New Journal of Physics
An Institute of Physics and Deutsche Physikalische Gesellschaft Journal

Experimental open-air quantum key distribution with a single-photon source

R Alléaume[1], F Treussart[1], G Messin[2], Y Dumeige[1], J-F Roch[1], A Beveratos[2], R Brouri-Tualle[2], J-P Poizat[2] and P Grangier[2]

[1] Laboratoire de Photonique Quantique et Moléculaire, UMR 8537 du CNRS, ENS Cachan, 61 avenue du Président Wilson, 94235 Cachan Cedex, France
[2] Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, F-91403 Orsay, France
E-mail: treussar@physique.ens-cachan.fr

New Journal of Physics **6** (2004) 92
Received 13 February 2004
Published 29 July 2004
Online at http://www.njp.org/
doi:10.1088/1367-2630/6/1/092

Abstract. We describe the implementation of a quantum key distribution (QKD) system using a single-photon source, operating at night in open air. The single-photon source at the heart of the functional and reliable set-up relies on the pulsed excitation of a single nitrogen-vacancy colour centre in a diamond nanocrystal. We tested the effect of attenuation on the polarized encoded photons for inferring the 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.

PII: S1367-2630(04)76192-3

Contents

1. Introduction

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

As Bennett and Brassard first proposed 20 years ago [2], quantum physics can be used to build alternative protocols for key distribution (see [3] for a recent review). 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) and 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 a secret and Alice and Bob publicly compare their basis choices. They retain only data for which polarization encoding and measurements were 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. Owing to the constraints on single-photon measurements laid by quantum physics, 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. However, if the error rate remains within acceptable bounds, Alice and Bob can distill a secure secret key, unknown to 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 fibres [6, 7] as well as in free space [8]–[10] and now to commercial products (MAGIQ Technologies, Somerville, MA, USA; IDQUANTIQUE SA, Genève, Switzerland). Nevertheless, several technological and theoretical barriers still have to be overcome to improve the performance of current QKD systems. Most of them rely on weak

coherent pulses (WCPs) 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 [11, 12], security hazard is introduced into the key distribution process. For QKD schemes relying on WCP, one has to throw away finally a part of the initially exchanged information, in proportion to what an eavesdropper could have learnt 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 the transmission rate at long distance becomes vanishingly small or complete security cannot be guaranteed.

The use of a 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 having high losses on the quantum transmission channel such as the envisioned satellite QKD [9]. Single-photon quantum cryptography has recently been implemented in two experiments [13, 14], which gave clear evidence for the advantage of SPS. Following the work of Beveratos *et al* [13], we have used a pulsed SPS, based on temporal control of the fluorescence of a single-colour nitrogen vacancy (NV) centre in a diamond nanocrystal. On the emitted polarized photons, we have then implemented the 'BB84' QKD method [2].

When compared with [13], our realization is closer to a practical QKD set-up. Quantum communication between Alice and Bob was realized in open air at night between the two wings of the Institut d'Optique's building. Thus the QKD set-up was operated with a realistic background light, in a configuration where Alice and Bob were two entirely remote parties communicating via a quantum transmission channel in free space and a classical channel using the internet. So as to bring our QKD experiment closer to practical reality, several technical aspects were also improved. Optimization of the polarization-encoding scheme allowed us to decrease the QBER to 1.7% and to decrease losses on Alice's side. This also led to a higher key exchange rate, which benefited from improvements in the collection efficiency of the emitted single photons. We also significantly increased the number of photons associated with each key exchange session. Error correction algorithms could then be applied with almost optimum efficiency. Finally, in addition to the improvements when compared with the previous experiments of [13], QKD sessions with different quantum channel attenuations were implemented to explore QKD resistance to loss.

In section 2, we describe the experimental set-up used to address single-colour centres and the QKD method 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 [15]. Finally, in section 5, we discuss 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 set-up has a measurable advantage over similar systems using WCP.

