Experimental open air quantum key distribution with a single photon source

R Alléaume[†] , F Treussart[†], G Messin[‡], Y Dumeige[†], J- F Roch[†], A Beveratos[‡], R Brouri–Tualle[‡], J- P Poizat[‡] and P Grangier[‡]

† Laboratoire de Photonique Quantique et Moléculaire, UMR 8537 du CNRS, ENS Cachan, 61 avenue du Président Wilson, 94235 Cachan Cedex France
‡ Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, F- 91403 Orsay France

Abstract. We present a full implementation of a quantum key distribution (QKD) system with a single photon source, operating at night in open air. The single photon source at the heart of the functional and reliable setup relies on the pulsed excitation of a single nitrogen-vacancy color center in diamond nanocrystal. We tested the effect of attenuation on the polarized encoded photons for inferring longer distance performance of our system. For strong attenuation, the use of pure single photon states gives measurable advantage over systems relying on weak attenuated laser pulses. The results are in good agreement with theoretical models developed to assess QKD security.

Submitted to: *New J. Phys.*

PACS numbers: 03.67. Dd, 42.50. Dv, 33.50. -j, 78.55. Hx

1. Introduction

Key distribution remains a central problem in cryptography, as encryption system security cannot exceed key security. Public key protocols rely on computational difficulty [1]. They cannot however guarantee unconditional security against future algorithm or hardware advances.

As Bennett and Brassard first proposed twenty years ago [2], quantum physics can be used to build alternative protocols for key distribution [3]. In their proposed "BB84" scheme for quantum key distribution (QKD), a first user (Alice) sends a second user (Bob) a sequence of single photons on an authenticated channel. Each of them is independently and randomly prepared in one of the four polarization states, linear-vertical (V), linear-horizontal (H), circular-left (L), circular-right (R). For each photon he detects, Bob picks randomly one of the two non orthogonal bases to perform a measurement. He keeps the outcome of his measurement secret and Alice and Bob publicly compare their basis choices. They only keep data for which polarization encoding and measurements are done in the same basis. In the absence of experimentally induced errors and eavesdropping, the set of data known by Alice and Bob should agree. Due to quantum physics' contraints on single photon measurements an eavesdropper (commonly named Eve) cannot gain even partial information without disturbing the transmission. The unavoidable errors introduced by Eve can be detected by the legitimate users of the quantum transmission channel. If the measured error rate is too high, no secret can be generated from the transmitted data. But if the error rate remains within acceptable bounds Alice and Bob can distill a secure secret key, perfectly unknown by Eve, using key reconciliation procedures. This perfectly secure key can then be used for data encryption.

Interest in experimental QKD has evolved from early proof-of-principle experiments [4, 5] to long distance demonstrations on optical fibers [6, 7] as well as in free space [8, 9, 10] and now to commercial products [11, 12]. Nevertheless, several technological and theoretical barriers still have to be overcome to improve performance of current QKD systems. Most of them relie on weak coherent pulses (WCP) as an approximation to single photons. Such classical states are very simple to produce but a fraction of them will contain two photons or more. Since information exchanges using such multiphotonic pulses can be spied on by potential eavesdropping strategies [13, 14], security hazard is introduced in the key distribution process. For QKD schemes relying on WCP, one has finally to throw away part of the initially exchanged information, proportional to what an eavesdropper could have learned from it. Indeed, in WCPs' schemes, the probability for multiphotonic pulses is directly connected to the mean intensity of the initial pulse that must therefore be attenuated more and more to guarantee security as line losses become higher. Therefore either transmission rate at long distance becomes vanishingly small or complete security cannot be guaranteed.

The use of true single photon source (SPS) presents an intrinsic advantage over WCPs' schemes since it potentially permits greater per-bit extraction of secure information. This advantage becomes significant for systems with high losses on the quantum transmission channel like envisioned satellite QKD [9]. Single photon quantum cryptography has recently been implemented in two experiments [15, 16] which gave clear evidence for that advantage. Following the work of Beveratos et al [15], we have used a pulsed SPS, based on temporal control of the fluorescence of single color nitrogen vacancy (NV) center in diamond nanocrystal. On the emitted polarized photons, we have then implemented the "BB84" QKD protocol [2]. In our realization, quantum communication between Alice and Bob has been realized in open air during night, between the two wings of the Institut d'Optique's building. The QKD system has been operated with realistic background light, key size in the kbit range and in a configuration where Alice and Bob are two entirely remote parties connected via a

quantum transmission channel in free space and a classical channel using internet link.

In Section 2 we describe the experimental setup used to address single color centers and the QKD protocol based on polarization encoding on the emitted photons. Section 3 deals with the parameters of the QKD experiment. In Section 4, we detail how the quantum key is extracted from raw data using QUCRYPT software [18]. Finally, Section 5 is devoted to the discussion of security models for absolute secrecy. We will show that in a realistic regime corresponding to high losses in the quantum transmission channel, our single photon QKD setup has a measurable advantage over similar systems using WCP.

