FROM BASIC RESEARCH to innovations in quantum technologies

Michèle LEDUC[1], **Sébastien TANZILLI**[2]
[1] Emeritus senior scientist at the Kastler-Brossel Laboratory (ENS, UPMC, CNRS) in Paris and former director of the Ile-de-France Cold Atom Research Institute (IFRAF).
[2] Senior scientist at the Nice Physics Institute (CNRS & Côte d'Azur University), head of the "Quantum Engineering, from Fundamental Aspects to Applications" (IQFA) CNRS research network, and missioned by the CNRS Physics Institute to coordinate "Quantum Technologies" at the national level.
sebastien.tanzilli@inphyni.cnrs.fr

First the physics, then the technology. The two main revolutions that took place in physics in the 20th century were quantum physics and relativity. Quantum theory has never been disproved, and although scientists continue to wrangle over what its concepts actually mean and how they should be interpreted, it has been successfully applied in many areas, and new applications are constantly emerging.

We owe almost all the fundamental discoveries in quantum physics to work conducted in the previous century by Bohr, Heisenberg, Schrödinger, Dirac, Pauli, de Broglie and many others. These discoveries have enabled us to understand the laws that govern matter, light, and the interactions between the two. Above and beyond these basic concepts, quantum physics has given rise to unprecedented technological developments (transistors, microprocessors, lasers, etc.) that have revolutionized our daily lives. The extraordinary experimental advances that have been made over the past few decades mean that we are now able not only to observe quantum objects such as photons, atoms and ions, but also to control them both individually and collectively, using the concepts of quantum superposition and entanglement to prepare and manipulate them (see Box). The applications are so promising that several countries, not least the United States and China, have made them a national priority. For its part, the European Commission launched its Quantum Technologies Flagship in October 2018, funding some 20 projects selected in an initial call for projects. In this article, we look at the Flagship's four application areas, namely quantum communication, quantum computing, quantum simulation, and quantum metrology and sensing, where spectacular results are expected over the short, medium and long term.

Secure quantum communication between cities and continents

Standard modes of communication and information processing have revolutionized society over recent decades. All five inhabited continents are now connected by undersea fibre-optic cables, and countries are criss-crossed with terrestrial and satellite links, allowing information to be carried and routed at high speed with no data loss over virtually limitless distances. However, when it comes to ultra-secure communication, the story is somewhat different. In many areas of public and private life, the need for data security has become a fact of life cornerstone, and represents a key strategic issue for businesses, large industrial groups, banks, governments, as well as for individuals. Current protocols for ciphering and unciphering messages are having to use increasingly complex codes and longer public keys, in a bid to keep one step ahead, as the classical computers capable of breaking these keys become ever more powerful. A more effective strategy must therefore be found, and this is where quantum physics comes in, as it can guarantee long-term immunity to hacking and spying on secure data exchanges.

Like classical cipher methods, quantum analogues rely on the exchange of randomly generated binary bits. However, whereas classical bits must be either 0 or 1, these two states can be superposed in quantum bits, or *qubits* (see *Box*). Photons are the preferred carriers for sending qubits over long distances, as they allow information to be encoded into observables such as light polarization (see *Figures* in *Box*). These photons are emitted either as single ones or by pairs by so-called single-photon (colour centres in diamonds,

https://doi.org/10.1051/photon/2019S446

quantum dots) or photon-pair (parametric nonlinear optics) sources. Some of the quantum protocols for establishing secret cryptographic keys therefore use individual qubits, while others use pairs of entangled qubits.

