What are single photons good for?
Nicolas Sangouard & Hugo Zbinden

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

TUTORIAL REVIEW

What are single photons good for?
Nicolas Sangouard* and Hugo Zbinden

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

(Received 2 February 2012; final version received 16 April 2012)

In a long-held preconception, photons play a central role in present-day quantum technologies. But what are sources producing photons one by one good for precisely? Well, in opposition to what many suggest, we show that single-photon sources are not helpful for point to point quantum key distribution because faint laser pulses do the job comfortably. However, there is no doubt about the usefulness of sources producing single photons for future quantum technologies. In particular, we show how single-photon sources could become the seed of a revolution in the framework of quantum communication, making the security of quantum key distribution device-independent or extending quantum communication over many hundreds of kilometers. Hopefully, these promising applications will provide a guideline for researchers to develop more and more efficient sources, producing narrowband, pure and indistinguishable photons at appropriate wavelengths.

Keywords: single photons; QKD; quantum optics (inc. quantum information)

1. Introduction

Single-photon sources are widely developed worldwide.1 Some produce single photons in a heralded way, e.g. from a pair source, the detection of one photon heralding the production of its twin. Others produce them on-demand, e.g. using a single quantum emitter. But what for?

For fun? Certainly. Because physicists enjoy manipulating individual quanta. Fine. But, you may have noticed that this argument does not provide good enough motivations for research proposals. Applications, even hypothetical, are often necessary to obtain research funding.

To build up a quantum computer? Maybe. It has been shown that linear optical quantum computing could work if the product of the detector efficiency and the single-photon emission probability is greater than 2/3 [3] (and even greater than 1/2 if one uses photon pair sources [4]) provided that the sources never emit more than one photon, that the corresponding photon wavepacket is pure and that the emission is perfectly indistinguishable from one source to another. But maybe not. A more realistic study, taking the multi-pair emissions into account, has recently shown that very basic entangling gates require photon-detector and single-photon sources with efficiencies of about 0.9 and single-photon purities ($g^2$ second-order autocorrelation function) better than 0.07 [5]. Note that these performance levels do not allow one to perform a useful calculation nor to show the superiority of quantum computation over its classical counterpart. They merely correspond to a guideline, e.g. for the implementation of a heralded entangled photon pair.

For quantum communication tasks? Good question. Quantum cryptography has become the field of preference for many of us [6]. This is an exciting research domain that benefits from the more fascinating concepts lying at the intersection between quantum physics and information theory to securely exchange keys. However, as quantum cryptography becomes more and more mature, we now know what it requires and what it doesn’t. For example, many developers of single-photon sources state that their device is useful for point to point quantum key distribution (QKD). But as we will see in the next section, high secret key rates can be achieved much more conveniently using weak laser pulses with appropriate protocols.

It is thus natural to wonder whether a source producing single photons is a useful resource. The aim of this paper is to highlight the central role that single-photon sources could play for future quantum communication. In Section 2, we recall the requirements to make single-photon sources useful for standard quantum key distribution protocols and we conclude that faint laser pulses do the job better today and will likely provide superior performance for a long time. We show in Section 3, that single-photon sources may open the way for new kinds of QKD protocols, which exploit non-local correlations to make the security of the key independent of the device that is used to

*Corresponding author. Email: Nicolas.Sangouard@unige.ch

ISSN 0950-0340 print/ISSN 1362-3044 online
© 2012 Taylor & Francis
http://dx.doi.org/10.1080/09500340.2012.687500
http://www.tandfonline.com
produce it. Interestingly, this would turn quantum non-locality from a fundamental question to an applied physics concept. The price to pay is that the photons need to be created with high efficiencies, at high rates, in pure and indistinguishable states and at telecommunication wavelengths. We also recall that, in this context, the on-demand production of photons would greatly speed up the secret key rate. In Section 4, we focus on long-distance quantum communication using quantum repeaters. We show how single-photon sources can be used to build up efficient architectures, significantly more efficient than protocols based on currently available photon-pair sources. We show that in addition to being in pure and indistinguishable states, the photons produced on-demand need to be compatible with the memory bandwidth to be useful in the framework of quantum repeaters. The last section is devoted to our conclusion.