2. Experimental setup

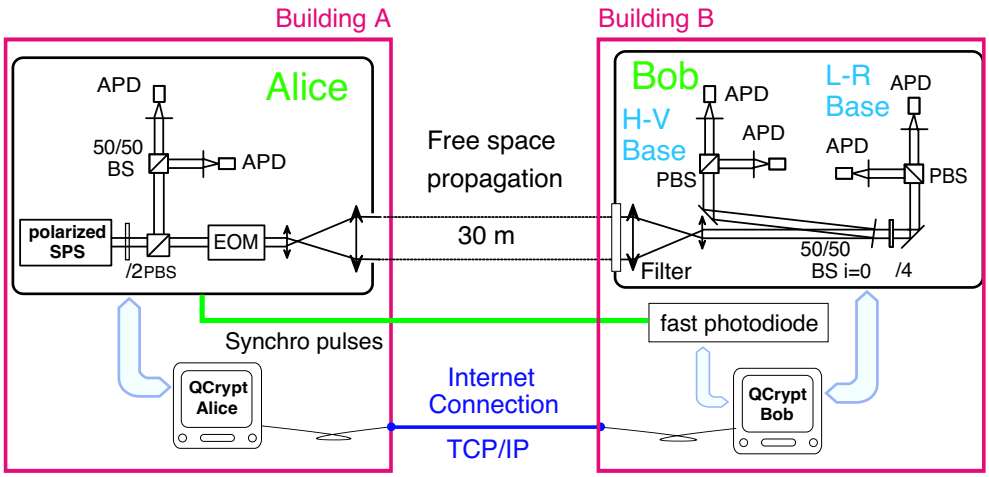

Figure 1. Experimental setup for our quantum key distribution system based on a polarized single photon source. This system corresponds to the implementation of the BB84 protocol. It was operated at night, using a free space quantum channel between Alice and Bob and the Internet as the classical channel. APD: silicon avalanche photodiode. BS: beam splitter. PBS: polarizing beam splitter. EOM: electro optical modulator. $\lambda/2$: achromatic half-wave plate. $\lambda/4$: achromatic quarter-wave plate

2.1. Single photon emission

Lots of effort have been put in the realization of single photon sources over the recent years. Since first proposals [17, 19, 20], a great variety of schemes have been worked out, based upon the control of fluorescence from different kind of emitters, like molecules [21, 22, 23], atoms [32], color center [36] or semiconductor structures [24, 25, 26, 27, 28, 29, 30, 31, 36]. Our single photon source is based upon the pulsed excitation of a single NV color center [33, 34] inside a diamond nanocrystal [35, 36]. This type of emitter, which shares many similarities with the emission from molecules, has important practical advantages since it can be operated at room temperature and is perfectly photostable for both cw and pulsed nanosecond excitation‡.

‡ Note that under femtosecond pulsed excitation, we observed the photoinduced creation of new color centers [37] in nanocrystal containing initially a single NV center. Such behavior under femtosecond laser illumination place some limitations on the use of sub-picosecond pulses to trigger single photon emission.

The nanostructured samples are prepared following a procedure described in Ref.[35], starting from type Ib synthetic powder (de Beers, Netherlands). The diamond nanocrystals are size-selected by centrifugation, yielding a mean diameter of about 90 nm. A polymer solution (polyvinylpyrrolidone, 1 % weight in propanol) containing selected diamond nanocrystals is deposited by spin-coating on a dielectric mirror, resulting in a 30 nm thick polymer layer holding the nanocrystals. The ultra-low fluorescing dielectric SiO_2/Nb_2O_5 mirrors (Layertec, Germany) have been optimized to efficiently reflect the emission spectrum of a NV color center, which is centered on 690 nm (60 nm FWHM). Background fluorescence around the emission of a single NV color center is moreover strongly reduced by photobleaching after a few hours of laser illumination, its emission properties remaining unaffected.

Under pulsed excitation with pulse duration shorter than the excited state lifetime (which for the considered samples of NV color centers is distributed around 25 ns [35]), a single dipole emits single photons one by one [19, 20]. As described in Ref. [36], we use a homebuilt pulsed laser at 532 nm with a 0.8 ns pulse duration to excite single NV color center. The 50 pJ energy per pulse is high enough to ensure efficient pumping of the emitting center in its excited state. Repetition rate was set to 5.3 MHz so that successive fluorescent decays are well separated in time. The green excitation light is focused on the nanocrystals by a high numerical aperture ($NA = 0.95$) metallographic objective. Fluorescence light is collected by the same objective. A long-pass filter (low cutting edge at 645 nm) is used to block reflected 532 nm pump light. The stream of collected photons is then spatially filtered by focusing into a 100 μm diameter pinhole which ensures the setup confocality. Linear polarization of the emitted photons is obtained by passing light through a polarizing cube. Since the fluorescence light emitted by a single color center is partially polarized, an achromatic half-wave plate is introduced in front of the cube. Its rotation allows to send that linearly polarized fraction of the NV fluorescence either towards Bob, or towards two avalanche silicon photodiodes (APDs) arranged in a Hanbury Brown and Twiss configuration. This setup is used to acquire an histogram of the delay between two consecutively detected photons (cf figure 2), from which we infer how far the source departs from an ideal SPS.

