, it radically changed our understanding of Nature, and it led to a new way of looking at it. The basic principles of classical physics that described the physical world at the time had to be put aside, and a fundamentally new approach was adopted to describe Nature at a more fundamental level.

One of the basic and revolutionary principles of quantum mechanics is the assumption of a **corpuscular nature of light, matter, and energy**, and indeed the word “quantum” means “indivisible unit”. The invention of the laser would have been impossible without the deep understanding of this concept, brought to us by the study of quantum mechanics. A laser, which is an acronym for “laser amplification by stimulated emission of radiation”, represents a key example of how quantum mechanics and the technologies that derive from it are deeply affecting our society and reshaping our lifestyle. Another concept that had to be introduced and accepted is the one of **superposition**. According to this principle, a physical system can be in two physical states at the same time. As Schrödinger put it to stress the weirdness of the concept, the theory predicts that a cat can be at the same time dead and alive. Last but not least, an historically very controversial quantum concept that does not have analogous in classical physics is **entanglement**. Particles that are in an entangled state present particularly strong correlations, which survive even when the particles are separated by very long distances. The counter-intuitive character of entanglement has been studied thoroughly in 1935 by Einstein, Podolsky and Rosen. In their famous paper, named EPR after the initials of the authors, they questioned the completeness of quantum theory, since this allowed the existence of pairs of particles that could affect one another instantaneously. As a matter of fact, Einstein never really accepted the intrinsically mysterious nature of quantum theory.

The discussion about the existence of a “spooky action at a distance” (as Einstein referred to

Theodore H. Maiman of Hughes Aircraft Company showing a cube of synthetic ruby crystal, the material at the heart of the first laser

Quantum mechanics changed our vision of the world, by introducing principles that may seem weird and paradoxical at first sight

entanglement) was merely theoretical during almost 50 years. By the late 80´s, entanglement was demonstrated experimentally using the so-called “spontaneous parametric down-conversion”, a process which naturally creates pairs of entangled photons. Nowadays, research laboratories and enterprises around the world commonly rely on this type of source to perform front-edge research and produce goods that have already found their way into the market.

Quantum mechanics changed our vision of the world, by introducing principles that may seem weird and paradoxical at first sight. However, scientist and engineers are working hard on making these paradoxes useful by developing new applications. Emerging quantum technologies indeed allow us to go beyond the intrinsic limitations set by classical physics. As we will see in the following, quantum technologies already find natural applications in fields as diverse as health, alternative energies, material processing and personal devices, secure communications and environment. By means of such advances, quantum theory is helping us to produce faster, smaller, and intrinsically more secure and efficient devices.

CatalunyaCaixa
Obra Social

2. Quantum Metrology

The GPS signal comes from a constellation of satellites in permanent orbit around the Earth. The timing needed to emit a precise GPS signal is provided by ultrastable atomic clocks mounted on board of each of the satellites

Research at the quantum level allows us to determine various physical quantities with an incredible precision, and this is helping us to make enormous progresses in many fields like engineering, medicine and science. A familiar example may be the navigation system called GPS (Global Positioning System). GPS receivers are nowadays integrated in all sorts of portable devices, such as mobile phones and cameras, and these can locate and guide us with an incredible accuracy. Their precision, which is today of order of one meter, is even more remarkable if we think that the GPS signal comes from satellites orbiting at 20000km above the Earth's surface. This accuracy is only possible thanks to the presence of an **atomic clock** in each of the satellites forming the backbone of the GPS system. Time lapses are determined in these clocks by measuring the very stable oscillatory signal given by the energy difference between two quantum energy states of an atom.

The latest achievements in trapping and cooling of atoms and ions, together with the development of optical combs based on ultrafast pulsed lasers, yielded a new generation of atomic clocks characterized by an astonishing precision. State-of-the-art clocks, based on optical frequency-comb techniques, lose nowadays a second in 60 million years.

From a very fundamental point of view, quantum devices like atomic clocks allow us to investigate fascinating scientific concepts such as the nature of space, time, matter and energy. In particular, they open the possibility of testing to which extent physical laws are indeed constant. One question of extreme scientific interest is, for example, whether or not the value of fundamental physical quantities, e.g., the electron charge or the gravitational constant, are drifting over time or space.

From a very fundamental point of view, quantum devices like atomic clocks allow us to investigate fascinating scientific concepts such as the nature of space, time, matter and energy

On the more applied side, clocks and magnetometers, imaging devices and interferometers are some of the tools that are having a strong impact in technological breakthroughs. GPS receivers, network synchronization devices and analog-to-digital converters are a few examples of economically significant applications of precise clocks. An accurate timing is needed for example in network synchronization devices to precisely regulate the huge amount of data transiting over networks, while analog-to-digital converters are used in radars to measure the position and motion of distant objects. Better oscillators will allow smaller clock jitters, and will then improve the performances of these devices. Micro-fabrication techniques are available today to create miniaturized atomic clocks with characteristics well suited to general purpose industrial applications and portable devices.