2. Requirements for QKD

QKD enables two parties, Alice and Bob, to share a random key known only by them, which can be subsequently used, e.g. to communicate in a secure way [9]. QKD protocols rely on the fascinating quantum property that information gain is impossible without introducing errors if the communication relies on non-orthogonal quantum states. In other words, the laws of Nature make QKD secure.

If you sketch QKD on a piece of paper, it is natural to consider a perfect single-photon emitter as a light source. By doing this, the security analysis is rather simple, as a potential eavesdropper, Eve, has no means to split the signal. However, if you are an experimentalist, you will quickly understand that the realization of a true single-photon source is not a piece of cake. You will be tempted to use strongly attenuated laser pulses |a⟩ as an approximation for single photons, choosing an average photon number per pulse μ = |a|² of less than 1, say 0.1. This approximation seems reasonable in the sense that the chance of finding two or more photons in a pulse becomes small (about 0.5% in this case). So, most early experiments of QKD were based on such faint laser sources without remorse with μ = 0.1. However, it was pointed out by Brassard et al. [7] that if the transmission of the quantum channel is actually smaller than the probability that a non-empty weak pulse contains more than one photon |

\[ (\alpha|\sum_{n>0} n)\|^2/(|\alpha|\sum_{n>0} n)\|^2, \]

the scheme is no longer secure. Indeed, in this case an eavesdropper can perform the so-called photon number splitting attack [7,8]. This attack consists in removing one photon of the pulses containing more than one and sending the remaining through a lossless fiber to Bob. All other pulses are blocked in order to keep the expected count rate at Bob’s location. The removed photons are stored in a quantum memory and measured once Alice and Bob have agreed on the measurement basis during the sifting process. Therefore, Eve obtains full information about the key without creating errors. The straightforward way to rule out this attack consists in reducing the average number of photon per pulse μ accordingly to the transmission efficiency t (μ = t has been shown to be optimum for the BB84 protocol [9]). Needless to say this reduces drastically the achievable bit rates and limits significantly the maximum transmission distance.

However, one should not precipitously conclude that single-photon sources are mandatory for QKD. Indeed, there are a couple of clever countermeasures allowing one to implement efficient QKD with faint laser pulses. The simplest trick is a mere change in the sifting procedure of BB84. Instead of announcing the basis, Bob announces his measurement result. Alice now knows when Bob did not measure in the right basis and the measurement basis can be used to form the raw key. Eve, on the other hand, does not know in which basis she should measure her photon, so she cannot retrieve full information. It has been shown that the corresponding optimum μ goes with \( \sqrt{t} \) [10].

A second option is the decoy state protocol [11], where Alice varies on purpose the intensity of the pulses. By acting differently on pulses with different photon numbers, Eve will alter the detection statistics of Bob and the photon-number splitting attack can be revealed. Finally another strategy consists in checking the coherence between different qubits, which prevents Eve acting on individual qubits as it is the case in a photon-number splitting attack. The differential phase shift [12] and the coherent one-way schemes [13] are based on this strategy. It turns out that these latter protocols allow one to use rather high μ, from 0.2 to 0.5 even for very long distances.

The question is now, can single-photon sources, so-called photon guns (on demand) or heralded single-photon sources, at telecommunication wavelengths, compete with the cheap and still efficient faint laser sources? The answer is clearly no for the following reasons: (1) The collection efficiency of single-photon sources is usually very small. However, even if one assumes a high collection efficiency of say 0.8, one has to take into account additional loss, e.g. for rapid integrated phase or polarization modulations with typical loss of 2 dB or more. So finally, at the output of Alice’s device, the average number of photons will not be higher than for faint laser sources. (2) Faint laser schemes run at repetition frequencies as high as 1 GHz. This means that single-photon gun should feature a jitter below 1 ns. Moreover, a (almost)
Fourier limited bandwidth is required in order to both limit the dispersion and to allow for dense wavelength division multiplexing. This is actually not the case for any single-photon source at telecommunication wavelengths. Heralded single-photon sources based on photon-pair sources cannot achieve such a rate as it would ask for photon counters with GHz count rates. (3) Admittedly, the two points mentioned above are technological and not fundamental limitations. If some technological progress is certainly possible, it will be at an unaffordable price. A DFB laser diode is available below 1000 dollars. This is out of reach for any single-photon source, even without cryogenic cooling. A much higher price without a significantly improved performance is of course inconceivable for a commercial product.