2.2. Implementation of the "BB84" QKD protocol

We then implement the "BB84" QKD protocol, by coding the bits on polarization states of the single photons. We use the horizontal-vertical ($H - V$) and circular left-circular right ($L - R$) polarization basis. Each of these polarization states is obtained by applying a given level of high voltage on a KDP electro-optical modulator (EOM, Linos LM0202, Germany). Homemade electronics provides fast driving of the high voltage, being capable of switching the 300 V halfwave voltage of the EOM within 30 ns. In our key distribution, the sequence of encoded polarization bits is generated with hardware electronics, using two programmable electronic linear shift registers in the Fibonacci configuration. Each register gives a pseudo-random sequence of $2^{20} - 1 = 1048575$ bits, and the "BB84" four states are coded with two bits, each of them belonging to one of the two pseudo-random sequences.

As shown on figure 1, quantum key distribution is realized between two parties, Alice and Bob, located in two remote wings of Institut d'Optique building (Orsay, France). Single photons are sent through the windows, from one building to another. To minimize diffraction effects, the beam is enlarged to a diameter of about 2 cm with an afocal setup made of two lenses, before sending it through 30.5 m of open air. Transmitted photons are collected on Bob's side by a similar afocal setup which reduces its diameter back to the original one.

On Bob's side, a combination of four Si-APDs was used to measure the polarization sent by Alice (see figure 1). The $H - V$ or $L - R$ basis is passively selected, as the single photons

are either transmitted or reflected on a 50/50 beam splitter used at almost 0° incidence to avoid any mixing between the four polarization states. In the linear polarization detection basis $H - V$, states H and V are simply discriminated by a polarizing beamsplitter whose outputs are sent onto two APDs. For the circular $L-R$ basis, an achromatic quater-wave plate transforms the incoming circular polarisations into linear ones, which are finally detected with a polarizing beamsplitter and two APDs.

The polarization state associated to each detection event on Bob's APDs is recorded by a high speed digital I/O PCI computer card (National Instrument, PCI-6534). In order to remove non-synchroneous APD dark counts, reading of each detector output is synchronized with the excitation pulses. Since the pumping laser is driven by a stable external clock, this synchronisation is achieved first by sending a small fraction of the excitation laser pulses toward a fast photodiode on Bob's side. The photodiode output is reshaped into a 30 ns TTL-like pulse which is electronically delayed while the output electric pulses from each APD are reshaped to a constant 60 ns duration TTL-like pulse, eliminating any APD pulse width fluctuation. The acquisition card reads its states inputs on the falling edge of the synchronization pulse. Optimal setting of the electronic delay therefore ends up in a time-gated measurement of the APD outputs, within a gate of 60 ns width.

The sequence of time-gated polarization state measurements constitutes Bob's raw key. It can be considered as the output of the "quantum communication phase" which lasts a period of 0.2 s. The remaining steps of the "BB84" QKD protocol are purely classical ones. They consist in taking advantage of the quantum correlations between Alice's information and Bob's raw key in order to distill secrecy between these two parties. All theses steps, detailed in Part 4.2, are realized over the internet using TCP/IP protocol, by the open source QUCRYPT software written by L. Salvail (Aahrus University, Denmark) [18].

3. Parameters of the QKD experiment

The principal goal of our experiment was to bring together a realistic setup in order to test practical feasibility of single-photon open air QKD. Experimental sessions were done from the end of August 2003 to the middle of September 2003. The system was operated at night so as to keep the influence of background light (in our case, moon and public lightning) at a relatively low level. Our room temperature SPS proved its convenience and reliability in these experimental conditions. Note that for consistency reasons, all the data analyzed in the article were obtained from the emission of a given single NV color center, chosen for its strong emission rate. Keeping always this same center allows to consistently investigate the effect of high attenuation on the quantum transmission channel.

3.1. Emission efficiency of the SPS and assessment of its subpoissonian statistics

Preliminary characterization of the SPS quality, performed on Alice's side, consists in measurements of the emission rate and the reduction in probability of multiphotonic emissions, compared with an equivalent WCP of same mean number of photons per pulse.

For a 0.2 s sequence of transmission and a pulsed excitation of 5.3 MHz a total of 8.8×10^4 photons is recorded on Alice's side. By correcting from the APD efficiency $\eta_{\mathrm{APD}} = 0.6$, we can thus infer that the overall emission efficiency of the polarized SPS is of about $\approx 2.8\%$. After polarization encoding in the EOM of transmission $T_{\mathrm{EOM}} = 0.90$ and transmission $T_{\mathrm{optics}} = 0.94$ through the optics of the telescope, the mean number of polarized single photon per pulse sent on the quantum channel is $\mu = 0.0235$.