Quantum cryptography can serve to generate keys for use in classical cipher protocols. This technology is already quite advanced, and has been used by a number of small companies to develop systems that are now on the market. For example, the Swiss firm ID-Quantique has applied it several times in real-world situations, including collecting information about online voting in the canton of Geneva. Tokyo has had a quantum crytography network since 2011, while China launched a quantum fibre link between Beijing and Shanghai in 2017. These cities are some 1200 km apart, and for the time being, data can only be reliably carried over distances of a few hundred kilometres in the absence of secure repeaters. A whole new area of research has therefore emerged to design quantum repeaters that can store bipartite entangled states at two remote locations, then synchronize the reemission of the photons. Alongside this research, quantum communication is starting to make inroads in space, as a source carried on a Chinese satellite distributed entangled photons to ground stations a record 1200 km apart. A new era of intercontinental quantum communication is therefore opening up for researchers and *quantum engineers*.

In a bid to increase the rate and range of quantum communication and make it even more secure, scientists are taking a close interest in the latest technological innovations in photonics and microelectronics. This should lead to the development of genuine quantum cryptosystems, starting with prototypes and eventually arriving at tested and certified devices. Recent experimental advances in the manipulation of entanglement at telecommunication wavelengths mean that researchers can now envisage quantum communication protocols on a large scale, whether this is in terms of the number of users who are connected or the

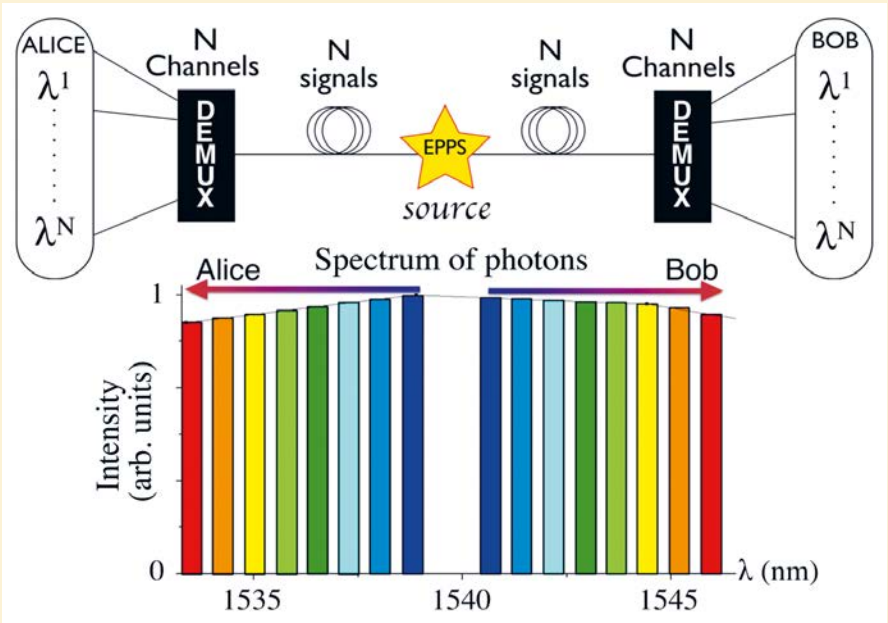


Figure 1. Operating principle of a quantum cryptography link over a distance of 150 km with a spectral demultiplexer at either end (Alice and Bob). The source delivers pairs of entangled photons with a spectrum covering the whole bandwidth. As the colour coding shows, the demultiplexing layers enable Alice and Bob to establish secret keys in each pair of complementary spectral channels. This strategy means that the total secret key rate is multiplied by the number of channel pairs that are used (Courtesy of Djeylan Aktas, Nice Physics Institute; see Aktas *et al.*, *Lasers & Photon. Rev.* **10**, 451-457, 2016). This figure is copyrighted and not subject to the Creative Commons license.