So, single-photon sources are useless for today’s QKD systems. However, looking further ahead, we will see below that they are definitively needed for more complex schemes like for device-independent QKD and for long-distance quantum communication based on quantum repeaters.

3. Requirements for device-independent QKD

We have seen above that weak pulse QKD is perfectly secure. However, the proofs are obviously only valid for correctly implemented systems. But how can one be sure that the implementation has no weakness? Indeed, a weakness could have been introduced by the manufacturer by negligence or even on purpose. This is obviously a major problem if one wants QKD to run between two black boxes installed in banks. The solution consists either in educating the bankers on quantum physics or to submit the black boxes to some certification agencies. However, it would be much more elegant if one could demonstrate security without any assumptions about the actual devices. This has led to the concept of device-independent QKD [14,15].

Device-independent QKD relies on entanglement based protocols [16]. The principle of the latter is quite simple. When both Alice and Bob perform measurements along the $z$-direction (or along $x$) on the singlet state, they get locally random results but perfectly anti-correlated. By repeating the experiment several times and by choosing the measurement settings randomly among $\{\sigma_z, \sigma_x\}$, they each get a string of random bits. Keeping the results for which the measurement setting were identical only (and if one of them flips the bits), they get the same copy of a string of random bits, that is, a key. But how can one make the security device-independent using entanglement based protocols?

Non-locality performs this trick. Indeed, a possible way to detect entanglement is to perform measurements whose correlations violate a Bell inequality. Importantly for QKD, the violation of a Bell inequality first ensures the presence of entanglement between Alice and Bob but also forbids a third party from sharing quantum correlations with them, independently of any details about the Hilbert space dimension and the measurement devices. This opens an avenue for bankers, and for everyone who doesn’t know anything about quantum physics, to communicate in a secure way.

An experimental implementation of device-independent QKD is still awaited since hitherto, all optical Bell tests are subject to the detection loophole. Indeed, all entangled photons are not detected because of unavoidable losses and the missed events could be used to perform powerful attacks. A potential eavesdropper could force the black boxes to produce results only if the measurement settings are in agreement with a predetermine scheme. Closing the so-called detection loophole in an optical Bell test is therefore a requirement for the implementation of device-independent QKD. However, the detection efficiency (i.e. the probability that Bob gets an answer once he asks a question) that is required to rule out attacks based on the detection loophole is larger than 82.8% for the CHSH inequality [17] in the absence of other limitations. But the transmission efficiency of a 5-km-long fiber at telecommunication wavelength is roughly 80%. Hence, transmission losses represent a fundamental limitation for the realization of a detection-loophole free Bell test on any distance relevant for QKD. The question that naturally follows is thus: how can we create entangled photon pairs at a distance in a heralded way?

The solution that has been proposed in Ref. [18] revolves around performing an entanglement swapping operation. Given two entangled photons, say the photons $a$ and $b$, and another entangled pair $c$ and $d$, it is possible to entangle $a$ and $d$ by performing a joint measurement of photons $b$ and $c$ in the Bell basis, provided that the result of the measurement is communicated to $a$ and $d$ [20]. The latter two end up entangled, even through they are located at remote locations. Furthermore, the creation of their entanglement is heralded by the joint measurement. This is exactly what we were looking for. The only remaining question is how can one perform an entanglement swapping operation in practice? The most natural approach would be to use pair sources based on spontaneous parametric down conversion and linear optical elements to perform a partial Bell measurement. However, the emission of multi-pairs, inherent to spontaneous parametric down conversion, inevitably corrupts the Bell state measurement and drastically reduces the fidelity of the resulting entangled state.
An attractive solution consists in using single-photon sources, because they never produce more than one photon. This is the central idea of the proposal presented in Ref. [18] which consists in performing a conventional entanglement swapping operation but with one entangled-photon-pair source replaced by two heralded single-photon sources producing one photon each that is subsequently sent to a beamsplitter. As a consequence, the state resulting from the joint measurement is maximally entangled, independent of the loss, provided that the reflection of the beamsplitter and the probability that the pair source produces multi-photon pairs are low enough, cf. Figure 1 for details. If Bob chooses a measurement only when he gets a successful joint measurement, the overall efficiency required to rule out attacks based on the detection loophole reduces to the detection efficiency.