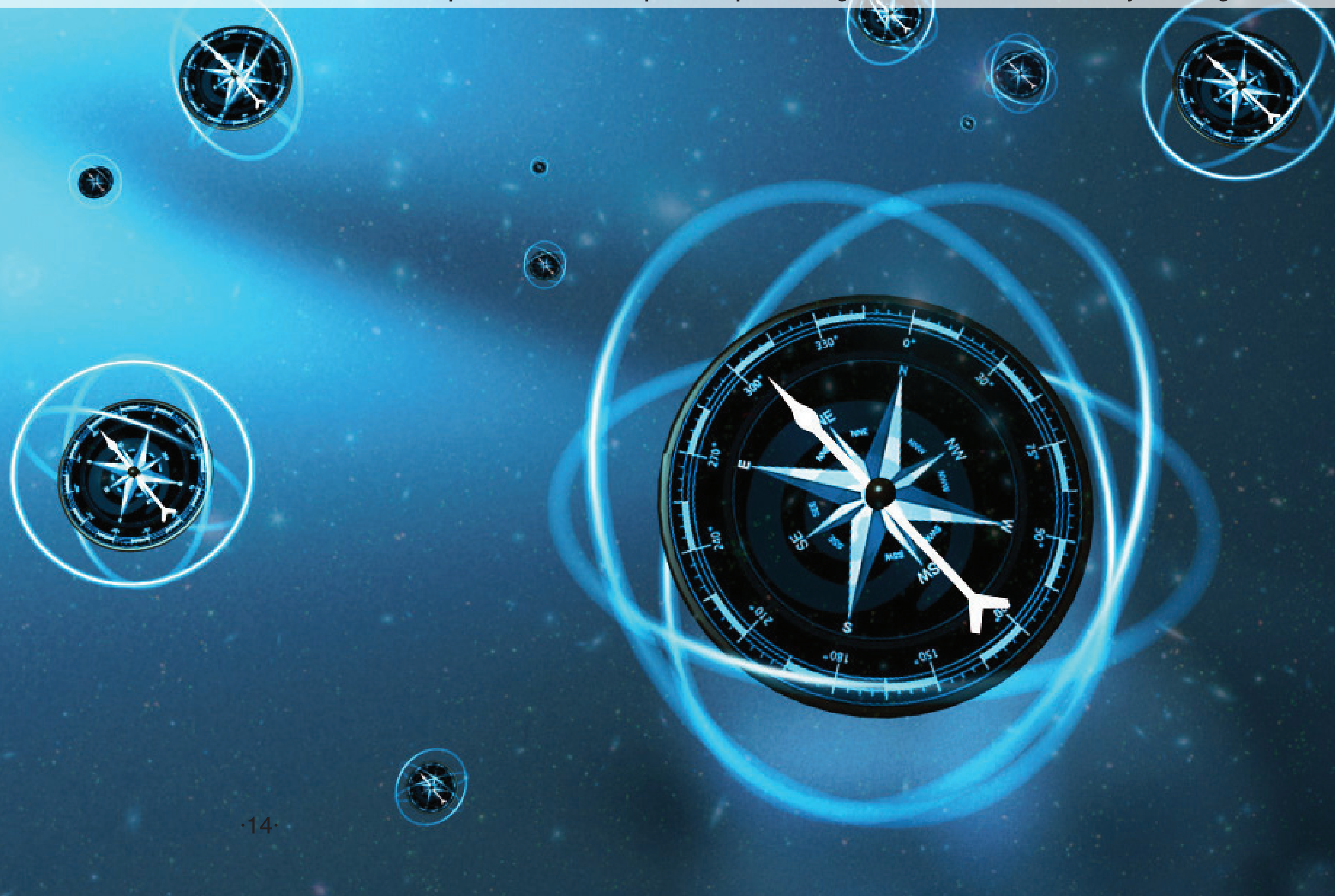
Various tasks of fundamental importance in health care and geophysical mapping, such as imaging of the human body or investigation of underground oil reservoirs, critically rely on the possibility of measuring weak magnetic fields with high accuracy. An instrument used to detect the strength and the direction of a magnetic field is called a **magnetometer**. Quantum mechanics forced us to accept another novel principle which has no analogue in classical physics: an intrinsic "spinning" must be associated to each fundamental particle such as an atom or an electron. The axis around which the particle spins is easily tilted by very weak magnetic fields, and therefore a measure of the axis orientation gives us very precious informations on the environment surrounding the particle. Atomic spin magnetometers are now surpassing in performance the superconducting quantum interference devices (SQUIDS) that have been formerly the industrial standard. In addition, the possibilities of miniaturization and coupling to optical fibers makes the new generation of magnetometers particularly interesting for the realization of sensors in hostile environments such as places where high electrical voltages or temperatures exist.

High-precision magnetometers have very important applications in medical diagnosis. For example, micro-sized atomic magnetometers allow us to perform **magneto-encephalography**, a non-invasive technique in which the detection of the weak magnetic fields produced by the brain is used to infer the location of neural currents inside the skull. This type of measurements is helping us to understand the physiology underlying cognitive processes in living beings.

The measurement of **nuclear spin resonance** in noble gases is opening possibilities for new diagnostic techniques. An interesting application has been found as an example for the imaging of human lungs. These may be filled during the examination with an inert gas, in which all the atoms are set to spin in the same direction. By studying the oscillation of the rotation axes of the particles, we are able to obtain pictures with a resolution much higher than the ones yielded by ordinary magnetic resonance imaging (MRI).

Twentieth century physics forced us to accept one more counter-intuitive phenomenon. Although Young and other scientists showed with beautiful experiments that light commonly

The "spin" of each atom is exploited in quantum magnetometers to measure extremely weak magnetic fields



behaves as a wave, Planck and Einstein demonstrated that under some circumstances one cannot neglect its corpuscular nature. Quantum mechanics introduced therefore the concept of **wave-particle duality**: although light has a corpuscular nature, its dynamics must be described in terms of wave propagation. Even more mysteriously, depending on the experiment one may observe either the corpuscular, or the oscillatory nature. But never both at the same time.

In a totally specular way, quantum mechanics assumes a dual character of matter: at sufficiently low temperatures atoms can behave either as particles or as waves, and therefore undergo both collisions and diffraction or interference. After more than 70 years of experimental strives, various groups in 1995 managed to cool a gas of about a million particles so close to the absolute zero (the lowest temperature admitted by Nature), that atoms started to behave coherently as a single matter-wave. These ground-breaking experiments effectively opened the possibility of investigating the wave nature of matter, and the pioneers of this field have been awarded with the 2001 Nobel prize in physics.

Matter-wave interferometry can be used as a tool to measure very precise motion by detecting changes in the interference patterns created by the merging of two atomic clouds. Matter-wave interferometry can drastically improve the accuracy and performance of, as an example, inertial navigation sensors, which would be fundamental in autonomous defense and communication systems.

The accurate measurement of the gravitational field is fundamental in order to identify underground oil deposits and mineral resources, since their presence creates anomalies in the gravity force generated by the Earth. Nowadays, state-of-the-art gravimeters are based on laser schemes, but atom-wave interferometers will soon enable us to do more precise measurements of gravitational anomalies, yielding an even more efficient detection of these hidden reservoirs of precious resources.