2. Experimental set-up

2.1. Single-photon emission

Much effort have been put in the realization of SPSs over the recent years. Since first proposals [16]–[18], a wide variety of schemes have been worked out, based on the control of fluorescence

from different kinds of emitters, such as molecules [19]–[22], atoms [23], colour centres [24] and semiconductor structures [25]–[32]. Our SPS is based on the pulsed excitation of a single NV colour centre [33, 34] inside a diamond nanocrystal [24, 35]. 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 ns excitations.[3]

The nanostructured samples were prepared by a procedure described in [35], by starting with type Ib synthetic powder (de Beers, Netherlands). The diamond nanocrystals were size-selected by centrifugation, yielding a mean diameter of about 90 nm. A polymer solution (polyvinylpyrrolidone, 1 wt.% in propanol), containing selected diamond nanocrystals, was 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) were optimized to reflect efficiently the emission spectrum of an NV colour centre, which is centred on 690 nm (60 nm FWHM). Background fluorescence around the emission of a single NV colour centre was also strongly reduced by photobleaching after a few hours of laser illumination, while NV colour centre emission properties remained unaffected.

Under pulsed excitation with a pulse duration shorter than the excited-state lifetime (which, for the considered samples of NV colour centres, is distributed around 25 ns [35]), a single dipole emits single photons one by one [17, 18]. As described in [24], we used a home-built pulsed laser at 532 nm with a 0.8 ns pulse duration to excite a single NV colour centre. The 50 pJ energy per pulse is high enough to ensure efficient pumping of the emitting centre in its excited state. The repetition rate was set at 5.3 MHz so that successive fluorescent decays are well separated in time. The green excitation light was focused on the nanocrystals by a high-numerical aperture ($NA = 0.95$) metallographic objective. Fluorescent light is collected by the same objective. A long-pass filter (low cutting edge at 645 nm) was used to block the reflected 532 nm pump light. The stream of collected photons was then spatially filtered by focusing into a 100 μm diameter pinhole to ensure the confocality of the set-up. Linear polarization of the emitted photons was obtained by passing light through a polarizing cube. Since the fluorescence light emitted by a single colour centre is partially polarized, an achromatic half-wave plate was introduced in front of the cube. Its rotation allowed us 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 set-up was used to obtain a histogram of the delay between two consecutively detected photons (see figure 2), from which we inferred how far the source departs from an ideal SPS.

2.2. *Implementation of the 'BB84' QKD protocol*

We then implemented the 'BB84' QKD method, by coding the bits on polarization states of single photons. We used the horizontal–vertical (H–V) and circular left–circular right (L–R) polarization bases. Each of these polarization states was obtained by applying a given level of high voltage on a KDP electro-optical modulator (EOM; Linos LM0202, Germany). Home-built electronics provides fast driving of the high voltage, being capable of switching the 300 V

[3] Note that under femtosecond pulsed excitation, we observed the photo-induced creation of new colour centres [36] in a nanocrystal containing, initially, a single NV centre. Such behaviour under femtosecond laser illumination places some limitations on the use of sub-picosecond pulses to trigger single-photon emission.

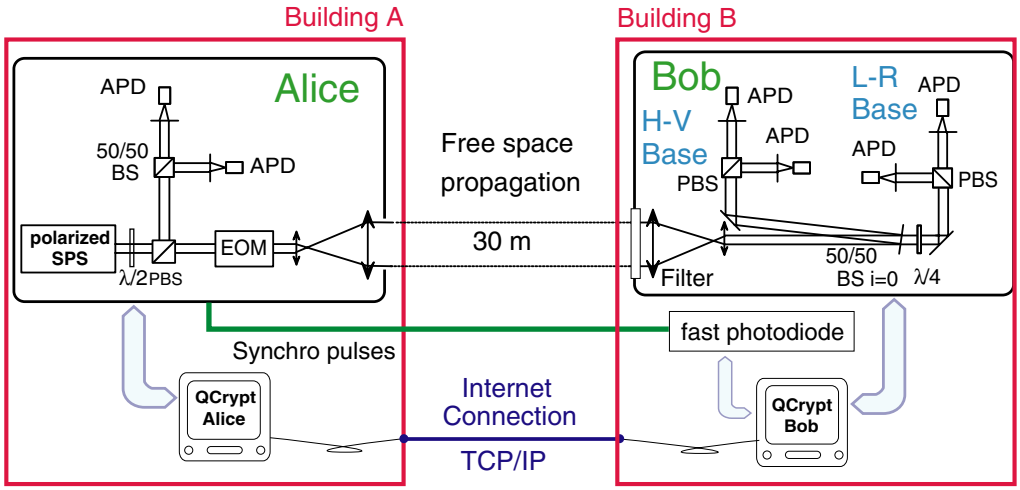

Figure 1. Experimental set-up for our quantum key distribution system based on a polarized SPS. This system corresponds to the implementation of the BB84 protocol. It was operated at night using a free space quantum channel between Alice and Bob and the internet as the classical channel. APD, silicon 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.

