Séminaire Poincaré 1 (2005) 223 – 233 Séminaire Poincaré

Experiments with Single Photons

Philippe Grangier
Laboratoire Charles Fabry de l'Institut d'Optique
(UMR CNRS 8501),
Bat. 503, Centre Universitaire
91403 Orsay

1 Back to the beginning : Einstein's 1905 and 1909 articles

The birth of the light quanta - "licht quanten" in their original version - is rightfully associated with the article [1] published by Albert Einstein in 1905, "An heuristic point of view about the production and transformation of light". Interestingly, several points expressed in a very collegial style in this article were exposed again in a more direct, "einsteinian" style, in a conference [2] that Einstein gave in Salzburg on september 21, 1909. This conference, entitled "The evolution of our conceptions about the nature and the constitution of radiation" reveals, and to some extend completes, the way of thinking that lead Einstein to the 1905 papers on relativity and radiation.

For instance, in 1909 Einstein gives again the list of open problems in the radiation theory, which briefly alluded to in the 1905 article. These problems were :

1. why does the appearance of a photochemical reaction depends only on the colour of light, and not on its intensity ?
2. why is short wavelength radiation generally more active chemically than long wavelength radiation ?
3. why is the kinetic energy of cathode rays (electrons) produced by the photoelectric effect independent on the light intensity ?
4. how to explain the lack of "energy dispersion" observed with X rays : secondary X-rays, produced from electrons generated by primary X-rays, may recover almost all the initial energy, while this energy should be "spread out" in free space.

This last point appears so surprising to Einstein that he writes : "From this point of view, it seems that Newton's emission theory contains more truth than the wave theory, since it says that the energy given to a light particle when it is emitted is not spread out in infinite space, but remains available for an elementary absorption process." It is then clear that Einstein wants to show that all these effects become understandable, if one admits that "the energy of light is distributed in a discontinuous way in space, as localized quanta which can move without division, and which can be absorbed or emitted only as a whole".

Another point clearly apparent in 1909 is that Einstein, though he fully admitted that Planck's formula can only be true, was really shocked by any attempt to make Planck's hypothesis compatible with the classical theory of radiation. He writes for instance : "One might believe, by looking at this (Planck's) demonstration, that Planck's formula can be considered as a consequence of the present theory of radiation. However, this is not the case, for the following reason". Then he points out on a simple example that the energy quantum $h\nu$ may be much larger (6.7 10^7 times larger in his example) than the mean energy of one oscillator. It thus appears that the energy should only take the values zero, 6.7 10^7 times the mean energy, or a multiple of this quantity. This is clearly in plain - and even shocking - contradiction with Maxwell's electromagnetic theory. Einstein's conclusion is thus : "Would it be possible to consider that this formula is true, but to provide a demonstration that does not rely on an hypothesis which is so monstrous at first sight ?".

In order to solve the dilemma, Einstein uses again thermodynamics, one of his favorite tools, and he concludes that in the domain of validity of Wien's law (the "quantum" domain), a monochromatic radiation behaves as if it was composed of independent energy quanta with a size $h\nu$. Interestingly again, he goes even further in the 1909 conference (as well as in another article [3] published also in 1909), and identifies two basic contributions to the fluctuations of radiation : one is a "particle-like" contribution, that we would call now shot-noise, and the other one is a "wave-like" contribution, which is due to random interferences, and that we would call now speckle-like fluctuations, or the Hanbury-Brown and Twiss effect. It is also really remarkable that his paper of 1925 about a perfect gas obeying the Bose-Einstein statistics [4], he recovers the same two terms, with the same interpretation - except that it applies now to "particles" and not to "radiation". In that case, the "particle-like" term appears natural, while the occurrence of a "wave-like term" is used by Einstein as a basis to a introduce "a very remarkable publication" by Louis de Broglie, which shows "how to associate a (scalar) wave field to a material particle" !

To our modern eyes, it is thus clear that through his deep analysis of thermodynamical fluctuations, Einstein was able to capture the essential features of quantum objects, which, whatever they are "classically", can exhibit both "particle-like" and "wave-like" fluctuations. At the end of his 1905 article, Einstein moves finally to his initial motivation, which was to solve the mysteries on the photochemical and photoelectric effects by using the light quantum hypothesis. He can thus interpret Stokes' law, and he gives the famous formula for the kinetic energy of the electrons produced by the photoelectric effect, which will be verified in 1916 by Millikan.