The possibilities of miniaturization and coupling to optical fibers makes the new generation of magnetometers particularly interesting for the realization of sensors in hostile environments such as places where high electrical voltages or temperatures exist

3. Quantum Control

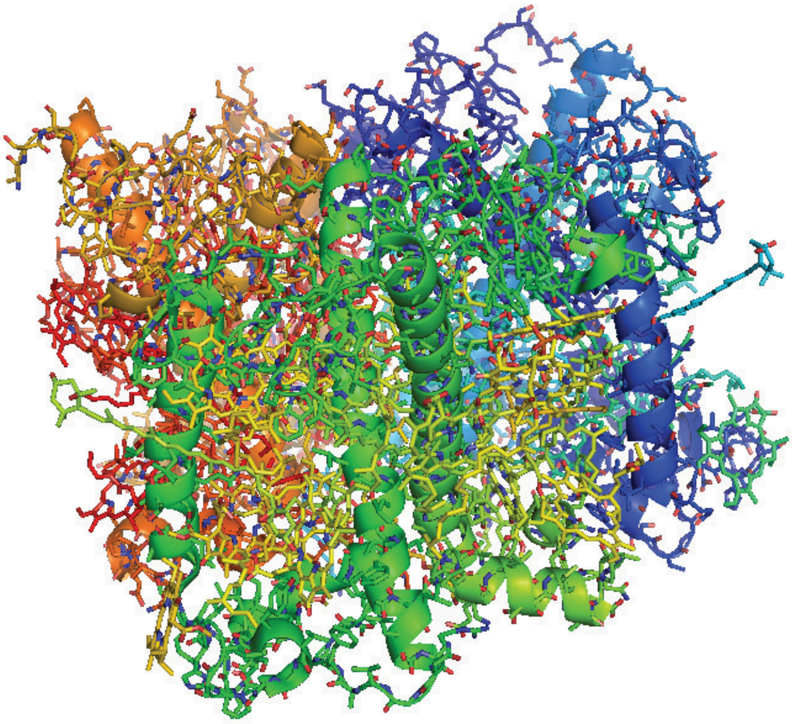

Eadweard Muybridge, Human and animal locomotion, Philadelphia 1887

Since atoms and molecules were identified as the building blocks of matter, scientists and engineers have dreamt of controlling and directing their behavior. The latest developments in laser technology are paving the way for the realization of this dream. Nowadays, laser sources with ultra-short temporal durations, operating at different wavelengths and intensities, can be used to control and prepare atoms and molecules in specific quantum states. In this way, we are learning about chemical and biological processes on the scale of single atoms, and we are becoming able to control and precisely tune the outcome of chemical reactions. This technology allows us to create novel molecules and materials for specific applications in health care, alternative energies, environmental sciences, safety and security. In addition, the control over atomic quantum states is of fundamental importance to realize the quantum information tasks that will be described in the following section.

Nowadays, laser sources with ultra-short temporal durations, operating at different wavelengths and intensities, can be used to control and prepare atoms and molecules in specific quantum states

The possibility of generating laser light at different wavelengths gives us a tool for investigation at very different spatial scales. Light at short wavelengths is necessary to study the structure of small objects. In particular, X rays have been instrumental in revealing the double helix of DNA molecule. Nowadays, table-top laser sources of X rays have been developed and are commercially available. In the future, X ray light sources will be useful to build even smaller microchips and nanomachines. Compact X ray microscopes will be useful for biomolecular imaging, since they give us access to the world of tiny objects with an unprecedented resolution.

As it happens in usual photography, the possibility of doing motion pictures requires a shutter faster than the event we wish to record. The mechanical shutter of a movie camera opens 25 times in a second, giving us a faithful reproduction of the



Light harvesting complex

motion of big objects such as people or cars. But in the quantum world, motion occurs on dazzlingly short time scales. Indeed, a molecule may rotate around itself in a picosecond (i.e., a millionth of a millionth of a second, or 10^{-12}s), while its vibration takes even shorter, just a few femtoseconds (10^{-15}s). As we come to the electrons, their motion is even quicker: a “slow” electron goes around a molecule in an attosecond (10^{-18}s), while a fast one may do the trip around an atom in just some zeptoseconds (10^{-21}s). At such incredible speeds, the role of the videocamera shutter can only be taken by the successive pulses of a laser beam: the shorter are the pulses, the faster will be the tracking of a process or a particle. Laser pulses in the X ray range have the characteristic of being extremely short in the temporal domain, and state-of-the-art devices are now yielding pulses with attoseconds durations. These strobes of light therefore are able to capture some of the fastest events in Nature, opening us the possibility of taking motion pictures even of electronic structures.

Molecules are kept together by strong bonds that involve the electrons of its constitutive atoms. Therefore, by studying the dynamics of the electrons we are able to understand why some atoms bind between each others, and others don’t. In this way we are getting a better understanding of chemical and biological mechanisms. On practical grounds, this results in the development of on-demand molecules for particular applications. In addition, X ray laser sources help us to understand why molecules in living organisms are able to carry specific tasks in very efficient manners.

Observing the movement of molecules, atoms and electrons is in some sense the first step towards our ability to control their behavior. However, femtoseconds pulses give us other mechanisms to determine the outcome and the speed of various chemical reactions. Indeed, quantum mechanics tells us that if a particular process can happen in many ways, all possible ways must be taken into account, and the final outcome is described by the sum of their “probability amplitudes”. Classically, each amplitude is a real and positive number, and their sum is always larger than each of the terms. In the quantum world, particles are instead described in terms of waves, which behave similarly to ripples on the surface of a pond. Their proba-