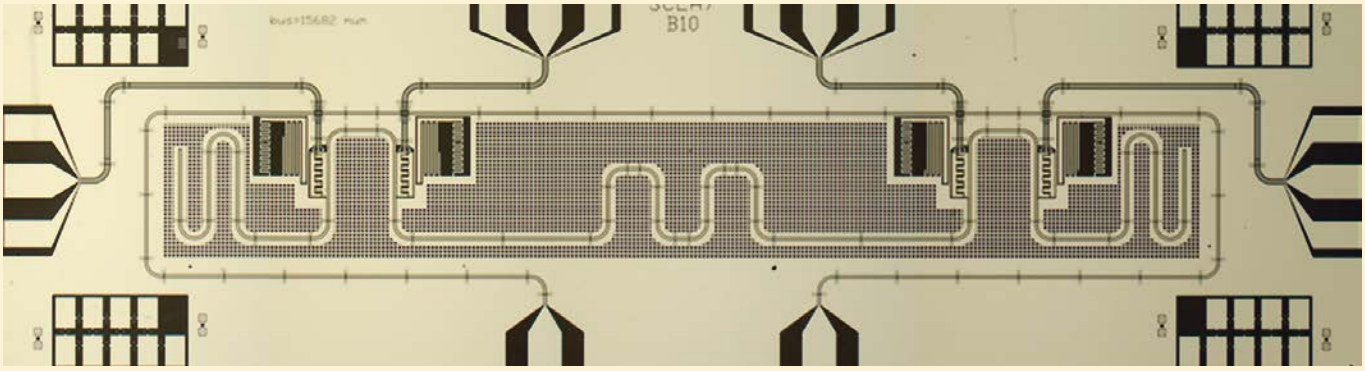


Figure 2. Prototype of a universal 4-qubit superconducting quantum processing system in aluminium that can measure individual qubits. Josephson junctions between the superconductors and microwave photons are the two key ingredients of this quantum processor, which has a total length of approximately 10 mm (Courtesy Daniel Estève, Quantronics Group, CEA-Saclay; see Dewes *et al.*, *Phys. Rev. B* **85**, 140503, 2012). This figure is copyrighted and not subject to the Creative Commons license.

distances between them (see *Fig. 1*). Entanglement should allow for the development of officially certified cryptosystems, that is, systems that are independent of the hardware (sources and detectors) being used. There is a constant stream of new hybridization ideas, some involving the introduction of quantum cryptography into existing telecommunications systems, others the creation of post-quantum solutions based on classical cryptography that cannot currently be attacked by quantum computers. It will take years of R&D before the general public have access to a truly global quantum Internet, but the distribution of ultra-secure private keys between remote sites is already being seen as a means of defusing the threat currently posed by quantum computers to classical encryption systems.

Towards an ultra-powerful quantum computer?

The immediate goal of designing a universal quantum computer or processor is to go beyond the bounds that classical supercomputers will soon have reached. So high are the underlying stakes that a huge research effort is currently underway all over the world to build just such a quantum computer, in both academia and industry, with IT and Internet giants such as Google, IBM, Intel and Microsoft investing huge amounts of resources in it.

The idea is to perform massively parallel computing with an exponentially increasing number of operations taking place at the same time. The problem is that the applications of quantum computing rely on specific quantum algorithms that have to be implemented at the same time. So far, only a few such algorithms have proven quantum processing to be more efficient than conventional processing. The two best known ones were developed by Shor and Grover: the former can prime factorize large integers, while the latter can search an unsorted database for a single entry.

The basic underlying concept relies on the use of an entangled qubit register (see Box). The result of the computation is produced via a process of interference that depends on the initialization of the qubit register to the given problem and its evolution via logic gates. Decoherence stands as the main problem, as it tends to destroy the entanglement during the various computation operations, as a result of interactions with the environment.

A wide variety of basic building bricks have been tested in the quest to produce these qubits and construct systems capable of withstanding decoherence. In the race to set the record for the highest number of qubits in a quantum calculator (at least 50 are needed to achieve *quantum supremacy*), the most promising solutions are Josephson junctions (supercurrent; see *Fig. 2*), trapped ions (internal electronic states; see *Fig. 3*) and crystalline silicon (spin qubits). Google, IBM and Intel all recently announced that they had developed superconducting quantum computers with 72, 50 or 49 qubits, while the current laboratory record is for a string of 20 cooled calcium ions, which were used to demonstrate various elementary processes (see *Fig. 3*). Quantum processors with two-qubit logic gates have recently been demonstrated with superconducting systems using either the Josephson effect, silicon spin qubits, or integrated photonic systems.