Despite these very convincing arguments, the light quantum hypothesis was the less successful among the three 1905 papers, in the sense that it was quasi-unanimously rejected by the scientific community. Apparently, though Einstein has insisted very much that the contradiction with classical electromagnetism was already present in Planck's hypothesis, the blame was put on him for making it too "visible". Also, many physicists were advocating that the light might "trigger" the photoelectric effect, rather than directly induce it. Nevertheless, the minds slowly evolved, and the last enemies of the light quantum vanished after the experiments done by Compton at the beginning of the 20's, on the energy-momentum conservation in the collision between an electron and a X-ray photon. The Nobel prize was attributed to Einstein in 1921, "for his services to Theoretical Physics, and especially for his discovery of the law of the photoelectric effect". In 1926 Gilbert Lewis invented the name of "photons", by which the light quanta have been known ever since.

One century later, what can we learn from these old debates ? We may first remember Planck's famous quotation, "truth never triumphs, but its enemies eventually die". First, it is clear that Einstein's arguments on the fluctuations were extremely strong, and should have been enough to convince his colleagues. On the other hand, the situation about the photoelectric effect itself was actually not so clear. Actually, it has been shown later that photoemission, taken by itself, does not really "prove" the quantization of the light. This can be realized by calculating [5] the ionization probability of quantized atoms submitted to a classical (wave-like) field oscillating at frequency ν : one does find the energy threshold effect, and even Einstein's formula. But then $h\nu$ appears from Fermi's golden rule, due to Bohr's formula $\nu = (E_{initial} - E_{final})/h$, rather than from the field quantization. Though the consistency of such a "semi-classical" model can be questioned, a full proof of the quantization of the field from photocounting events had yet to come. Of course, isolating a single photon would have put this ambiguity to an end. But in spite of its early birth, a single photon had never been "seen" for the first eighty years of its existence, essentially because it had not been possible to control how individual photons are emitted by a light source.

2 Quantum optics and the photon.

Things started to change between the late 1960's and early 1980's, with the emergence of quantum optics, a discipline dedicated to the study of the quantum properties of light and, of course, of photons. It was then realized that quantitative discrepancies between the fully quantized and semi-classical descriptions of light-matter interaction can hardly be found by looking at single photodetection events, but that they appear straightforwardly when looking at correlations between several - in practice, at least two - photodetection events.

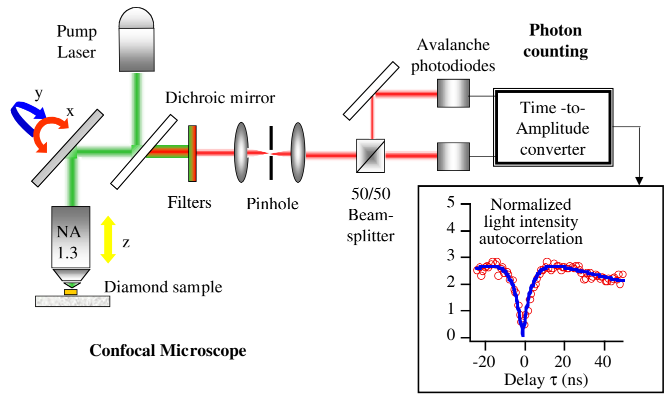

Figure 1: Modern version of an antibunching experiment : A single emitting dipole (here a colour center in a diamond nanocrystal) is irradiated by a continuous-wave green laser. The red fluorescence from the center is collected and split towards two photon-counting detectors (avalanche photodiodes). The number of coincidence counts vanishes at zero delay (i.e. for simultaneous detections), and increases at later times : this "antibunching effect" is the signature of the quantum character of the light emitted by a single dipole.

Since the proof of the photon is the "seeing", the first question that could be asked was "if we somehow can isolate a single photon, how can we see that we actually have one and only one photon?" A clever trick is to send that unknown state of light onto a beamsplitter (i.e. a half-silvered mirror), so that half the intensity is reflected and half is transmitted. Since a single photon cannot be split into two halves, it will **either** be reflected **or** transmitted with 50/50 probabilities, but will never go both ways at once. So, if sensitive photodetectors are set in each of the two outputs of the beamsplitter, the probability of both detectors producing an electric pulse simultaneously will be at a minimum, in other words the two pulses will never be bunched. A first experiment [6] along these lines was realized by John Clauser in 1974, and then the "antibunching" effect [7] itself was observed in 1976 by Leonard Mandel and coworkers in Rochester (fig. 1). It clearly appeared as a phenomenon that is truly due to the quantum mechanical nature of light, since only quantum mechanics could provide a consistent explanation of the observed results.