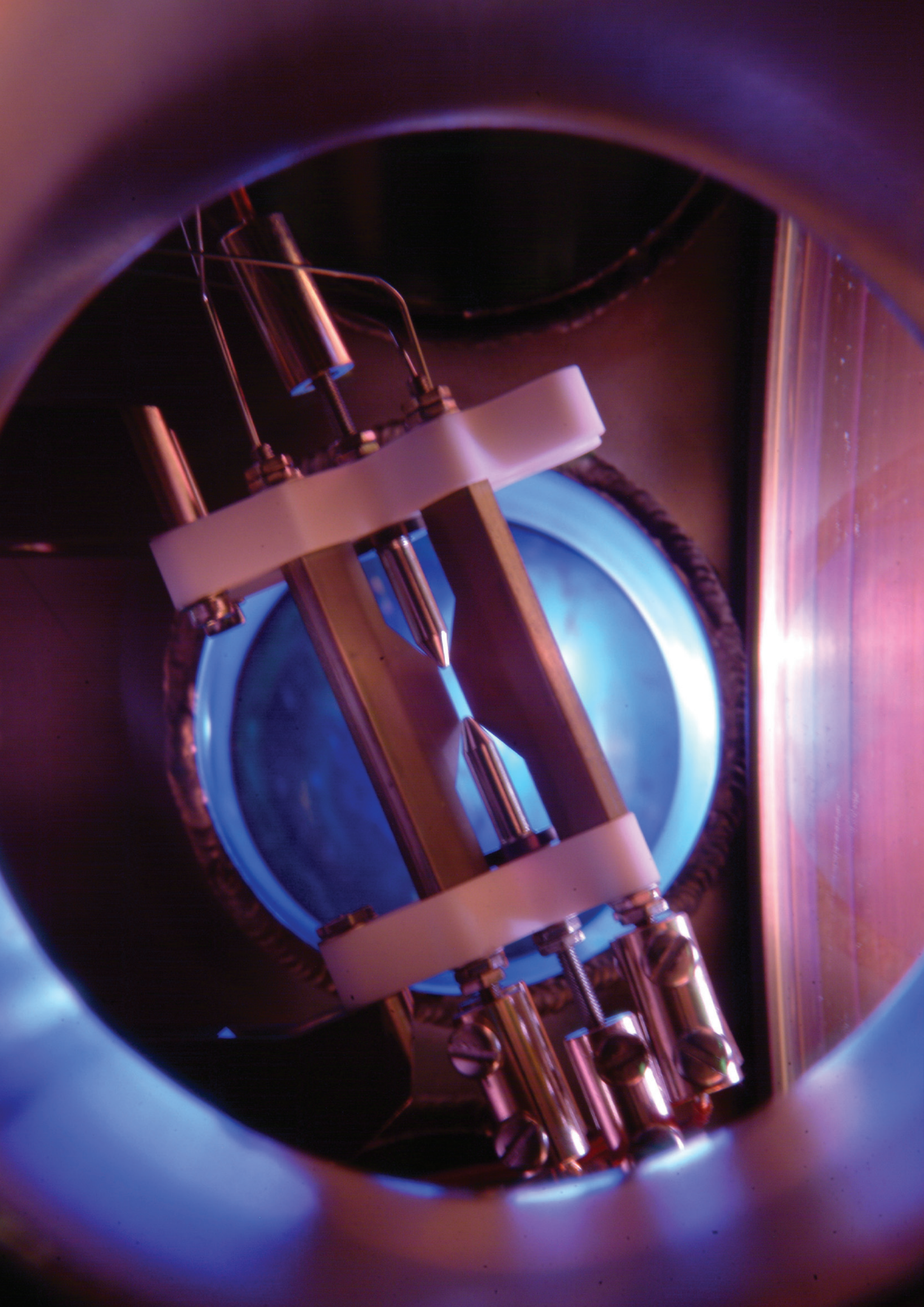
The development of tools and techniques for quantum control helps us to understand phenomena on time scales that are relevant for atomic and molecular physics, chemistry, life sciences and material sciences

bility amplitudes must be represented by complex numbers, and these can add up or cancel each other. As a consequence, when a determinate reaction is theoretically possible through many possible ways, we may either get a faster reaction, or even no reaction at all. In technical terms, these two alternatives are respectively called constructive and destructive interference. Femtoseconds pulses interact with the atomic dynamics, opening and closing these reaction paths. Therefore, using tailored laser pulses we are able to control chemical reactions, speeding them up or slowing them down.

This approach has been used to optimize the production of desired quantum states, and also to control the paths of energy flow in bacterial light-harvesting systems. Very recently, it has been shown that it is possible to control the quantum dynamics of single molecules even at room temperature. This discovery opens whole new paths for our understanding of the role played by quantum mechanics in everyday life.

The development of tools and techniques for quantum control helps us to understand phenomena on time scales that are relevant for atomic and molecular physics, chemistry, life sciences and material sciences. In particular, it is becoming possible to learn about the duration of chemical reactions, and to understand phenomena as chemical catalysis or absorption of sunlight in photosynthesis. This acquired knowledge and understanding will surely translate into practical applications. In the future, it will be possible to tailor new molecules and control a chemical reaction in such a way that products are enhanced and by-products are minimized. These achievements will result in applications that range from enhancing the efficiency of solar cells to developing new biosensors and light-harvesting systems.

4. Quantum Information and Simulation



The advent of the first computing machines in the late 1930's showed the urgent need for a solid theory of information, which could investigate how information is stored, processed and transmitted. Conventional computing machines, or computers, use bits as fundamental units of information, i.e., physical entities that can take the value 0 or 1. Half a century later, scientists and mathematicians proposed to substitute the bit with a qubit, or a quantum state. The main difference is that, thanks to the superposition principle, a qubit can take a value corresponding to any superposition of 0 and 1. It was soon realized that a machine based on qubits, the so-called **quantum computer,** would be able to solve certain tasks much faster than its classical counterpart.

A qubit can take a value corresponding to any superposition of 0 and 1. It was soon realized that a machine based on qubits, the so-called quantum computer, would be able to solve certain tasks much faster than its classical counterpart

The most celebrated problem is the factorization of a number into its prime factors. The problem is easily stated: given two prime numbers A and B, it is straightforward to calculate their product C=A*B, no matter how large A and B are; nonetheless, if C is a number of some 50 digits, it can be a formidable task to retrieve its prime factors A and B: on the fastest supercomputer available today, this operation may take years. Therefore, we can publicly share the number C, and nobody will be able (in a reasonable time) to figure out what are its prime factors A and B. Standard cryptography methods used over the internet, such as SSL, indeed rely on this computational challenge to provide secure communications between two parties, e.g., a bank and its clients.

It was first demonstrated by the mathematician Peter Shor that a quantum computer could completely outperform a classical machine on this problem. Shor's contribution was to write **quantum algorithm** able to calculate the same result in an exponentially shorter time. Shortly after, it was noted that quantum computers may have the same enormous advantage over traditional machines in other notoriously hard problems. One of those is of great importance today: finding "the needle in the hay", or how to browse through and sort large amounts of information. Research engines on the web would profit enormously from the implementation of this algorithm. And the number of similarly powerful quantum algorithms keeps growing day by day.

With the rapid development of quantum information it became clear, at least theoretically, that quantum computers would help us to solve complex and very time-consuming tasks. Nonetheless, their practical implementation is far from trivial. Today, qubits can be prepared by using polarization states of photons, or electronic and nuclear spin states of atoms. Unfortunately, these quantum states are very fragile, and currently their manipulation requires very cumbersome infrastructures since even the weakest interaction with the environment may destroy the integrity of the qubit's superposition. Millions of

qubits would be needed to implement a powerful quantum computer, but today's most "advanced" realizations contain only a few tens of those. This clearly results in a very limited computational ability, but a whole community of scientists and industries is working hard, looking for scalable systems which could be easily manufactured at an industrial level. Proposals aimed at obtaining a large number of qubits are currently focusing mainly on solid state superconducting circuits, or ultracold atoms in optical lattices.