The first hurdle facing all these potential systems is how to upscale the devices. The second one is how to control the errors introduced by the imperfect components of experimental devices, which make the system far less reliable. The number of errors increases extremely rapidly with the number of logic gates, and ever more sophisticated algorithms are being constructed (so far only theoretically) to detect and correct such errors. Programming a quantum computer is also very different from programming a classical computer, and requires new research by computing experts. In short, although it may seem extraordinarily difficult to develop technologies for quantum computers, there is no fundamental law of physics that prohibits it, and the privately held company D-Wave is already selling

https://doi.org/10.1051/photon/2019S446

quantum computers.

Possible applications have yet to be identified. Above and beyond the threat looming over current public key encryption methods in classical cryptography, the main benefits are likely to be seen in quantum chemistry, with the discovery of new molecules, and high-temperature superconductors. Such is the power of quantum computing that it should also allow the flows of human and other resources to be optimized in the future (meshing of power and road traffic networks, etc.).

Quantum simulation of complex phenomena

It takes extremely powerful computers, or supercomputers, to design many of the complex objects and structures that fill our everyday world, such as cars, planes and public buildings. However, these computers are powerless when it comes to describing the behaviour of systems made up of more than a few dozen atoms and predicting whether they will conduct electricity, become magnetic or superconducting, or produce unexpected chemical reactions. Quantum simulation research is aimed precisely at answering these key questions, particularly in the field of condensed matter science, by applying the quantum simulation methods envisioned by Feynman, who was already talking about *"a quantum machine that could imitate any quantum system, including the physical world"* back in 1982. A range of different platforms or artificial systems can be used to gain a fuller understanding of how real-life systems made up of interacting quantum objects behave in conditions that cannot be directly observed. Theoretical and experimental scientists are working together on the design these artificial systems, which need to be flexible and adjustable (i.e., some or all of their parameters can be controlled), the general idea being that they obey the same quantum physics equations as the real-life systems they are intended to simulate.

One of the current approaches to quantum simulation involves the use of cold atoms, which offer a prime opportunity to conduct model experiments. Atoms are trapped in an optical lattice created by stationary waves from retro-reflected laser beams, ideally with one atom in each site, or held in a lattice by optical tweezers (see *Fig. 4*). Scientists can use Bosonic atoms (e.g., initially forming a Bose-Einstein condensate), Fermionic atoms (e.g., cooled to the degenerate regime below the Fermi

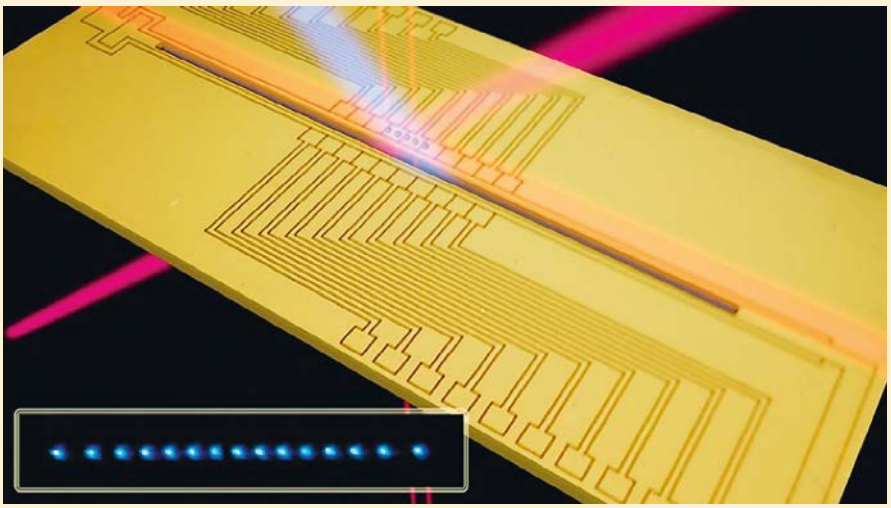


Figure 3. Image of calcium ions cooled and held in a single line in an electromagnetic trap (Paul trap). In the middle of the trap, two neighbouring ions are held 10-20 µm apart. The trap is mounted on an electronic chip where current-carrying wires create the electric and magnetic fields needed for the trap (Courtesy of Rainer Blatt, IQOQI, Innsbruck). This figure is copyrighted and not subject to the Creative Commons license.