Shortly after this experiment, scientists started playing with it to illustrate and verify all the strange things taught in elementary quantum mechanics courses, many of which had remained for all these decades as unchecked articles of faith. Beyond the antibunching effect, an important goal was to generate a "single photon state", that is the first excited state of the quantized radiation field, containing only one quantum of energy. Such states were produced simultaneously in 1986 in Rochester by Chung Ki Hong and Leonard Mandel [8], and in Orsay by Philippe Grangier, Gérard Roger and Alain Aspect [9], by using light sources which emit *pairs* of photons. The detection of the first photon in the pair "heralds" the second one, and at that instant the electromagnetic field is prepared in a "single photon state". For an ideal single photon state, the probability of joint detection on both sides of the beamsplitter is strictly zero - the photon does not split (see fig. 2). In addition, the Orsay team set out to illustrate the wave-particle duality of quantum mechanics. They reasoned that the photon behaves like a particle because, by determining which detector got activated, we are actually answering a particle-like question, namely "which way did the photon go when it hit the beamsplitter ?" But by putting a second half-silvered mirror to make a Mach-Zehnder interferometer (fig. 2) they could see the interference of the two paths that the single photon could take, thus bringing into evidence its wave-like nature. In other words, by not trying to answer the question of which way the photon went, they allowed it to go **both ways** at once and produce an interference pattern, just like any wave would do.

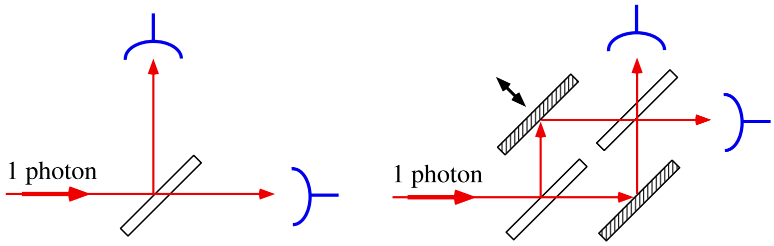

Figure 2: Wave-particle duality for a single photon : A one-photon state of the light is prepared and sent towards a beamsplitter. In the left part of the figure, the single photon exhibits a particle-like behaviour : it is detected by either one of the detectors, but there is never a "double click". One would conclude classically that the photon "chooses its way" on the beamsplitter. In the right part of the figure, the output beams are recombined to form a Mach-Zehnder interferometer. For a single-photon input, the photon output channel can now be controlled by moving any of the two mirrors (double arrows on the figure) : for instance, one can adjust the mirror's position so that the photon always goes to the upper channel (with probability one). This is the single-photon equivalent of having a totally destructive interference in the lower channel ("real" fringes can also be reconstructed by sending many individual photons, for various mirrors positions). Classically, one would conclude that each photon has to go through both ways like a wave, but this conclusion is contradictory with the previous one. Only the quantum theory of light is able to give a consistent description of both experiments.

3 Using single photons : Quantum Key Distribution

In the meantime, scientists started thinking of how to exploit the quantum properties of the photon to do useful things. Transmitting information by coding it on a train of single photons is not such a good idea, since transmission losses would produce random deletions of photons, thus making any predetermined message unintelligible. However, a random number does not suffer from this disadvantage, since it remains random (but not the same) after a random decimation of its digits. And random numbers constitute a valuable resource, because they cannot be guessed and can therefore be used as cryptographic keys to encode messages for subsequent secure transmission. In 1984, Charles Bennett and Gilles Brassard proposed a protocol [10] (known as BB84), for sending a random number using a train of single photons. This turned out to be a very fruitful idea that gave birth to a new research field, often called "quantum cryptography", or more technically "quantum key distribution" (QKD). Over the years, a large number of groups explored both the theoretical and experimental sides of these ideas. The security proofs of QKD became more and more powerful and general, while hardware implementations of QKD systems made considerable progress.

The BB84 protocol for sending a random sequence of bits permits the authorized users (often named Alice and Bob) to detect any attack in which an eavesdropper (usually called Eve) tries to intercept the key, for instance by measuring each photon and then re-emitting it so as not to interrupt the transmission. The security of the transmission is unconditionally guaranteed by a strategy based on the quantum theory of measurement and the use of superposition states. For that purpose, the bits are coded by establishing a non-unique correspondence between a bit value and the polarization states of the photon. For example, the bit values 0 or 1 may be coded by emitting a photon polarized along $\hat{x}$ or along $\hat{y}$ respectively (fig. 3).