As an example of where quantum information could provide a solution to a very common problem, it is interesting to think back at one of the first proposals emerged within this field. Maybe the oldest security issue that men had to face within a society was the "security of money". Indeed, ever since there have been coins and banknotes, thieves have been there trying hard to counterfeit it. The problem is evident: if a paper bill may be printed by a bank, everybody could produce copies of it, provided that he or she has a good enough "copying machine." A physicist named Wiesner in the late sixties came up with an ingenious solution to the problem: the concept of **quantum money**. He realized that, if each of the bills contained a randomly-generated quantum state known only to the bank that printed it, nobody would be able to create an identical copy of the banknote without destroying the original one. The issuing bank would then be able to realize that the money has been counterfeited. The idea relies on an alternative formulation of the celebrated Heisenberg's uncertainty principle, the so called "No-Cloning Theorem", which guarantees rigorously that there cannot be a "Xerox machine" which takes an unknown quantum state and spits out two identical copies of it. Although the proposal by Wiesner is very appealing and provides us a solution to this longstanding problem, its practical implementation has been up to now impossible for two main reasons. In first instance, quantum states are currently very fragile, and would hardly stand the interaction with an unprotected environment such as a wallet in a man's pocket. Second, on a level at the same time more abstract and practical, the originality of a banknote may be checked only by the issuing bank and not by a shop at some other location. Despite the apparently simple formulation of the problem (is it possible to have 100% secure money, which may be tested at any point by everyone?), 40 years of intense theoretical efforts have not yet given us a positive answer, and the question still constitutes a very hot topic of investigation.

Nowadays, the most prominent contribution to society from the field of quantum information was given in the field of **secure communications**. As discussed above, common encryption algorithms are based on computational complexity, and are therefore intrinsically vulnerable: two parties share a coded message, and the secretness of the communication relies on the fact that decrypting the message simply takes too much time. But both the key and the coded messages are at all times public, and it is in principle always possible to decrypt the message, given enough time and computational resources. The two communicating parties will never be able to know whether their message has been intercepted and decrypted during or after its transmission. A revolution came in this sense with the proposal of using quantum states as encryption keys. Indeed, a fundamental quantum mechanical principle states that

Interference of water waves in a pond

the mere observation of an object inevitably alters its state. Therefore, if the encryption key is smartly encoded in a quantum state, the two communicating parties will be always able to detect the presence of a third party, a secret eavesdropper. By checking the integrity of the key after transmission, the communication may be ensured to be 100% free of eavesdroppers. In times dominated by long-distance communications, privacy and secrecy have a vital role in national security, industrial development and inter-personal communication. Nowadays, quantum cryptography provides the only totally fail-safe solution to this key-issue. As we will see in the coming section, various companies produce and distribute since a number of years affordable and packaged quantum cryptography solutions, which have already found their first applications in large scale public projects.

Another promising quantum application is the realization of the so-called **quantum simulators**, i.e., experimental setups able to accurately model other complex systems whose properties are still generally unknown.

The main advantage of working with ultracold atoms and ions is that a very large “toolbox” for their manipulation has been developed in the past years. Indeed, we are able to change at will the temperature, the number of the atomic species, and even the strength of the inter-particle interactions. Moreover, atoms may be confined in tubes, two-dimensional planes, or regular periodic crystals.

These ultracold gases are so dilute that their dynamics can be modeled in most cases exactly, starting from very first principles. Therefore, in a quantum simulator we are able not only to reproduce the behavior of very complex systems, but also to understand thoroughly the underlying physical mechanisms. The most acclaimed achievement of a quantum simulator has been the study of the role played by interactions in the transition between a conductor and an insulator. Many more applications have been put forward in the past years, which are expected to lead to the development of new materials, to the accurate description of chemical reactions and to a deeper and better understanding of high temperature superconductors.

5. Quantum Companies, Projects and Products

Quantum technologies have since a number of years already trespassed the threshold of commercial viability. Various dedicated enterprises and university spin-offs are currently producing and commercializing some of the products described in the previous sections. As an example, it is now possible to buy ready-to-use, packaged solutions for secure quantum cryptography and all sorts of tailored laser devices.

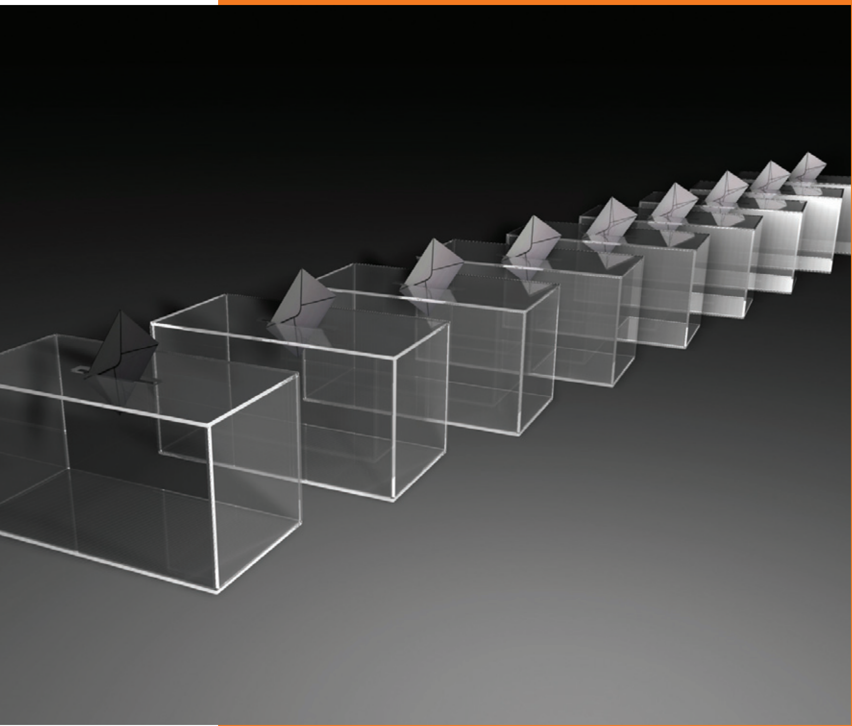
World-leader companies as IBM, Toshiba and Hewlett-Packard have research units dedicated to quantum technologies and participate actively in projects together with universities and research institutions. An important part of the leading edge research done at Pirelli Labs is devoted to quantum optics. In particular, researchers at Pirelli focus on the implementation of advanced methods for transmission of quantum-encrypted information over fiber optics networks, and the development of the basic building blocks for optical quantum computing. NEC Laboratories America also has a Quantum Information Technology group. This is a theoretical group that complements the experimental group at NEC Nano Electronics Research Labs. Their main objective is to find problems of practical importance for which a quantum computer has a significant advantage over its classical counterparts. Also Microsoft has a research group, called Station Q, dedicated to study methods towards the realization of efficient quantum computers. In particular, the group combines researchers from mathematics, physics and computer science, and focuses on topological quantum computation, a technology which promises to solve the decoherence problem by exploiting error-resistant systems.