halfwave voltage of the EOM within 30 ns. In our key distribution, the sequence of encoded polarization bits was generated with hardware electronics, using two programmable electronic linear shift registers in the Fibonacci configuration. Each register gave a pseudo-random sequence of $2^{20} - 1 = 1\,048\,575$ bits, and the four 'BB84' states were coded with two bits, each of them belonging to one of the two pseudo-random sequences.

As shown in figure 1, quantum key distribution was realized between two parties, Alice and Bob, located in two remote wings of the Institut d'Optique's building (Orsay, France). Single photons were sent through the windows from one building to the other. To minimize diffraction effects, the beam was enlarged to a diameter of about 2 cm using an afocal set-up made of two lenses, before sending it through 30.5 m of open air. The transmitted photons were collected on Bob's side by a similar afocal set-up that reduced 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 was passively selected, as the single photons were 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, the states H and V were simply discriminated by a polarizing beam splitter whose outputs were sent on to two APDs. For the circular L–R basis, an achromatic quarter-wave plate transformed the incoming circular polarizations into linear ones, which were finally detected with a polarizing beam splitter and two APDs.

The polarization state associated with each detection event on Bob's APDs was recorded by a high-speed digital I/O PCI computer card (National Instrument, PCI-6534). To remove non-synchronous APD dark counts, the reading of each detector output was synchronized with the excitation pulses. Since the pumping laser was driven by a stable external clock, this synchronization was achieved first by sending a small fraction of the excitation laser pulses

towards a fast photodiode on Bob's side. The photodiode output was reshaped into a 30 ns TTL-like pulse, which is electronically delayed, while the output electric pulses from each APD were reshaped to a constant 60 ns duration TTL-like pulse, eliminating any APD pulse width fluctuation. The acquisition card reads its state 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 for a period of 0.2 s. The remaining steps of the 'BB84' QKD method were 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 these steps, detailed in section 4.2, were realized with the internet using TCP/IP method and the open source QUCRYPT software written by L Salvail (Aahrus University, Denmark) [15].

3. Parameters of the QKD experiment

The principal goal of our experiment was to bring together a realistic set-up to test the feasibility of single-photon open-air QKD. Experiments were carried out from the end of August 2003 to the middle of September 2003. The system was operated at night to keep the influence of background light (in our case, moon and public lighting) 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 analysed in the present paper were obtained from the emission of a given single NV colour centre chosen for its strong emission rate. Keeping always this same centre allowed us to investigate consistently the effect of high attenuation on the quantum transmission channel.

3.1. Emission efficiency of the SPS and assessment of its sub-Poissonian statistics

Preliminary characterization of the SPS quality, performed on Alice's side, consists in measurement of the emission rate and reduction in probability of multiphotonic emissions, compared with an equivalent WCP having the 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 infer that the overall emission efficiency of the polarized SPS is 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 afocal setup, the mean number of polarized single photons per pulse sent on the quantum channel was $\mu = 0.0235$.

Direct evidence for the reduction in multiphotonic emission probability comes from acquisition of the delays with the Hanbury Brown and Twiss set-up 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 $P_{\mathrm{d}}(1) = 7.6 \times 10^{-3}$ and $P_{\mathrm{d}}(2) = 2.7 \times 10^{-6}$. From these numbers, we can infer the amount of reduction of multiphotonic emission probability with respect to the photon statistics of an equivalent WCP [18]. Note that