Alternatively, the "diagonal" basis may be used to encode 0 and 1 by polarizing the photon along $\hat{u}$ or $\hat{v}$ respectively. We may remark, however, that since the two bases are not orthogonal to each other, a definite bit value in one of them is expressed as a superposition state in the other, for example $\hat{u} = (\hat{x} + \hat{y})/\sqrt{2}$. During the transmission the two bases are interchanged randomly, so that a receiver who does not use the same basis as the emitter will receive a superposition state

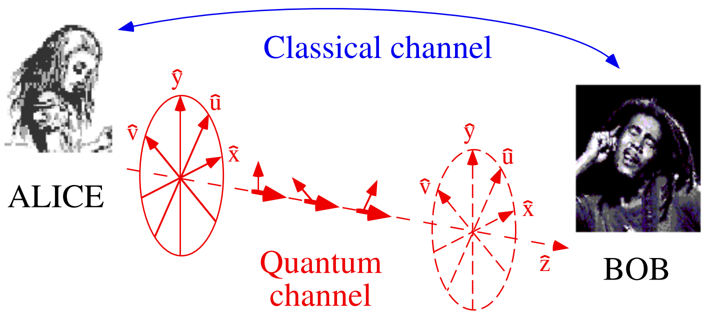

Figure 3: Quantum Key Distribution : Using the quantum channel, Alice sends to Bob a stream of photons that are individually polarized along any of the four directions $\hat{x}$, $\hat{y}$, $\hat{u}$,$\hat{v}$. By agreeing on the measurement basis after Bob has received the photons, and comparing a subset of the exchanged data through the public channel, Alice and Bob can extract a fully secure secret key.

and thus get erroneous results half of the time. For example, if a 0 is coded by emitting a photon polarized along $\hat{x}$ but the measurement is carried out in the diagonal basis, the photon will be detected with equal probability to have a $\hat{u}$ or $\hat{v}$ polarization (thus interpreted as a 0 or a 1 with equal probability), producing an error half of the time. This is not a problem for Alice and Bob, because after the transmission is complete they can compare the basis sets used in emission and reception and discard the events in which the basis sets were different. When the eavesdropper, however, uses the wrong basis set in the course of the transmission (and this will occur statistically for half of the bits received) she has no way of comparing it with the basis used in emission, and thus the errors in her reception mean that she retransmits erroneous data 25% of the time. The legitimate users can then detect the presence of the eavesdropper simply by comparing a random sample of the bits received to obtain the error rate of the transmission.

In practice, there are always transmission errors, and merely interrupting the transmission as soon as the error rate increases (possibly due to Eve, but possibly not), would not be of great use to Alice and Bob. But a crucial point is that, as long as the error rate is not too large, the authorized parties are always able to extract from the exchanged quantum data a secret key that is *absolutely secure*. This is obtained by using provably secure classical algorithmic techniques, known as "privacy amplification", that rely on suitably designed hashing functions. As a result, the effect of an increase in the error rate will be to decrease the rate of transmission of the secret key, but not its security. Obviously, only a finite error rate is tolerable, and in practice the secret key rate drops to zero when the error rate goes above a value close to 15%.

Presently, several laboratories have demonstrated the quantum transmission of a cryptographic key in optical fibers, for distances up to 70 kilometers and transmission rates on the order of a few kbits/s [11]. Such systems are now commercially available, from companies such as "id Quantique" based in Geneva [12]. These devices may be relevant for specialized economic niches that require absolute security over concentrated areas, like business or management centers, and that are not too sensitive to cost and infrastructure complexity. There has also been proposals to implement global key distribution by using satellite-borne QKD.

Research on quantum key distribution has also stimulated interesting technological developments, in particular in the field of single photon detectors. Silicon avalanche photodiodes (APD) are sensitive enough to detect single photons in the visible and near-infrared range, and have found uses in many fields, for instance in single-molecule detection for biological applications. In the window of minimal attenuation in optical fibers (1550 nm) which is interesting for long distance telecom transmissions, QKD applications have pushed forward the development of InGaAs APDs, and although their performance does not match yet that of silicon APDs, complete photon-counting devices are now commercially available. QKD has also stimulated technological progress in other domains, such as non-linear optics (e.g. high-efficiency parametric fluorescence in periodically poled waveguides), and software (such as the full-size quantum cryptography software “QUCRYPT” designed by Louis Salvail, and now publicly available [13]).

4 Single photon sources

A research area on which QKD has had a particularly deep impact is the development of novel light sources. To date, most of the practical realizations of QKD have relied on strongly attenuated laser pulses, with an average number of photons per pulse much smaller than one. But in that case the Poisson photon statistics of laser light imposes two unwanted consequences : first, a fraction of the pulses contain two or more photons, and this is an open door to information leakage towards an eavesdropper; second, most of the attenuated laser pulses actually do not contain any photons at all, thus resulting in penalizingly low transmission rates. Clearly, an efficient source able to emit one, and only one, photon in each light pulse would considerably improve the performance of QKD systems, especially in high-loss situations, such as satellite communications. The need for such light sources, combined with the more fundamental interests of academic laboratories - improving our understanding and mastering of quantum optics - have given a strong impetus to research for sources capable of emitting single photons “on demand”, and a great variety of approaches have been proposed and implemented in recent years [14].