At the European level, significant funding is dedicated to foster collaborations between companies, universities and research institutions. In particular, various projects with a strong focus on quantum technologies are being brought forward within the Seventh Framework Programme (FP7) run by the European Commission. Some of the most recently financed projects are:

- Quantum interfaces, sensors and communication based on entanglement (Q-ESSENCE)
- Quantum Computer Science (QCS)
- Quantum repeaters for long distance fibre-based quantum communication (QUREP)
- Quantum integrated photonics (QUANTIP).

It is now possible to buy ready-to-use, packaged solutions for secure quantum cryptography and all sorts of tailored laser devices

LARGE SCALE PROJECTS



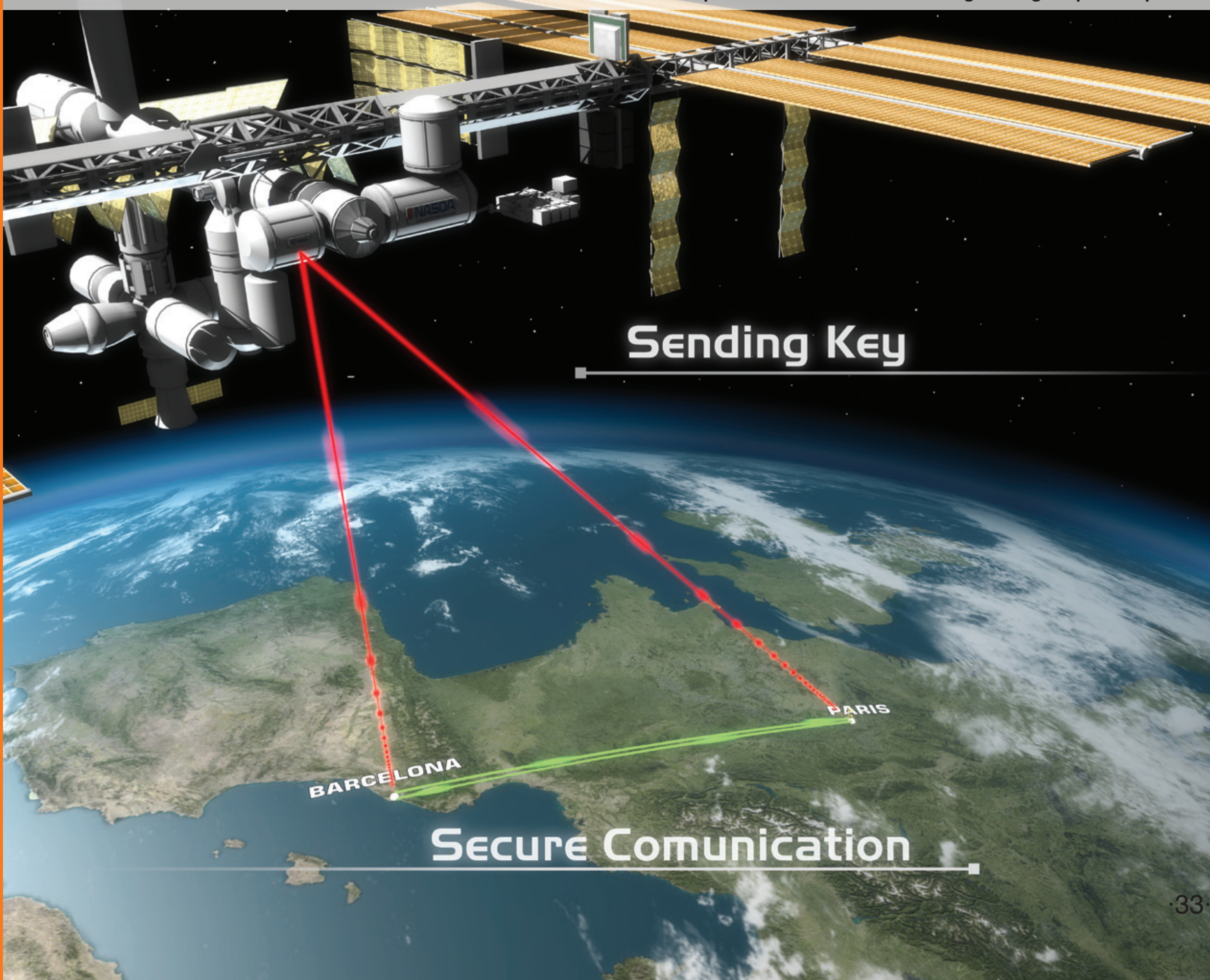
- In the fall of 2007, IDQuantique deployed Cerberis, an integrated cryptography solution to secure the Swiss federal elections. Cerberis used quantum cryptography for the management of encryption keys. The Gigabit Ethernet connection between the central counting station located in downtown Geneva and the data center where all the results were stored and processed run perfectly during the elections. Cerberis represents the world's first application of quantum cryptography in a large scale public project.

- The European Space Agency (ESA) and the national space agencies of various european countries worked together aiming to send entangled photons into space. The Space-QUEST proposal aims to place a quantum communication transceiver containing an entangled photon source, a weak pulsed laser source and single photon counting modules in space. This will accomplish the first-ever demonstration in space of fundamental tests on quantum physics and quantum-based telecom applications.