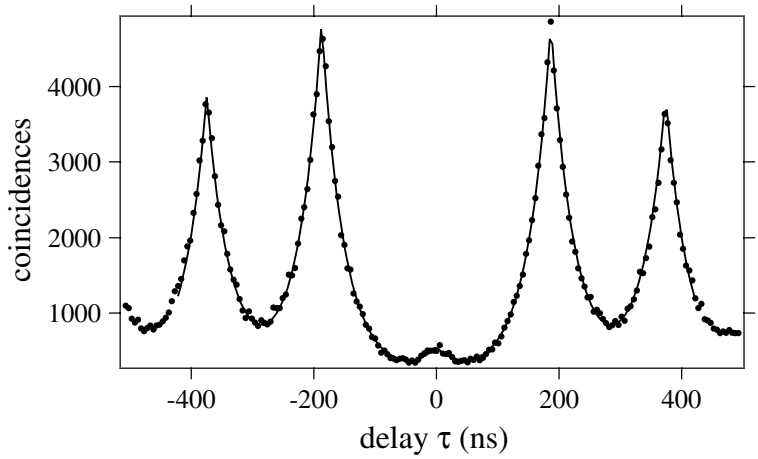

Figure 2. Histogram of time intervals between consecutive photon detection events in Alice's correlation set-up. Integration time is 175 s. Lines are exponential fits for each peak, taking into account the background level. Radiative lifetime given by the fit is 35 ns and the repetition period was 188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

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 $P_{\mathrm{d}}(2)$ to detect two photons is only 5/8 of the probability for Bob to receive two photons, and the probability that two photons arrive on the same APD is 3/8.

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

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

This result agrees well with the sub-Poissonian 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 [24]. 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 detail 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

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

whereas for the SPS, that parameter can be evaluated as

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

3.2. Parameters of Bob's detection apparatus

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

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 detail 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 colour centres, benefit of spectral filtering was limited and the experiment could not be run under usual day light conditions. At night, the measured dark count rates on Bob's APDs (under experimental conditions after stopping the SPS beam), d_{H}, d_{V}, d_{L} and d_{R}, were 60, 70, 350 and 150 s^{-1}. Considering the ratio of the 60 ns detection timeslots compared with the 35 ns radiative lifetime of the NV colour centre, 82% of the SPS photons fall within the detection gate, whereas only 32% of the dark counts are introduced into the key exchange process. Thus the probability of a dark count record within a given detection timeslot is $p_{\mathrm{dark}} = 3.8 \times 10^{-5}\ \mathrm{s}^{-1}$.

3.3. Evaluation of quantum bit error rate (QBER)

QBER is computed by comparing Alice and Bob's data corresponding to the same polarization basis. Errors are due to two experimental imperfections of the system. First, non-ideal polarization encoding and detection can result in optically induced errors, which is proportional, by a factor α, to the rate of photodetection events $\mu\eta_{\mathrm{t}}\,\eta_{\mathrm{Bob}}$, where η_{t} stands for the transmission of the quantum channel. Secondly, dark counts of the APDs induce errors within the transmission sequence, the average of which is independent of the mean number of photons/pulse.

Following the analysis given in [12] and accounting for the specificities of our detection set-up on Bob's side, QBER e is given by

$$e = \alpha \frac{\mu\eta_{\mathrm{t}}\,\eta_{\mathrm{Bob}}}{p_{\mathrm{exp}}} + \frac{p_{\mathrm{dark}}}{p_{\mathrm{exp}}}. \tag{4}$$

Measurements of QBER e for different quantum channel transmission values are given in table 1. The measured values of $e \times p_{\mathrm{exp}}$ correlate well with η_{t} values in accordance with equation (4). A linear fit gives $\alpha = (13 \pm 2) \times 10^{-3}$ and $p_{\mathrm{dark}} = (35 \pm 6) \times 10^{-6}$, a result compatible with a previous direct estimate. These values will be used in our subsequent numerical simulations.

4. Experimental implementation of the 'BB84' QKD method

4.1. Raw key exchange and sifted data

During a key transmission sequence lasting 0.2 s, Bob detects only a fraction $\eta_{\mathrm{Bob}}\mu$ of the 1 048 575 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

Table 1. Measured experimental parameters as a function of quantum channel transmission η_t. To limit statistical fluctuations, values of the QBER e and p_{exp} have been computed on samples of at least 3000 bits, obtained by concatenation of several raw data samples.