At the heart of all single photon sources lies a single nanoscopic object, which is small enough so that a transition between its electronic states corresponds to light emission from a single Such is the case, for example, of an atom, a molecule or a semiconductor nano-aggregate. If such an emitting dipole is brought to an excited state, then from the mere conservation of energy it will emit one only photon. In general, spontaneous photon emission can occur in any direction, and thus usually only a very small fraction will go in a direction where it can be useful, making the emitter very inefficient. To increase efficiency, the nanoscopic emitter can be embedded in a high finesse optical cavity whose dimensions are of the order of the optical wavelength, that is a few hundred nanometers. Microscopic optical cavities are subject to “Cavity Quantum Electrodynamics” effects in which the structure of the electromagnetic field and the spontaneous emission are modified. In particular, in the so-called “Purcell effect”, spontaneous emission into the cavity modes can be greatly enhanced, so that most emitted photons are funneled in one particular direction and thus generate a highly directional output beam. In addition, a “user-friendly” single photon source should preferably work at room temperature, it should have a high quantum efficiency, and it should be able to achieve a high pulse repetition rate without blinking or burning out.

Such single photon sources were achieved first by using single molecules, such as as terylene embedded in a crystal of para-terphenyl, which was used first at cryogenic temperatures, and then at room temperature. Other candidates, such as rhodamines or cyanines, have also been identified, but a significant drawback of molecules at room temperature is that they irreversibly turn off after some irradiation time. The exact mechanism responsible for this photobleaching is still under investigation, and improvements may occur in the future.

Another well-explored system, studied both in the United States and in Europe, is the single self-assembled semiconductor quantum dot, consisting of an InAs nano-aggregate embedded in GaAs. The single photon that is emitted when one electron hole pair is injected in the quantum dot can easily be identified thanks to its wavelength. In addition, in view of maximizing the collection efficiency of the single photon that is emitted, the InAs quantum dots can easily be incorporated in a microcavity (fig. 4) made of semiconductor through the standard processing technologies used for microelectronics. In such systems, cavity-enhanced spontaneous emission (Purcell effect) has been observed experimentally to be faster than in free space by a factor of up to 20, while factors of several hundred should be possible according to theory. Presently, quantum dots operation requires liquid helium temperatures, but this should improve in forthcoming years.

Another avenue is using individual nitrogen-vacancy (NV) color centers in diamond. The NV centers have many similarities with molecules but are extremely photostable, even at room temperature. Another advantage is that they appear both in bulk diamond or in diamond nanocrystals, and are therefore easy to manipulate (fig. 1). A stable source emitting single photon pulse trains based on an NV center in a diamond nanocrystal excited by a small solid-state laser was recently

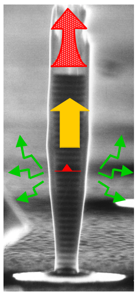

Figure 4: Electron micrograph of a GaAs micro-post cavity. The photons are emitted by an InAs quantum dot (depicted schematically by a triangle) embedded in the center of the microcavity, and resonant with the fundamental cavity mode. These photons will be channeled preferentially into that mode, and thus produce a highly directional beam (image : Izo Abram, LPN Marcoussis).

implemented in Orsay [14]. The overall system is a reasonably compact, all-solid-state set-up operating at room temperature, that is probably the simplest single-photon source developed so far. Using this compact source delivering trains of single-photon pulses, Alexios Beveratos and his colleagues were able to demonstrate a complete quantum key distribution scheme [14, 15], where the rate of pulses containing two photons is strongly reduced with respect to an attenuated laser (by a factor 14 for the same rate of one-photon pulses). This makes interception by the so-called "two-photon attacks" virtually impossible. The cryptographic exchange is then more robust with respect to on-line losses, providing a clear advantage over an attenuated laser source for QKD applications. The performance of this set-up should improve further in a near future, providing a highly efficient, easy to use, and reliable single photon source that would constitute a basic piece of hardware for practical quantum key distribution (see fig. 5).

Another way to avoid two-photon attacks is to use the trick of "heralded" single photons, that was used in 1986 to produce single-photon states as said above. In the context of quantum cryptography, the experiment was realized e.g. in Geneva, by using pairs of twin photons, generated by a nonlinear optical process called "parametric downconversion", so that one member of the pair heralds its twin. The quantum mechanical "entanglement" that exists between the twins was also exploited with success. Though these schemes produce photons at irregular intervals, with effective counting rates that are subject to various technical limitations, they do provide also quite interesting QKD schemes [11].