- The DARPA quantum network operates continuously across Cambridge (Massachusetts, USA) since 2004. BBN Technologies designed and built the world's first Quantum Network testbed, delivering end-to-end network security via high-speed Quantum Key Distribution (QKD). BBN has wired this ultrahigh-security network into commercial fiber across the metro Boston area. BBN's QKD network comprises 10 nodes. It is both extremely secure and 100% compatible with today's Internet technology. Six of the ten nodes are constantly running over the Boston metropolitan telecom fibers between BBN, Boston University and Harvard University, protecting their Internet traffic against undesired intrusions; the four other nodes are instead connected via aerial laser links.

- The SECOQC project (an acronym for 'global network for secure communications based on quantum cryptography') represents a collaboration between european research organizations, universities and companies including Hewlett Packard, IDQuantique, Qinetiq, Siemens, Thales and Toshiba Research Europe. The SECOQC QKD demonstration took place in October 2008 in a standard metropolitan fibre-optic network connecting five of Siemens' sites around Vienna, encrypting applications such as VoIP, video-conferencing and Web services with constantly refreshed quantum keys, 24 hours a day.

Satellite-based quantum communication using entangled photon pairs



QUANTUM COMPANIES

Here below, we give a short list of quantum companies on the market, together with a resume of their commercial products:

Qutools

(Munich, DE www.qutools.com) | Entangled Photon Pair Sources, quantum Random Number Generators (qRNG), Quantum Key Distribution (QKD) systems and various components for research in quantum optics.

MagiQ

(Boston, USA www.magiqtech.com) | Security Gateways based on QKD, fiber optics acoustic sensors and interferometers.

IDquantique

(Geneva, CH www.idquantique.com) | Quantum Random Number Generators, QKD network encryption products, single photon counters.

BBN

(Cambridge, USA www.bbn.com) | Establishment of the DARPA quantum network, the first operational secure network based on QKD. Development of LADAR, a laser-based radar technology which exploits quantum squeezed states to increase resolution up to 10 times over a standard radar system. Superconducting Digital Signal Processors (SDSP) and quantum circuits.

QuantumWise

(Copenhagen, DK www.quantumwise.com) | Developers of Atomistix ToolKit, a quantum-mechanical software package to simulate electrical transport properties of nanodevices on the atomic scale. The software nowadays is used by over 100 research groups at leading universities, government laboratories, and electronics companies around the world, in a wide range of applications.

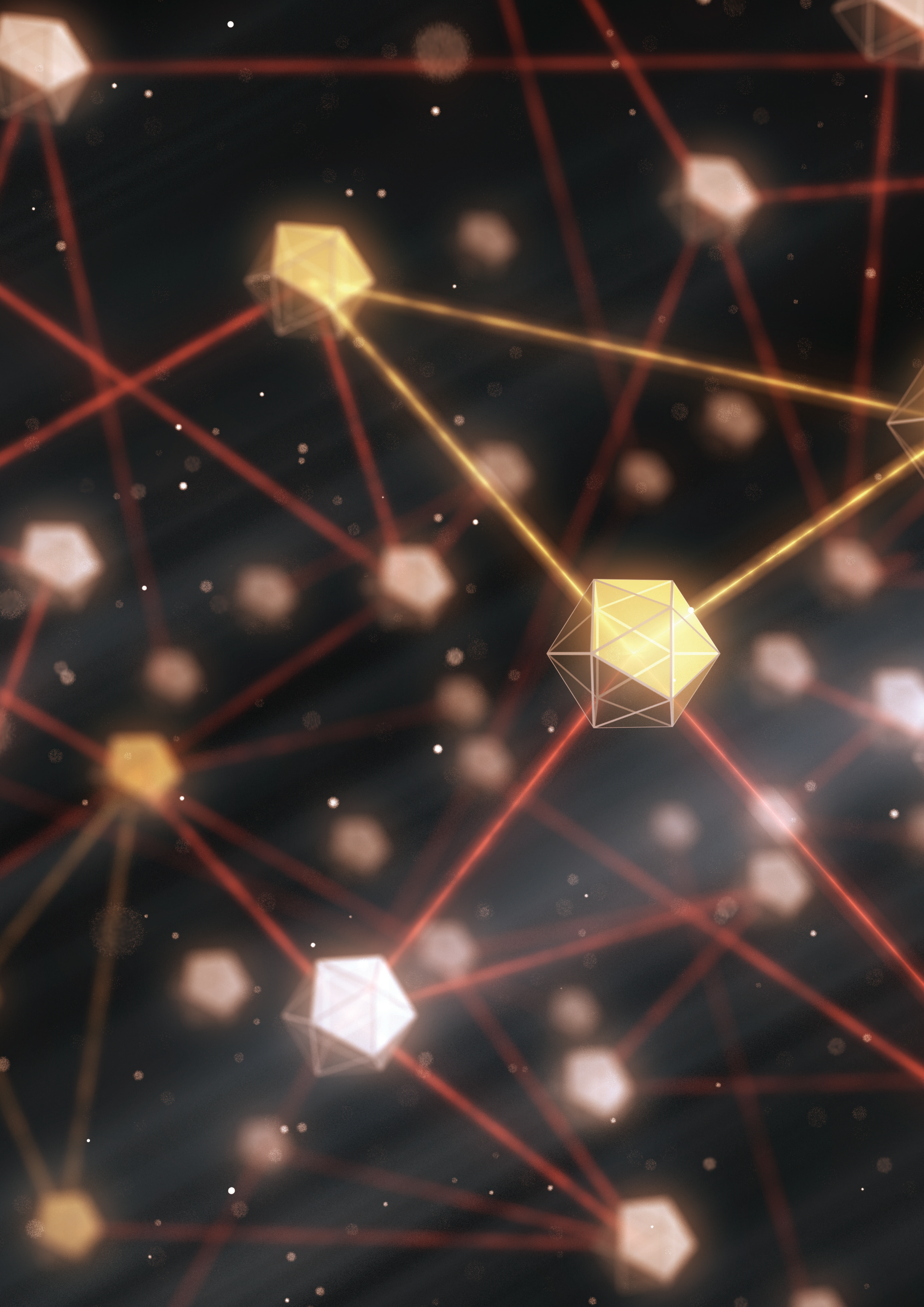
QinetiQ

(Malvern, UK www.qinetiq.com) | Defense, security and technology company setting up a QKD network in London.

Swiss Quantum

(Geneva, CH www.swissquantum.com) | Large scale project realized in Geneva, consisting of a broadband QKD link connecting the University with CERN and with the Engineering School.