η_t	Average size of raw data (bits)	p_{exp}	QBER (%)
1	8000	7.6×10^{-3}	1.7
0.50	4250	4.0×10^{-3}	2.2
0.25	2100	2.0×10^{-3}	3.2
0.13	1025	9.8×10^{-4}	4.2
0.057	395	3.8×10^{-4}	9.4

exchanged through the physical quantum channel. Starting with 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 photodetection 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 bases and should be retained. This process ends up in sifted data; the size of sifted data $N_{sifted} \approx 4000$ bits is, on average, half of the size of Bob's recorded data.

4.2. Key distillation from sifted data

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

Starting with those data, complete secrecy is then obtained by error correction followed by privacy amplification [37]. This two-step 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 [15].

QUCRYPT uses the algorithm CASCADE for error correction [38]. It implements an iterative dichotomic splitting of Alice and Bob sifted data into blocks and compares their parity 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 a 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 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. The latter part has to be evaluated according to the 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 [15].

More efficient and subtle attacks can be used. We therefore assessed the security of our data by the approach of N Lütkenhaus, who developed a theoretical framework for the secure experimental QKD implementations of the 'BB84' method [12]. In that model, all the errors including the ones due to photodiode dark counts, are interpreted as a possible source of information leakage towards an eavesdropper. Even though this security assumption is very strong, it has the nice feature of allowing us to establish a positive security proof for realistic experimental systems under an entire class of attacks, the so-called 'individual attacks'. The proof is based on the fact that Eve's optimal strategy is to perform a photon number splitting (PNS) attack on multiphotonic pulses, allowing her to finally extract all the information carried by those pulses. Under such working assumptions, numerical values for the QBER and for the source statistics allow one to calculate a bound on Eve's information and, thus, to assess the amount of secure key that can be shared by Alice and Bob.

Less drastic security assumptions (considering for example that Eve acquires no information on the key from dark counts) allow a wider range of parameters to be spanned for secure QKD. However, security analysis becomes in that case more complex, since the PNS attack strategy might not always be optimal [39]. We thus adopted the working assumptions of Lütkenhaus [12] for the practical estimate of QKD security.

Note also that alternative methods, more robust against the PNS attack than the 'BB84' method, have been proposed recently [40]. They might constitute an efficient way to increase the span of experimental QKD systems relying on WCPs. Under high attenuation of the quantum transmission channel, such schemes allow us to work with a higher mean number of photons per pulse μ, since information carried on two-photon pulses appears to be less vulnerable to eavesdropping. It would be interesting to compare the performance of SPSs with respect to WCPs for these alternative methods. Such an analysis is, however, beyond the scope of the present paper.

5. Performance of the QKD set-up 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 levels of losses in the quantum channel. The results were compared with numerical simulations based on the analytical derivation of the number of secure bits/pulse, G, after privacy amplification and error correction evaluated from the analysis

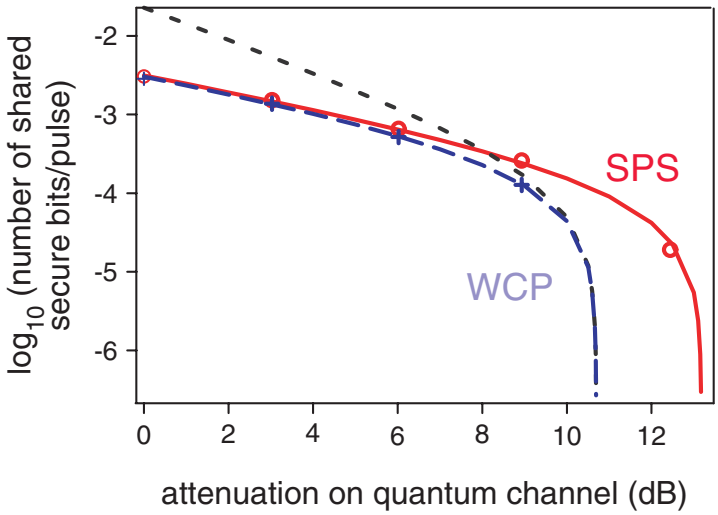

Figure 3. Simulation and experimental data for the number of exchanged secure bits per time slot versus attenuation in the quantum channel. Solid (red) and long-dashed (blue) lines correspond, respectively, to numerical simulations of equation (6) for SPS and WCP, using experimental parameters given in section 3. The short-dashed line 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.