Finally, schemes based on single trapped atoms or ions in high-finesse cavities are clearly more complex to implement, but might produce single photons with interesting spectral properties, as discussed in the section below. State-of-the-art results were obtained by dropping or trapping cold atoms through a high-finesse cavity : when going through the cavity each atom emits a burst of single-photon pulses. Each photon emission is triggered by a sequence of laser pulses, including excitation, emission in the cavity mode, and repumping to the initial level. Several recent results along these lines are described in ref. [14].

5 Coalescing photons

Looking further to the future, several recent proposals for all-optical quantum photonic networks have been advanced recently based on indistinguishable single photons acting as flying qubits, carrying information from node to node and interacting with each other. These ideas can even be extended towards the realization of a full-fledged quantum computer, using a scheme that was proposed recently by Emmanuel Knill, Raymond Laflamme and Gerald Milburn. For such schemes to work, photons must be indistinguishable, that is they must be in the same "single mode of the electromagnetic field". In should be noted that most of the single-photon sources described above produce photons that are incoherently spread over many modes of the radiation field and, although

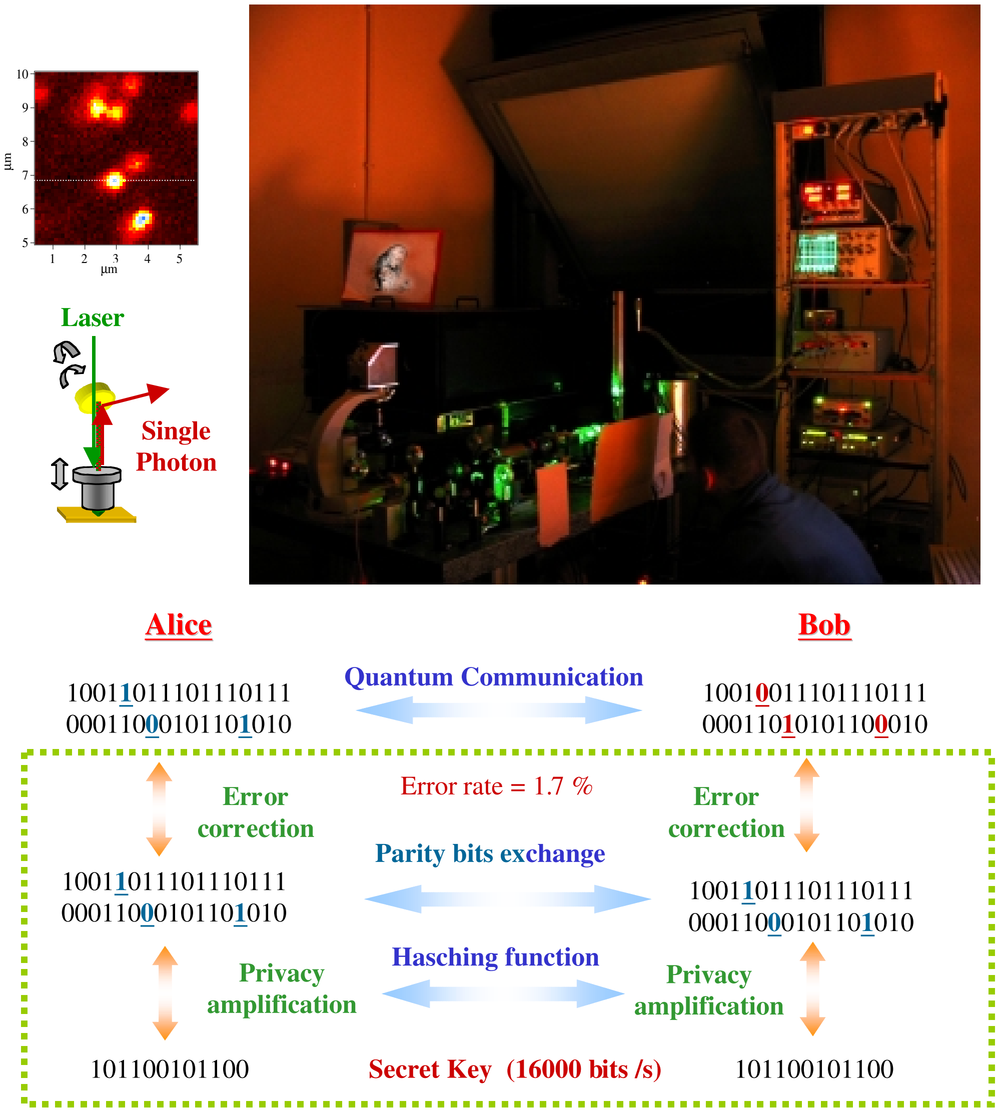

Figure 5: Quantum key exchange with a single photon source, obtained by exciting diamond nanocrystals by a pulsed laser. The upper left image shows light emission by the diamond nanocrystals (bright spots on the image). The upper right photograph shows the experimental set-up, where the photons are sent though a window to Bob's detection apparatus, located in another building. The lower part of the figure shows the various steps of the protocol which is used to extract the final secret key.