temperature), or both. Other types of experimental platforms for quantum simulation include cold trapped ions (see *Fig. 3*), or cold molecules, polaritons or excitons in semiconductors, networks of superconducting qubits or quantum dots, and even entangled photons in coupled waveguide arrays.

Each of these platforms allows some (but not all) of the simulation parameters to be controlled (temperature, number of particles, range and sign of the interactions, coupling with the environment, etc.).

We can therefore simulate many properties of matter, including the new low-temperature quantum phases, magnetism, nonequilibrium quantum systems (notably disorder-assisted quantum transport), topological phases, and materials. The Holy Grail is understanding the conditions needed for high critical temperature superconductivity, which remains shrouded in mystery. This would allow for the design of new materials capable of conducting electricity at ambient temperature with no energy loss, which would have huge repercussions for energy transport. Interfaces are also being developed with quantum chemistry, high energy physics and astrophysics.

Quantum sensors for high-precision metrology

Quantum state superposition is extremely sensitive to the environment, and can therefore be used to build high-precision sensors. Cold-atom accelerometers and gyroscopes

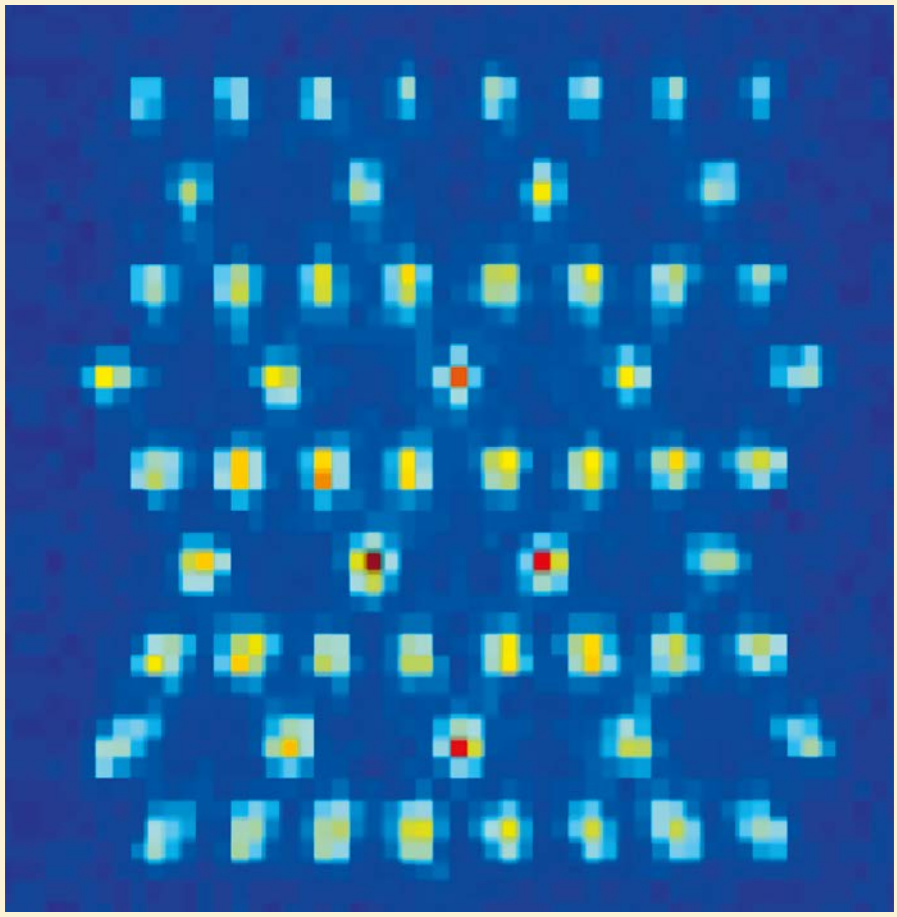
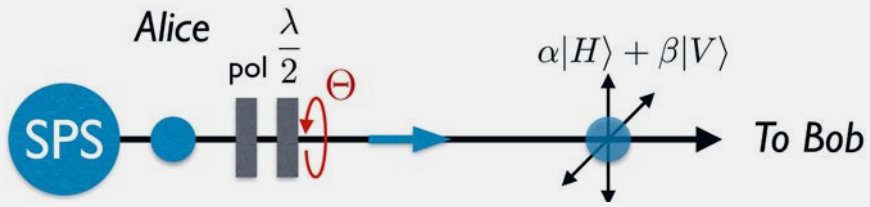