By considering an implementation with sources based on parametric down conversion only, producing pure and indistinguishable photons, with a repetition rate of 10 GHz, a fiber attenuation of 0.2 dB/km corresponding to telecommunication wavelength photons, coupling efficiencies into fiber of 0.9, detection efficiencies of 0.8, this proposal achieves a key rate of a few bits per minute on a typical distance of 10 km. Note that if the photons emitted from the single-photon sources are produced on-demand, the achievable key rate is increased by several orders of magnitude. The usefulness of on-demand single-photon sources in the framework of device-independent QKD is well illustrated by Figure 2.

We will now see that single-photon sources could also play a central role for quantum repeaters.

4. Requirements for quantum repeaters

The distribution of quantum states over long distances is limited by photon loss. For example, the transmission efficiency of a 1000 km long optical fiber is $10^{-20}$.

Even under a very optimistic assumption on the repetition rate of the source, say 10 GHz, this translates into the distribution of one quantum state every 300 years on average! Moreover, the problem of loss cannot be overcome by straightforward amplification as in classical communication, because of the no-cloning theorem [23]. But let us keep hope alive!

Briegel et al. [24] proposed an attractive solution that relies on the amazing properties of entanglement, the so-called quantum repeater. The principle is sketched in Figure 3. It consists in dividing the overall distance into elementary links, distributing the entanglement in each of the links, and then swapping repeatedly the entanglement between neighboring links until it is extended over the desired distance. If $\eta$ is the transmission efficiency within one link and if the quantum repeater of interest is made with $N$ links, then the average rate with which entanglement is distributed scales as $\eta^N$ for quantum repeaters whereas it scales as $\eta^N$ for the direct transmission of photons through an optical fiber. However, the price to pay is that first the distribution of entanglement in each link needs to be heralded. Furthermore, the entanglement has to be stored in each link and processed many times to be swapped between adjacent links.
Duan and co-authors [25] (DLCZ) have shown how to meet all the above requirements using linear optical elements for entanglement processing operations and atomic ensembles for quantum memories. It basically requires one photon pair source and one memory at each location. The two sources are coherently excited so that the detection of a single photon which could have been emitted from either of two sources, heralds the entanglement between the two memories, cf. Figure 4. However, because of the rapid growth (quadratic with the number of links) of errors due to multiple emissions during the entanglement swapping operations, it is necessary to work with low emission probabilities, i.e. to weakly excite the pair sources so that multi-pair emission is negligible [28]. This inevitably decreases the achievable entanglement distribution rate.

The use of single-photon sources, to eliminate errors due to two pair emissions, leads to a significant improvement in the achievable entanglement distribution rate. Let us focus on an example consisting of the distribution of entangled pairs over 1000 km and consider detector and memory efficiencies of 0.9. If one demands that the overlap between the distributed state and the singlet state is at least equal to 0.9, it can be shown that a protocol based on single-photon sources (cf. Figure 5) with source efficiencies of 0.95 and two-photon emission of the order of $10^{-4}$, achieves entanglement distribution rates 18 times greater than the DLCZ protocol [29]. Note that efficient sources are required to take advantage of the protocol of Ref. [29]. More precisely, the single-photon source protocol of Ref. [29] achieves an advantage over the DLCZ scheme as soon as the single-photon source efficiencies are larger than 0.67.