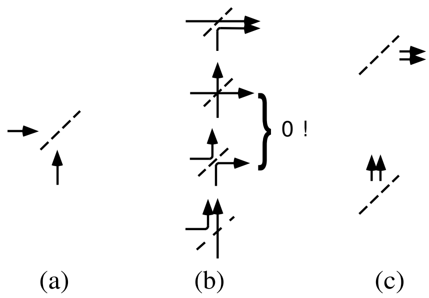

Figure 6: Coalescing photons on a beamsplitter : When two "single mode" (but otherwise independent) photons enter a 50-50 beamsplitter (a), they may be transmitted or reflected in various ways, as shown in (b). In particular, both photons may be transmitted, or both may be reflected, and it happens that the corresponding probability amplitudes cancel out. Then the two photons must go to the same output beam, as shown in (c) : they "coalesce" on the beamsplitter.

they are usable in QKD, they do not have the appropriate properties for quantum computation.

In order to illustrate what is specific to indistinguishable photons, let us consider fig. 6(a) : Two photons are sent onto a beamsplitter, in such a way that when one photon is transmitted it ends up in exactly the same mode as the other photon which is reflected. The four possible configurations for the two photons being transmitted or reflected are depicted in fig. 6(b). As it is usual in quantum mechanics, a probability amplitude in attached to each of these configurations, and it turns out that the amplitudes of the two diagrams in the middle of fig. 6(b) (both corresponding to one photon in each of the two output ports of the beamsplitter) have opposite signs. Clearly, if the two photons are indistinguishable (having exactly the same frequency, direction, and polarization) the two diagrams are identical and, since their amplitudes are of opposite sign, they cancel each other out! The immediate consequence of the two surviving diagrams is that the two photons must go to the same output beam : They "coalesce" as they meet on the beamsplitter to form a "two-photon state", that is the second excited energy state of the corresponding mode of the quantized electromagnetic field. This surprising quantum interference effect was first predicted and observed in 1987, by Leonard Mandel and coworkers. They used actually pairs of "twin photons", simultaneously produced in parametric down-conversion, so it was possible to argue that the two photons knew about each other before, since they were "twins" emitted in a single parametric fluorescence event. Would it be possible to get the same effect by using truly independently emitted (albeit indistinguishable) photons? The quantum answer to this question is yes, and it is not pure rhetoric, because interference between independently emitted photons is actually what is required for applications in quantum information processing, using the Knill-Laflamme-Milburn scheme.

The coalescence of two indistinguishable but independently generated photons, from a source consisting of a single quantum dot in a semiconductor microcavity, was experimentally demonstrated very recently in Stanford [16]. This experiment can be seen as a first step towards the realization of conditional quantum logic gates that would make photon-based quantum computing possible. But difficulties should not be underestimated : with present-day setups the error rates would be by orders of magnitude too large, compared with the range where quantum error-correcting codes can play an efficient role. Also, the number of interfering photons required to implement a useful computation is huge, and the integration of the devices would have to be pushed well beyond the present technological capabilities.

6 "En guise de conclusion" : towards entangled photons on demand

Photon pairs emitted in parametric downconversion have often been mentioned above, because they have many applications in quantum optics : conditional preparation of single photon states, quantum key distribution, and last but not least, they can be prepared in an entangled state. When two photons are entangled, their states are always correlated no matter how we choose to measure them, as if the two photons constituted a single quantum object. For instance, a pair of polarization-entangled photons will exhibit correlations in every possible polarization basis, and performing polarization correlation measurements on the two photons once they are far apart leads to a violation of Bell's inequalities. This means that the correlations that appear between the results of the polarization measurements on the two remote photons are so strong, that no classical model based on "local realism" is able to explain them. In quantum information processing, such a quantum entanglement is a "resource", because it cannot be created by local actions on two remote photons, and it allows one to perform some specific tasks, such as quantum teleportation of the (unknown) polarization state of a third photon. Entangled photon pairs also provide a way towards the so-called "quantum repeaters", that would allow one to develop quantum key distribution schemes over arbitrarily long distances (it is noticeable that "classical repeaters", commonly used in optical telecommunication, do not preserve the quantum cryptographic security).