Figure 4. Image showing the fluorescence of cold rubidium atoms held in position by optical tweezers. These atoms can be used to build 2D networks with a variety of patterns (here hexagonal) and spacings (here 5 µm). The colour gradient at each site (from blue to red) indicates the probability of an atom being present (Courtesy of Antoine Browaeys, Charles Fabry Laboratory, Institut d'Optique Graduate School). This figure is copyrighted and not subject to the Creative Commons license.

https://doi.org/10.1051/photon/2019S446

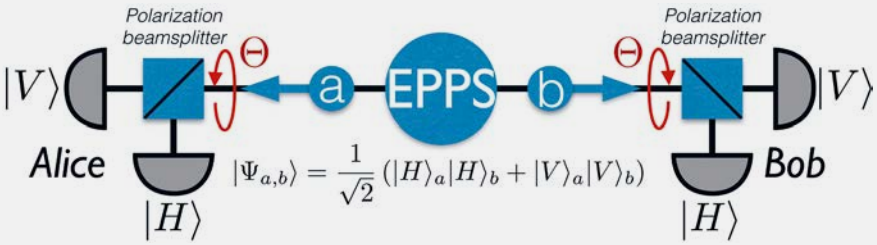
Coherent-state superposition, qubits and entanglement

Classical computing relies on bits, which can have two values (0 or 1) corresponding to states labelled by the notation $|0\rangle$ and $|1\rangle$. Quantum physics offers infinite possibilities, with all the combinations given by the *coherent superposition of two basis states* $|0\rangle$ and $|1\rangle$. For example, let us consider a photon that is horizontally polarized after passing through a polarizer (see figure, where SPS stands for single-photon source). If we add a half-wave plate and rotate it by an angle θ (shown in red in the figure), we obtain the superposition $\sin\theta\,|H\rangle + \cos\theta\,|V\rangle$ of the horizontally $|H\rangle$ and vertically $|V\rangle$ polarized states. This gives rise to a qubit in the form of $\alpha\,|0\rangle+\beta\,|1\rangle$, with the relative weights α and β varying with the angle θ while satisfying the normalization rule $|\alpha|^2 + |\beta|^2 = 1$.



Photonic qubits encoded into the polarization observable are widely used in quantum cryptography, as are those encoded into the time and frequency observables. Qubits can be based on any quantum system – whether it involves natural or artificial particles – that has two distinct states that can be superposed. They are emitted by SPSs that are located here with Alice, who encodes the qubits into the polarization observable using a polarizer (P) and a half-wave plate. The blue arrow indicates the direction of photon propagation from Alice to Bob.

Entanglement represents the generalization to two or more quantum systems of the coherent superposition of states defined for creating a qubit. Staying in the field of optics (see figure below), let us consider a source that emits pairs of entangled photons (EPPS). The usual way of creating this source is to use a nonlinear crystal, which turns a single photon from a pump laser field into a pair of photons with half the energy (not shown in the figure). The pair of entangled photons must be considered as a single quantum system, made up of two subsystems, from the moment it is created to the moment when the photons are detected, if they are far apart. When a measurement is made on one of the two photons, the result of the measurement on the other is immediately determined.