We emphasize that single-photon sources can be exploited to herald the production of high fidelity
entangled photon pairs from a probabilistic pair source based, e.g. on spontaneous parametric down conversion, as shown in Figure 1. It has also been shown in Ref. [19] how the potential imperfections affecting the states created from this source caused, e.g. by detectors with non-unit efficiencies, can be systematically purged from an entanglement swapping operation, the latter being used for entanglement creation within the elementary links. Near perfect fidelity entangled states are thus distributed in each link and this fidelity is preserved when the entanglement is extended over long distances through appropriate entanglement swapping operations. The architecture presented in Ref. [19] fully exploits the properties of single-photon sources and is currently the most efficient quantum repeater known to us based on atomic ensembles and linear optics. The resulting entanglement distribution rate is three orders of magnitude greater than that corresponding to the DLCZ protocol [25]. Still, it leads to the distribution of roughly one entangled pair every second only. However, temporal, spatial or any other form of multiplexing would greatly increase the achievable entanglement distribution (see, e.g. Ref [27]). Furthermore, protocols consuming a less secret key than the One Time Pad (e.g. Advanced Encryption Standard), could be considered as an option for encryption.

Figure 4. Heralded entanglement creation within an elementary link which is inspired by the DLCZ protocol [25]. Photon-pair sources, producing two-mode squeezed states (as obtained with spontaneous parametric down conversion in a nonlinear crystal) are coherently excited so that one of them emits a photon pair. The modes $a'$ and $b'$ are stored locally in atomic ensembles, whereas the modes $a$ and $b$ are sent to a central station where they are combined into a beamsplitter. The detection of one photon after the beamsplitter heralds the storage of a single excitation delocalized among the two crystals, i.e. the entanglement between the two memories. The entanglement can then be swapped by releasing the stored photons using linear optics and photon counting techniques [27]. (The color version of this figure is included in the online version of the journal.)

Figure 5. Heralded entanglement creation within an elementary link for the protocol of Ref. [29] which is based on single-photon sources. The two on-demand sources produce one photon each, subsequently sent into a beamsplitter. This creates entanglement between the modes $a'\sim a$ and $b'\sim b$. The modes $a'$ and $b'$ are stored locally. The detection of one photon at the central station where the modes $a$ and $b$ are combined into a beamsplitter, heralds the creation of entanglement between the remote memories (i.e. a superposition of memory A and B being excited). The swapping operations are identical to those used in the DLCZ protocol. (The color version of this figure is included in the online version of the journal.)

5. Conclusion

Single-photon sources never produce more than one photon at a time. However, present day quantum cryptographers could not care less because faint lasers are efficient, cheap and easy to use. Nevertheless, QKD would gain more users’ trust by making the security independent of the devices. Single-photon sources could play a key role in the first implementations of device-independent quantum key distribution which pleases everybody, both non-physicists and post-quantum cryptographers. In parallel, there is a need to extend the range of quantum communication. Here also, single-photon sources could well be the main ingredient for the realization of the first long-distance quantum communication based on quantum repeaters. Time will tell.

Acknowledgments

We thank Ci Wen Lim, Clara Osorio, Bruno Sanguinetti and Rob Thew for interesting discussions. We gratefully acknowledge support by the EU projects Qessence and Qscale, and from the Swiss NCCRs QP and QSIT.
Notes
1. A single-photon source is defined as a device delivering photons one at a time. Theorists would prefer to say that it creates Fock states filled with one excitation [1]. Experimentalists would emphasize that a single-photon source is characterized by a second-order autocorrelation function $g^{(2)} = 0$. See [1,2] for recent reviews on single-photon sources.

2. The loss of a typical telecommunication optical fiber is 0.2 dB/km for the optimal wavelength around 1.5 μm. Note also that optical fibers are not the only way of implementing a quantum channel. The long-distance distribution of photons through free space is also an active field of investigation (see for example [21] or [22] for nice illustrations). We emphasize that the quantum repeater principle can be applied to any kind of channel to overcome the problem of loss.

3. For a review of quantum repeaters based on atomic ensembles and linear optics, see [26].

References