Presently, the main source of entangled photon pairs are parametric fluorescence events, but these events are essentially random, so that the pair production process obeys Poisson statistics. In the same way as deterministic single photon generation is useful, deterministic pair production would allow new quantum communication protocols to be developed. How can this be achieved? One may simply try to improve upon the old idea of the radiative cascade, that was used in the 70's and 80's for performing experimental tests of Bell's inequalities. But instead of using many-atom sources as it was done at that time, one should use a two-photon radiative cascade of a single emitter. Several groups have shown that a quantum dot does display such a cascade, corresponding to the radiative transitions between the electronic states of the quantum dot containing two, one, or zero electron-hole pairs. However, the first experiments did not produce the results hoped for : The photons exhibited correlations only for one polarization basis. In other words, they were correlated as if they were classical objects, and were not entangled quantum mechanically, because, apparently, decoherence processes in the quantum dot rapidly destroy the entanglement. Exploitation of the Purcell effect to reduce the radiative lifetime beyond the decoherence time should, in principle, permit the production of entangled photon pairs "on demand".

While the long-term goal of building a quantum computer is far-fetched, a medium-term goal for these experiments is to develop long-distance quantum communication networks, that would allow for the implementation of QKD systems over arbitrary large distances. One may think also about more elaborate protocols, able to share a quantum secret between many (rather than two) users. Such things are presently still far from being implemented, but this is one very fascinating aspects of quantum information : by exploiting the strangest properties of single photons and single atoms, it allows us to move continuously from science to science-fiction, and back.

References

[1] This article and the following ones are translated in french in "Albert Einstein : Quanta", by F. Balibar, O. Darrigol and B. Jech, Éditions du Seuil, Paris, 1989.

A. Einstein, Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt, *Annalen der Physik* **34**, 591 (1905).

[2] A. Einstein, Über die Entwicklung unserer Anschauungen über das Wesen und die Konstitution des Strahlung, *Physikalische Zeitschrift* **10**, 817 (1909)

[3] A. Einstein, Zum gegenwärtigen Stand des Strahlungsproblems, Physikalische Zeitschrift **10**, 185 (1909)

[4] A. Einstein, Quantentheorie des idealen gases, *Preussische Akademie des Wissenschaften, Phys.-math. Klasse, Sitzungberichte* 18 (1925).

[5] W.E. Lamb and M.O. Scully, *The Photoelectric Effect Without Photons*, in "Polarisation, Matière et Rayonnement", ed. A. Kastler, Presses Universitaires de France, 363–369 (1969).

[6] J.F. Clauser, Experimental Distinction Between the Quantum and Classical Field Theoretical Predictions for the Photoelectric Effect, *Phys. Rev. D* **9**, 85 (1974).

[7] H.J. Kimble, M. Dagenais and L. Mandel, Photon antibunching in resonance fluorescence, *Phys. Rev. Lett.* **39**, 691 (1977).

[8] C.K. Hong and L. Mandel, Experimental realization of a localized one-photon state, *Phys. Rev. Lett.* **56**, 58–60 (1986).

[9] P. Grangier, G. Roger and A. Aspect, Experimental evidence for a photon anticorrelation effect on a beam-splitter : a new light on single-photon interferences, *Europhysics Lett.* **1**, 173 (1986).

[10] C.H. Bennett and G. Brassard, Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 175 (1984).

[11] A review on quantum cryptography may be found in : N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).

[12] id Quantique SA, http://www.idquantique.com

[13] http://www.cki.au.dk/experiment/qrypto/doc/

[14] Many experimental results on single photons pulses can be found in three special issues :

"Quantum interference and cryptographic keys : novel physics and advancing technologies (QUICK)", in *The European Physical Journal D* **18** (2) (February 2002), edited by P. Grangier, J.G. Rarity and A. Karlsson;

"Proceedings of the Tenth International Conference on Modulated Semiconductor Structures (MSS 10)", in *Physica E* **13** (2-4) (March 2002), edited by G. Bauer;

"Focus on Single Photons on Demand", in New Journal of Physics **6** (2004), edited by P. Grangier, B. Sanders and J. Vukovic (free access at http://www.iop.org/EJ/abstract/1367-2630/6/1/E04).

[15] A. Beveratos *et al.*, Single photon quantum cryptography, *Phys. Rev. Lett.* **89**, 187901 (2002);

[16] C. Santori *et al.*, Indistinguishable photons from a single-photon device, *Nature* **419**, 594 (2002).