Here, an EPPS emits a pair of entangled photons where the quantum information is encoded into the polarization observable. The pair of photons is then prepared in a well-defined state $|\psi_{a,b}\rangle$, unlike the states of the individual photons. In other words, quantum information is encoded on the quantum object made up of the two photons, from the creation of the pair until its detection: we talk about entangled qubits. Experimentally, the photons are sent to two distant users, Alice and Bob, who each have a polarizing beamsplitter cube, set at an angle of 90° to each other, followed by two detectors. This enables them to project the state of the received photon into an analysis basis, here, the horizontal and vertical polarizations basis. By rotating the half-wave plate (red arrow), they can change the analysis basis. The crucial point is that until Bob has made a measurement, Alice's photon has no defined polarization, as it is solely the state of the pair that counts from the viewpoint of the information. This strategy enables the two communicating parties to reveal nonlocal correlations or to establish secret keys for use in cryptography operations.

are based on the principle of atomic interferometry. They detect motion-induced phase shifts between matter waves that have travelled along the two paths (or *arms*) of an interferometer (see *Fig. 5*). These accelerometers and gyroscopes can measure acceleration or rotation extremely accurately, thus making them highly reliable for inertial navigation systems.

When these interferometric systems are vertically positioned, they can be used as gravimeters. The atoms fall under the effects of gravitational acceleration (g), which can therefore be continuously measured for an unlimited time as an absolute value, with a relative uncertainty of less than 1‰. Present and future applications for these kinds of systems lie in seismology as well as oil, gas and mineral exploration.

Interferometry is also key to the functioning of atomic clocks - quantum systems that measure electron transition frequency. Now used in the field of optics, the latest generations of atomic or cold-atom clocks achieve truly spectacular precision (drift of just one second in 14 billion years, the believed age of the universe!). They can serve many purposes, such as defining universal time (synchronization of all clocks on Earth), enhancing the current Global Positioning System, and facilitating space navigation. Their sensitivity to gravitational shift means that they can complement gravimeters, which will doubtless be used in the future to improve our knowledge of the geoid. All these laboratory quantum instruments are set to become more compact, and some are already being made market ready, such as the gravimeters designed and manufactured by the Bordeaux-based company Muquans.

Major advances in the control and reduction of classical sources of noise mean that the sensitivity of these sensors will soon reach the *fundamental limit* of the achievable signal-to-noise ratio (i.e., *quantum noise*). Current research is therefore focused on finding ways of going beyond this limit, using particular quantum states of matter or radiation (e.g., spin-squeezed states). By applying the appropriate optical method, it is possible to reduce fluctuations in the intensity of a light beam to the detriment of fluctuations in phase, or even reduce fluctuations in the position of atoms in a gas to the detriment of fluctuations in their speed. Advanced LIGO and Advanced Virgo, two giant laser interferometers that were built to detect cosmic gravitational waves, are currently undergoing squeezed light upgrades to enhance their sensitivity.

Lastly, photonics-based precision measurement techniques are also starting to emerge, notably with the use of pairs of entangled photons to determine optical material properties such as the refractive index and chromatic dispersion. Scientists are already talking about quantum white-light interferometry, which could lead to the development of new fibre optic systems operating on new wavelengths, such as lasers for medicine or molecular spectroscopy.