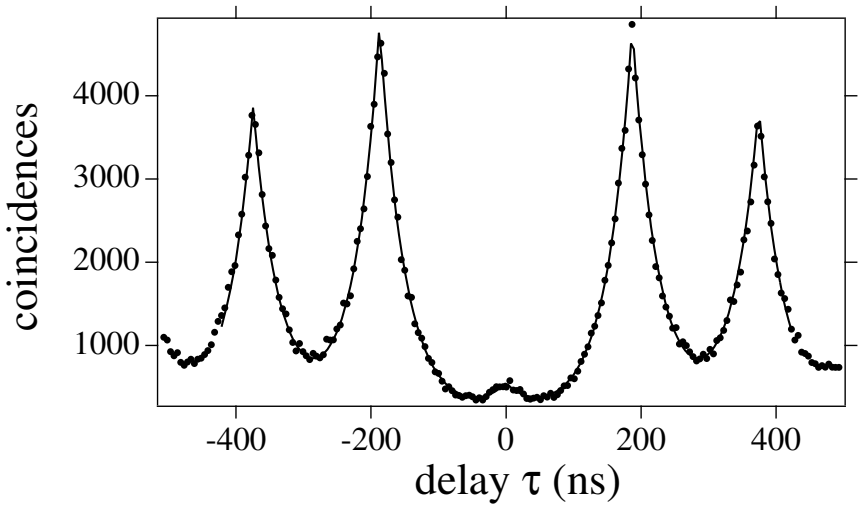

Figure 2. Histogram of time intervals between consecutive photon detection events in Alice's correlation setup. Integration time is 175 s. Lines are exponential fits for each peak, taking into account background level. Radiative lifetime given by the fit is 35 ns and the repetition period is of 188 ns. The strong reduction of coincidences at zero delay gives evidence for single photon emission by the excited color center.

Direct evidence for the reduction of multiphotonic emission probability comes from the acquisition of the delays with the Hanbury Brown and Twiss setup on Alice's side (figure 2). The photon statistics of the SPS can be quantified more precisely from Bob's measurements which give the probability distribution of the number of photocounts within the 60 ns timeslots used for time-gated detection. To perform such evaluation, we have gathered the data corresponding to more than 40×10^6 pulses registered by Bob's acquisition card. For a given detection timeslot probabilities for detecting one and two photons are respectively $P_d(1) = 7.6 \times 10^{-3}$ and $P_d(2) = 2.7 \times 10^{-6}$. From these numbers, we can infer the amount of reduction of multiphotonic emission probability with respect to the photon statistics of an equivalent WCP [20]. Note that one needs to take into account the fact that each avalanche photodiode cannot detect more than one photon per timeslot, due to their detection deadtime. From the configuration of the APDs detection scheme on Bob's side, the probability $P_d(2)$ to detect two photons is only $5/8$ of the probability for Bob to receive two photons, the probability that two photons arrive on the same APD being $3/8$.

Reduction factor $\mathcal{R}$ of the multiphotonic probability is therefore

$$\mathcal{R} = \frac{5}{8} \times \frac{P_d(1)^2/2}{P_d(2)} = 6.7 \; . \tag{1}$$

That result agrees well with the sub-poissonnian reduction factor of 6.1 that can be inferred from the normalized area of figure 2, taking into account the 60 ns integration time and the lifetime of the emitter [36]. For security analysis and numerical simulations, a value of $\mathcal{R} = 6.7$ for the sub-poissonian reduction factor will be taken since it corresponds to a direct outcome of the photocounts record.

As it will be discussed in more details in the section concerning security models, information leakage towards potential eavesdropper is directly linked to $S^{(\mathrm{m})}$ which is the probability per excitation pulse that a multiphotonic pulse leaves on Alice's side. For the

equivalent WCP, that parameter is:

$$S_{\rm WCP}^{(\rm m)} = 1 - (1+\mu)\mathrm{e}^{-\mu} = 2.7 \times 10^{-4} \tag{2}$$

whereas for the SPS, that parameter can be evaluated as

$$S_{\rm SPS}^{(\rm m)} = \frac{1}{6.7}\left[1 - (1+\mu)\mathrm{e}^{-\mu}\right] = 4.1 \times 10^{-5}\ . \tag{3}$$

3.2. Parameters of Bob's detection apparatus

Probabilities for recording a photocount on one of Bob's detectors within a given timeslot is $p_{\rm exp} \simeq 7.6 \times 10^{-3}$. Making the reasonable assumption that absorption in the 30 m open-air transmission beam is negligeable and taking into account the $\mu = 0.0235$ value, one can infer an estimate of the efficiency of Bob's detection apparatus as $\eta_{\rm Bob} \simeq 0.3$

Detector dark counts and fake photocounts due to stray light are responsible on Bob's side for errors in the key exchange process. As it will be discussed in more details below, these errors contribute to the practical limit of secure transmission distance. Particular care was taken to protect Bob's APDs from stray light, using shielding and spectral filtering. Nevertheless, due to the broad emission spectrum of NV color centers, benefit of spectral filtering remains limited and the experiment could not be runned under usual day light conditions. At night, the measured dark count rates on Bob's APDs (in experimental conditions after stopping the SPS beam), (d_H, d_V, d_L, d_R) are (60,70, 350, 150) s^{-1}. Considering the ratio of the 60 ns detection timeslots compared to the 35 ns radiative lifetime of the NV color center, 82% of the SPS photons are falling within the detection gate while only 32% of the dark counts are introduced in the key exchange process. The probability of a dark count record within a given detection timeslot is thus $p_{\rm dark} = 3.8 \times 10^{-5}\ \mathrm{s}^{-1}$.