6. Towards the Future

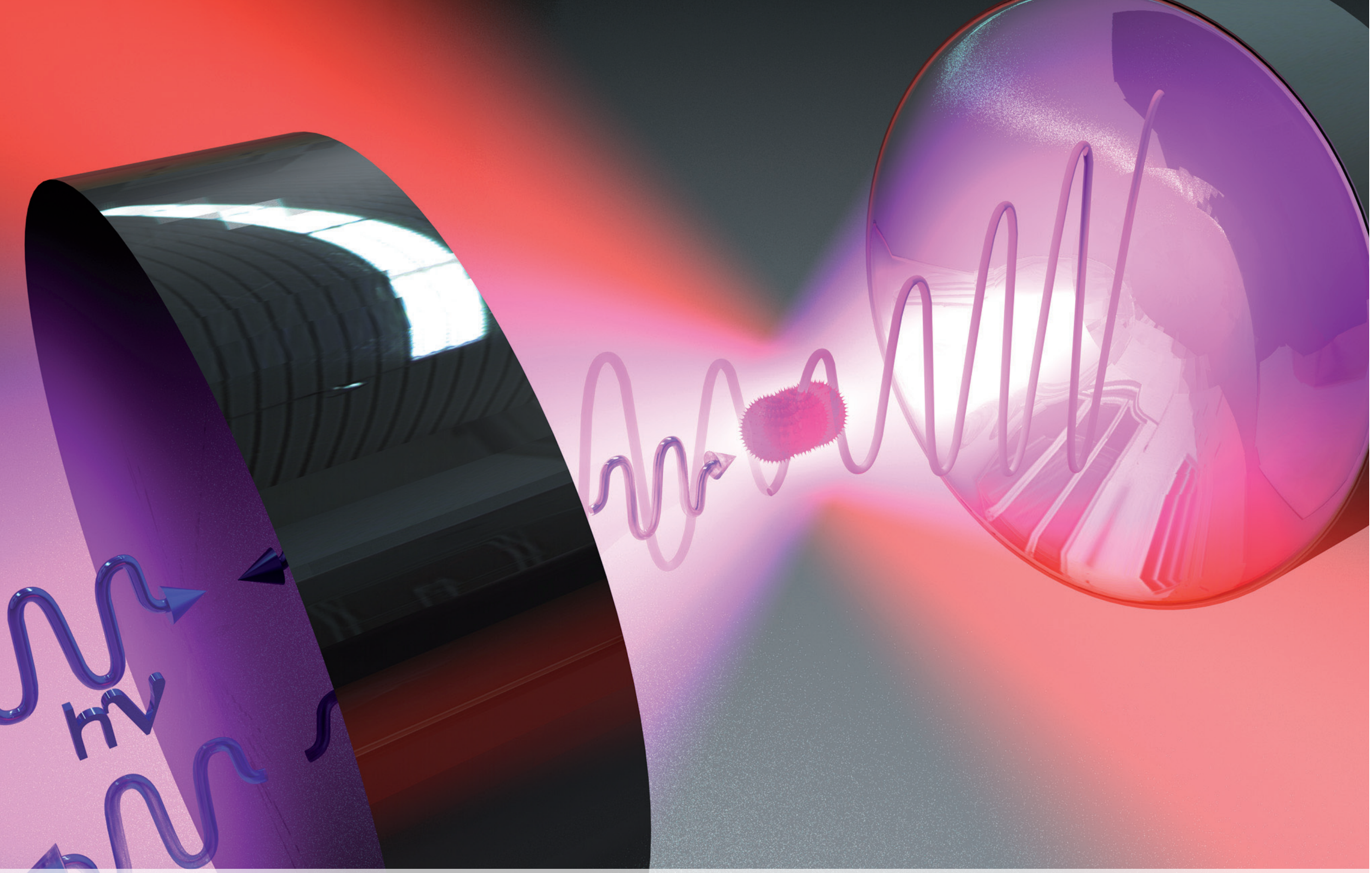


Artist view of a quantum network

As shown in the previous section, **quantum networks** have already found their first applications in real life, ensuring intrinsically secure connections between physically distant nodes. Although the realizations in Harvard and Geneva are still within an university environment, their future extension to a larger community is clearly within close reach.

After all, Internet as well started as a very restricted network, developed first in the late fifties by the US military agencies for security concerns. Subsequently, it was extended to a greater public by scientists at CERN in the late eighties, to share the experimental results collected in Geneva with universities across the globe. Twenty years was all it took to Internet to explode, and occupy the key role it has today: this is how fast a powerful technology can deeply affect the lives of billions of people.

Scientists now dream of realizing large quantum networks, in which many distant nodes are set in entangled states. This kind of setup would give us not only perfectly secure communications, but also extremely fast computations, since quantum computers are effectively able to perform large parallel computations.



Proposal for a setup to realize a quantum superposition of living beings

But the quantum world keeps offering us incredible chances to explore, understand, and reshape our environment. As an example, it has been recently proposed that, by exploiting micro-traps and sophisticated cooling techniques, it will soon be possible to put **macroscopic objects in a quantum superposition** of two different states. The proposal goes so far as to propose that even living beings, such as the "tobacco virus", could be transferred in this exotic state. This is clearly one step forward towards the realization of the puzzling "Schrödinger cat".

Moreover, recent discoveries are showing that **quantum processes play a key role in biological systems**. As an example, it has been demonstrated that some algae developed a very efficient photosynthetic cycle (the process converting solar light into energy) which exploits the constructive interference between distinguishable quantum paths.

Once more, we see that the observation and the understanding of the ingenious solutions found by organisms in Nature can show us the way towards the efficient solution of complex problems, such as the efficient generation of environmentally-friendly energy. The ongoing research in quantum technologies provides us with key ideas and results that are contributing to build safer, faster and smarter devices and products.

The ongoing research in quantum technologies provides us with key ideas and results that are contributing to build safer, faster and smarter devices and products

Generalitat de Catalunya

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Fundació CELLEX Barcelona

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

icrea
Institució Catalana de Recerca i Estudis Avançats

European Regional Development Fund
European Social Fund

ICFO

Centres de recerca de Catalunya

Mediterranean Technology Park | Av. del Canal Olímpic s/n | 08860 Castelldefels (Barcelona), Spain
Tel. (+34) 93 553 40 01 | Fax (+34) 93 553 40 00
E-mail secretariat@icfo.es