Benefits for society

We can start by saying that none of the quantum technologies described here could have been imagined as little as 30 years ago. Today, the long-held dreams of scientists across many different disciplines – not least physics and computer science – are finally being fulfilled, as subtle theories and sophisticated experiments give rise to exciting new technologies. Although it is too early to say how long it will be before these are commercially produced on a small or large scale, they are bound to change our daily lives. But will it be to the greater good of humanity? Given the threat of terrorism, some may wonder whether totally secure communication is really such a good thing, but then again, if it becomes possible one day to hack the classical keys to certain state secrets, then global geopolitics will be thrown into disarray. Taking this to its logical extreme, if the security of the classical Internet we all use can no longer be guaranteed, what will be the consequences for the world in which we currently live? The ethical ground rules for the responsible use of all these new quantum technologies have yet to be laid down. We can nonetheless look forward to the optimization of existing processes through quantum computing and algorithms, and the use of quantum sensors to provide increasingly accurate measurements of physical parameters. ■

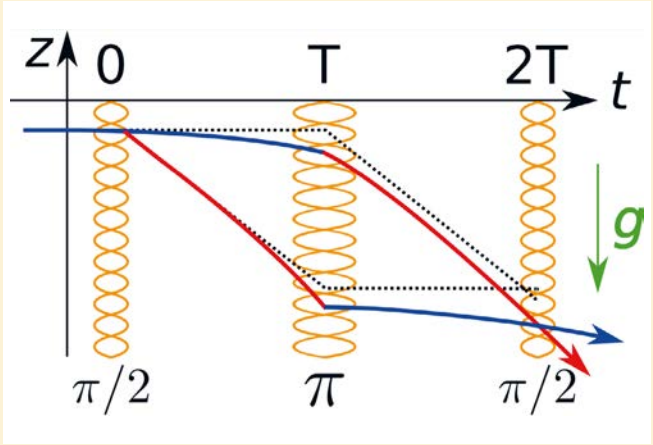


Figure 5. Diagram showing the working principle of an atom interferometer using free-falling cold atoms. The z-axis represents acceleration due to gravity (g) in the vertical direction. Matter waves arriving from the left interact three times with stationary laser beams that apply pulses to them. After the first pulse, the matter wave undergoes a phase shift of $\pi/2$ (referred to as a $\pi/2$ pulse), and is split into two propagation paths (shown in red and blue). These two colours represent the two quantum states paired by the lasers, which differ in their pulse state. The following $\pi/2$ pulse serves as a mirror, redirecting the two components of the matter wave. The interference produced after the final recombination $\pi/2$ pulse depends on the phase differential accumulated along the two arms of the interferometer. In the absence of gravity, there would be no interference (dotted lines). However, as the atoms fall vertically, the phase shift is proportional to g, which is inferred by the displacement of the interference fringes. This is how a cold-atom gravimeter is made (Courtesy of Franck Pereira dos Santos, SYRTE Laboratory, Paris Observatory).

https://doi.org/10.1051/photon/2019S446

Boost your lab's performance

AWGs

starting at
EUR 4.330,-
per channel

→ 2.4 GSa/s, 16 bit, 750 MHz
→ 4, 8 and more channels
→ <50 ns trigger latency

Typical Applications

Semiconductor testing, quantum computing, phased-array radar design & test, lidar, spectroscopy, NMR

Impedance Analyzers

starting at
EUR 9.800,-

→ DC to 5 MHz, 1 mΩ to 1 TΩ
→ 0.05% basic accuracy
→ Compensation Advisor and Confidence Indicators

Typical Applications

High-Q dielectrics, capacitive sensors, supercapacitors, PV materials, component characterization

Lock-in Amplifiers

starting at
EUR 5.400,-

→ Up to 600 MHz
→ Scope, FFT, FRA, Sweeper, Imaging tool
→ Optional: AWG, PID, PLL, Boxcar, Counter, AM & FM

Typical Applications

AFM, LVP, CARS, SRS, SNOM, graphene, optical PLL, THz, pump-probe, RFID, MEMS, NEMS, gyros, NDT, MRFM

LabOne® Software

All instruments are equipped with LabOne®, the Zurich Instruments control software, providing a wealth of features, efficient workflows and ease of use. Access your instruments from any web browser or integrate it into your LabVIEW®, MATLAB®, Python, C, and .NET programs.

Intl. +41 44 515 0410
info@zhinst.com
www.zhinst.com

Let's discuss your application
Start the conversation today

Zurich Instruments