3.3. Evaluation of quantum bit error rate

Quantum bit error rate (QBER) is computed by comparing Alice and Bob's data corresponding to same polarization basis. The errors are due to two experimental imperfections of the system. First, non ideal polarization encoding and detection can result in optically induced errors, which number is proportional to detected signal level. Second, dark counts of the APDs induce errors within the transmission sequence, which average number is independent of the mean number of photon per pulse.

Following the analysis of Ref. [14] and accounting for the specificities of our detection setup on Bob's side, QBER e is given by

$$e = \alpha \frac{p_{\rm signal}}{p_{\rm exp}} + \frac{p_{\rm dark}}{p_{\rm exp}} \tag{4}$$

where α an adjustable parameter and $p_{\rm signal}$ is the probability to detect a signal photon independently of dark count. $p_{\rm signal}$ is an estimated value, based on a calculation taking into account μ as well as the value of the attenuation on the quantum channel. Measurements of QBER e for different attenuation values of the quantum transmission channel (i.e. variations of $p_{\rm signal}$ and $p_{\rm exp}$) are given in Table 1. Measured values of $e \times p_{\rm exp}$ correlate well with $p_{\rm signal}$ values, accordingly to Eq. (4). Linear fit gives $\alpha = 1.3 \times 10^{-2}$ and $p_{\rm dark} = (35 \pm 6) \times 10^{-6}$, a result compatible with previous direct estimate. These values will be used in all following numerical simulations.

Added attenuation	Average size of raw data (bits)	$p_{\rm exp}$	QBER
1	8000	7.6×10^{-3}	1.65 %
0.498	4250	4.0×10^{-3}	2.2 %
0.25	2100	2.0×10^{-3}	3.2 %
0.128	1025	9.8×10^{-4}	4.15 %
0.057	395	3.8×10^{-4}	9.4 %

Table 1. Measured experimental parameters as a function of the added attenuation on the quantum channel. In order to limit statistical fluctuations, values of the QBER e and of $p_{\rm exp}$ have been computed on samples of at least 3000 bits, obtained by concatenation of several raw data samples.

4. Experimental implementation of "BB84" QKD protocol

4.1. Raw key exchange and sifted data

During a key transmission sequence lasting 0.2 s, Bob detects approximatively a fraction $\eta_{\rm Bob} \times \mu$ of the 1048575 bits initially encoded by Alice. Without any added attenuation on the quantum transmission channel, Bob detects on average 8000 bits, which constitute the initial raw data exchanged through the physical quantum channel. Starting from this shared information, Alice and Bob then extract a key by exchanging classical information for basis reconciliation. Bob reveals the index of the pulses for which a photocount has been recorded and publicly announces to which polarization basis ($H-V$ or $L-R$) it belongs. Events corresponding to more than one photodection on Bob's APDs are discarded since they are ambiguous. Note that one should nevertheless impose an upper bound on the acceptable number for such events, so that discarding them does not introduce a backdoor for any eavesdropper. Considering the low number of multiple photodetection events in our experiment, such filtering does not introduce any practical limitation in the key distillation process. Alice then reveals which bits correspond to identical polarization basis and should be retained. This process ends up in sifted data, which number $N_{\rm sifted} \approx 4000$ is on average half the number of Bob's recorded data.

4.2. Key distillation from sifted data

Sifted data shared by Alice and Bob have imperfect correlations since they are affected by errors. They are moreover not perfectly secure since an eavesdropper may have gained some information on exchanged bits during the quantum transmission sequence.

Starting from those data, complete secrecy is then obtained by error correction followed by privacy amplification [39]. That two-steps procedure, which allows one to distill a secret key for the sifted data, is achieved throughout the IP network using the public domain software QUCRYPT [18].

QUCRYPT uses the algorithm CASCADE for error correction [40]. It implements an iterative dichotomic splitting of Alice and Bob sifted data into blocks and compares their parity in order to spot and correct the errors. This algorithm is optimized to correct all the errors while revealing a minimum number of bits. For a QBER e, the Shannon information

$$f(e) = -\log_2 e - (1-e)\log_2(1-e) \tag{5}$$

gives a lower bound on the amount of information that needs to be exchanged on the public channel to correct one error.

A random subset of 1% of the data used by QUCRYPT is taken to evaluate the QBER e. With such length of tested data the number of secure bits extracted from the sifted data fluctuates by less than 5% from one run of QUCRYPT to another. Moreover, for our data samples of a few thousands of bits, CASCADE corrects errors with a good efficiency. We indeed checked that the information disclosed to correct one error is only 10% greater than the limit imposed by the Shannon bound.

The total amount of information an eavesdropper may have gained on the sifted data is a crucial parameter for the final privacy amplification step. It is the sum of two contributions: the information classically disclosed during error correction added to the information that Eve may have gained during the quantum transmission. This later part has to be evaluated accordingly to security requirement and model.

By setting an upper bound on the QBER in data processing by QUCRYPT we ensure that all our QKD sessions are secure against a first class of attack. We set this bound to 12.5%, which corresponds to the minimum probability for Eve to introduce an error by performing measurements on a single pulse without knowing Bob's measurement basis [41]. However more efficient attacks can be used. We therefore assessed the security of our data in reference to the approach of N. Lütkenhaus, who developed a theoretical framework for the secure experimental QKD implementations of the "BB84" protocol [14]. It has the nice feature of giving a positive security proof for realistic experimental systems under the so-called individual attacks. The calculations are based on the assumption that Eve's optimal strategy is to perform a Photon Number Splitting (PNS) attack on multiphotonic pulses, allowing her to finally get all the information carried on those pulses.

Although such strategy might not always be the optimal one [42], it becomes the most efficient eavesdropping scheme on the "BB84" protocol for strong transmission losses on the quantum channel. Note that alternative protocols to the"BB84" protocol, robust against the PNS attack, have been recently proposed [43] and might constitute an efficient way to increase the span of experimental QKD systems relying on WCPs. Under high attenuation, such schemes allow to work with higher μ (mean number of photons per pulse) since information carried on two-photon pulses is less vulnerable to eavesdropping. It would be interesting to compare the performance of SPSs with respect to WCPs in this case, although such analysis is beyond the scope of the present article.

5. Performance of the QKD setup and resistance to losses

Secure key distribution performance of the QKD system is characterized by the mean amount of secure information exchanged on each sent pulse. Experimental measurements of that parameter have been performed for different level of losses in the quantum channel. The results are compared to numerical simulations based on the analytical derivation of the number of secure bits per pulse G after privacy amplification and error correction evaluated from the analysis of Ref. [14] and given by

$$G = \frac{1}{2}\, p_{\mathrm{exp}} \left\{ \frac{p_{\mathrm{exp}} - S^{(\mathrm{m})}}{p_{\mathrm{exp}}} \left(1 - log \left[1 + 4e \frac{p_{\mathrm{exp}}}{p_{\mathrm{exp}} - S^{(\mathrm{m})}} - 4 \left(e \frac{p_{\mathrm{exp}}}{p_{\mathrm{exp}} - S^{(\mathrm{m})}} \right)^2 \right] \right) + 1.1 \left[\log_2 e + (1-e) \log_2 (1-e) \right] \right\} \quad (6)$$

Theoretical curves giving G versus attenuation on the quantum transmission channel are displayed on figure 3, together with experimental points corresponding either to our SPS

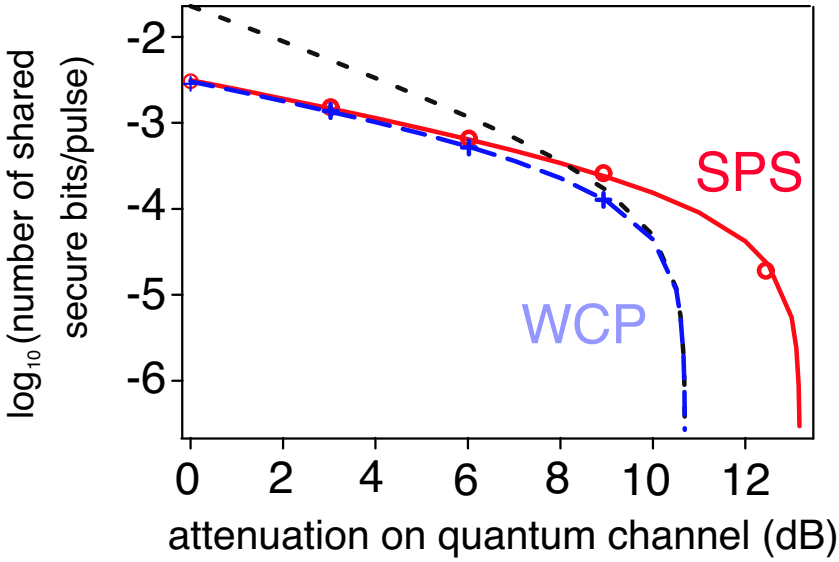

Figure 3. Simulation and experimental data for the number of exchanged secure bits per time slot, versus attenuation in the quantum channel. Solid-line red curve and wide-dashed blue curve correspond respectively to numerical simulations of equation (6) for SPS and WCP, using experimental parameters given in section (3). The narrow-dashed curve is obtained by optimizing G with respect to μ in equation (6). It corresponds to the limit of WCP performance under our experimental conditions and security model.

or to an equivalent WCP. Measured experimental rates correspond to data samples large enough to ensure a statistical accuracy better than 5 %. They are in good agreement with theoretical curves showing that experimental parameters have been correctly assessed and that data samples are large enough for efficient error correction

In the absence of attenuation, an average of 3200 secure bits can be exchanged within the 0.2 s transmission sequence. It corresponds to a 16 kbits/s rate, twice larger than the one of the first experimental realization [15]. As it can be seen on figure 3, reduction of the proportion of multiphotonic pulses gives a significant advantage of our system over WCP, in the strong attenuation regime. Since our setup is affected by relatively high level of dark counts § and since we have adopted a restrictive security model, our system cannot work under attenuation stronger than 13 dB. It however allows us to directly check for the influence of the photon statistics on the experimental QKD system.

A first comparison consists in keeping a constant value of $\mu = 0.0235$ and calculating the effect of either sub-poissonian or poissonian statistics on the size of the final key. This directly relates to the comparison of the "SPS" and "WCP' curves on figure 3. When the system is operated with WCP, one can try to optimize G over μ for different attenuation values. However, even with this strategy (cf figure 3) it clearly appears that our SPS overcomes WCP operated in same experimental conditions, as soon as attenuation reaches 9 dB. In all cases the maximum distance at which secure key distribution can be guaranteed is increased by more than 2 dB.

§ There are several reasons for that. The main one is inherent to the long emission liftetime of our SPS, forcing us to use long (here 60 ns) detection window. There are two other reasons that coud be subject to improvement : we are using a passive determination of the detection basis on Bob side, which increases dark counts by a factor of two, and two of our Si APDs have dark count rate higher than the common value of 70 Hz.

6. Conclusion

In this paper we have demonstrated a free space QKD setup using the "BB84" protocol. The system is based on a stable, simple, and reliable pulsed single photon source (SPS). The open air experimental conditions in which it was operated are reasonably close to those for practical application. They might be extended to kilometric distances using previously established techniques [10]. Advantages of SPS over equivalent weak coherent pulses (WCP) have been experimentally assessed for increasing propagation losses. The results demonstrate quantitatively that QKD with SPS outperforms QKD with WCP, when transmission losses exceed 10 dB.

There clearly remains much room for improvement. For instance, SPS sources using quantum dots [27, 28, 29, 30] are able to emit much shorter pulses with much narrower bandwidths than diamond NV color centers. Those properties are indeeed very favorable for efficient QKD but presently require a cryogenic (liquid He) environment. This constraint makes quantum-dot-based QKD much less suitable for outdoor applications than our SPS. Avenues might be found either by developing semiconductor quantum dots operating at higher temperature (e.g. with II-VI semiconductors), or by finding other color centers with improved performances. New improvement can also be foreseen on the protocol side [43], where both SPS and non-SPS sources deserve to be examined.

Presently, neither color-center- nor quantum-dot-based SPS can operate at the telecom wavelength range around 1550 nm. Their main application given their emission wavelength is free-space QKD, especially QKD from satellite [9]. Compactness and reliability then become major issues. Development of nanofabrication techniques should allow the realization of compact sources based on diamond nanocrystals. In any case, QKD systems have in recent years overcome many difficulties initially considered insurmountable. It is promising that such progress will continue in the near future.

Acknowledgements

We thank Thierry Gacoin for realizing the NV centers samples and Louis Salvail and Martial Tarizzo for help with the QUCRYPT software. This work was supported by the European Commission (IST/FET program), by France Telecom R&D and by the "ACI Jeunes Chercheurs" (Ministère de la Recherche et des Nouvelles Technologies).

[1] Diffie W, and Hellman M E, 1976, New directions in cryptography, *IEEE Trans. Inf. Theory* **IT-22** 644
[2] Bennett C H, and Brassard G, Quantum cryptography: public key distribution and coin tossing, *Int. Conf. on Computers, Systems and Signal processing (Bangalore, India, Dec. 1984)* pp. 175-9
[3] For a recent review, see Gisin N, Robordy G, Tittel W, and Zbinden H, 2002, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145
[4] Bennett C H, Bessette F, Brassard G, Salvail L, and Smolin J, 1992, Experimental quantum cryptography, *J. Cryptology* **5**, 3
[5] Townsend P, 1994, Secure key distribution system based on quantum cryptography, *Electron. Lett.* **30** 809
[6] Ribordy G, Brendel J, Gautier J-D, Gisin N, and Zbinden H, 2001, Long-distance entanglement-based quantum key distribution *Phys. Rev.* A **63**, 012309
[7] Kosaka H, Tomita A, Nambu Y, Kimura T, and Nakamura K, 2003, Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector, *Electron. Lett.* **39**, 1199
[8] Hughes R J, Nordholt J E, Derkacs D, and Peterson C G, 2002, Practical free-space quantum key distribution over 10 km in daylight and at night, *New Journal of Physics* **4**, 43
[9] Rarity J G, Tapster P R, Gorman P M, and Knight P, 2002, Ground to satellite secure key exchange using quantum cryptography, *New Journal of Physics* **4**, 82

[10] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P M, and Rarity J G, 2003, A step towards global key distribution, *Nature* **419**, 450
[11] MAGIQ Technologies (Somerville, USA), `http://www.magiqtech.com/`
[12] IDQUANTIQUE SA (Genève, Switzerland), `http://www.idquantique.com/`
[13] Brassard G, Lütkenhaus N, Mor T, and Sanders B C, 2000, Limitations on practical quantum cryptography, *Phys. Rev. Lett.* **85**, 1330
[14] Lütkenhaus N, 2000, Security against individual attacks for realistic quantum key distribution, *Phys. Rev.* A **61**, 052304
[15] Beveratos A, Brouri R, Gacoin T, Villing ., Poizat J-P, Grangier P, 2002, Single photon quantum cryptography, *Phys. Rev. Lett.* **89** 187901
[16] Waks E, Inoue K, Santori C, Fattal D, Vučković J, Solomon G, and Yamamoto Y, 2002, Secure communication: quantum cryptography with a photon turnstile, *Nature* **420**, 762
[17] Imamoglu A, and Yamamoto Y, 1994, Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions, *Phys. Rev. Lett.* **72**, 210
[18] Nielsen P M, Schori C, Sorensen J L, Salvail L, Damgard I, and Polzik E, 2001, Experimental quantum key distribution with proven security against realistic attacks, *J. Mod. Opt.* **48**, 1921 ; `http://www.cki.au.dk/experiment/qcrypto/doc`
[19] De Martini F, Di Giuseppe G and Marrocco M, 1996, Single-mode generation of quantum photon states by excited single molecules in a microcavity trap, *Phys. Rev. Lett.* **76** 900
[20] Brouri R, Beveratos A, Poizat J-P and Grangier P, 2000, Single-photon generation by pulsed excitation of a single dipole, *Phys. Rev. A* **62** 063814
[21] Brunel C, Lounis B, Tamarat P, and Orrit M, 1999, Triggered source of single photons based on controlled single molecule fluorescence, *Phys. Rev. Lett.* **83** 2722
[22] Lounis B and Moerner W E, 2000, Single photons on demand from a single molecule at room temperature, *Nature* **407** 491
[23] Treussart F, Alléaume R, Le Floc'h V, Xiao L T, Courty J-M and Roch J-F, 2002, Direct measurement of the photon statistics of a triggered single photon source, *Phys. Rev. Lett.* **89** 093601
[24] Michler P, Kiraz A, Becker C, Schoenfeld W V, Petroff P M, Zhang L, Hu E and Imamoğlu A, 2000, A quantum dot single photon turnstile device, *Science* **290** 2282
[25] Santori C, Pelton M, Solomon G, Dale Y and Yamamoto Y, 2001, Triggered single photons from a quantum dot, *Phys. Rev. Lett.* **86** 1502
[26] Moreau E, Robert I, Gérard J-M, Abram I, Manin L and Thierry-Mieg V, 2001, Quantum cascade of photons in semiconductor quantum dots, *Appl. Phys. Lett.* **79** 2865
[27] Santori C, Fattal D, Vučković J, Solomon G and Yamamoto Y, 2002, Indistinguishable photons from a single photon source, *Nature* 419 594
[28] Pelton M, Santori C, Vučković J, Zhang B, Solomon G, Plant J and Yamamoto Y, 2002, Efficient source of single photons: a single quantum dot in a micropost microcavity, *Phys. Rev. Lett.* **89** 233602
[29] Hours J,Varoutsis S, Gallart M, Bloch J, Robert-Philip I, Cavanna A, Abram I, Laruelle F and Gérard J-M, 2003, Single photon emission from individual quantum dots, *Appl. Phys. Lett.* **82** 2206
[30] Vučković J, Fattal D, Santori C, Solomon G and Yamamoto Y, 2003, Enhanced single photon emission from a quantum dot in a micropost microcavity, *Appl. Phys. Lett.* **82** 3596
[31] Yuan Z, Kardynal B E, Stevenson R M, Shields A J, Lobo C J, Cooper K, Beattie N S, Ritchie D A and Pepper M, 2002, Electrically driven single photon source, *Science* **295** 102
[32] Kuhn A, Hennrich M and Rempe G, 2002, Deterministic single-photon for distributing quantum networking, *Phys. Rev. Lett.* **89** 067901
[33] Kurtsiefer C, Mayer S, Zarda P and Weinfurter H, 2000, A robust all-solid-state source for single photons, *Phys. Rev. Lett.* **85** 290
[34] Brouri R, Beveratos A, Poizat J-P and Grangier P, 2000, Single photon emission from colored centers in diamond, *Opt. Lett.* **25** 1294
[35] Beveratos A, Brouri R, Gacoin T, Poizat J-P, and Grangier P, 2001, Nonclassical radiation from diamond nanocrystals, *Phys. Rev.* A **64**, 061802
[36] Beveratos A, Kühn S, Brouri R, Gacoin T, Poizat J P and Grangier P, 2002, Room temperature stable single photon source, *Eur. Phys. J.* D **18** 191
[37] Dumeige Y, Treussart F, Alléaume R, Gacoin T, Roch J-F and Grangier P 2004, Photo-induced creation of nitrogen related color centers in diamond nanocrystals under femtosecond illumination, to appear in *J. of Lumin.*
[38] Alléaume R , Treussart T , Courty J M and Roch J F, 2004, Photon statistics characterization of a single photon source, submitted to *New Journal of Physics*
[39] Bennett, C H, G. Brassard, Crépeau C, and Maurer U M, 1995, Generalized privacy amplification, *IEEE Trans. Information Th.* **41**, 1915-1923
[40] Brassard G and Salvail L, Secret-key reconciliation by public discussion, in Tor Helleseth ed., *Advances in*

Cryptology —EUROCRYPT '93, vol. 765 of Lecture Notes in Computer Science, 410 (Springer Verlag, 1994)
[41] Nielsen P M, Scori C, Sørensen J L, Salvail L, Damgård I, Polzik E 2001 **48**, 1921-1942
[42] Curty M, Lütkenhaus N, 2003, Practical quantum key distribution: on the security evaluation with inefficient single-photon detectors, *Eprint* quant-ph/0311066
[43] Acin A, Gisin N, and Scarani V, Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks *Phys. Rev.* A **69** 012309 (2004)