in [12] and given by

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

Theoretical curves giving G versus attenuation on the quantum transmission channel are displayed in figure 3, together with experimental points. Measured experimental rates correspond to data samples large enough to ensure a statistical accuracy higher 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 a 0.2 s transmission sequence. It corresponds to a rate of 16 kbits s^{-1} rate, double that of the first experimental realization [13]. As seen in figure 3, reduction in the proportion of multiphotonic pulses compared with WCP gives a significant advantage to our system, in the strong attenuation regime. Since our set-up is affected by the relatively high level of dark counts[4] and since we have adopted a restrictive security model, our system cannot work under attenuation stronger

[4] There are several reasons for that. The main one is inherent to the long emission lifetime of our SPS, forcing us to use a 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's 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.

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 in 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 is clearly seen that our SPS overcomes WCP operated under the same experimental conditions, as soon as attenuation reaches 9 dB. In all cases, the maximum distance at which a secure key distribution can be guaranteed is increased by more than 2 dB.

Our SPS was compared with WCPs for the same photodetector dark count probability p_{dark}. It allowed us to evaluate directly the gain in performance due to reduction in the multiphotonic probability $S^{(\mathrm{m})}$. Such a comparison may seem unfair for WCP since the level of dark counts can be decreased by tighter temporal filtering. However, a long emission lifetime is not an intrinsic limitation of SPS-based QKD. Alternative systems like quantum dots exhibit sub-ns emission lifetimes [14]. However, they require operation at cryogenic temperatures. Concerning the properties of colour centres in diamond, we carefully investigated the distribution of their fluorescence lifetimes. We found a non-negligible fraction of single NV centres in diamond nanocrystals having lifetimes of about 10 ns, which is significantly shorter than the one presented in this paper. Use of other colour centres, such as the one recently reported in [41], is also a promising method to realize an SPS well suited for QKD.

6. Conclusion

In the present paper, we have demonstrated a free-space QKD set-up by the 'BB84' method. The system is based on a stable, simple and reliable pulsed SPS. The open-air experimental conditions under which it was operated are reasonably close to those for practical application. They might be extended to km distances using previously established techniques [10]. Advantages of SPS over equivalent WCPs have been assessed experimentally for increasing propagation losses. The results demonstrate quantitatively that QKD with SPS can have measurable advantages over QKD with WCP when transmission losses exceed 10 dB.

There clearly remains much room for improvement. For instance, SPS sources using quantum dots [28]–[31] are able to emit much shorter pulses with much narrower bandwidths compared with diamond NV colour centres. These properties are indeed very favourable for efficient QKD but currently require a cryogenic (liquid He) environment. This constraint makes quantum-dot-based QKD much less suitable for outdoor applications when compared with our SPS. This limitation can be overcome either by developing semiconductor quantum dots operating at higher temperature (e.g. with II–VI semiconductors) or by finding other colour centres with improved performances. Other improvements can also be foreseen on the protocol side [40], where both SPS and non-SPS sources deserve to be examined.

At present, neither colour-centre- nor quantum-dot-based SPS can operate at the telecom wavelength range of approx. 1550 nm. Given their emission wavelength, their main application is free-space QKD, especially QKD from a 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 of the difficulties initially considered insurmountable. It is expected that the progress will continue in the near future.

Acknowledgments

We thank T Gacoin for realizing the NV-centre samples and L Salvail and M Tarizzo for assistance with the QUCRYPT software. We thank Mathieu Ferreira, Frédéric Moron and André Villing for their crucial contributions in improving the electronics and data acquisition setup. We also thank Robin Smith for studying the dispersion of NV centre emission lifetimes. This work was supported by the European Commission (IST/FET programme), by France Telecom R&D and by the 'ACI Jeunes Chercheurs' (Ministère de la Recherche et des Nouvelles Technologies).

References

[1] Diffie W and Hellman M E 1976 *IEEE Trans. Inform. Theory* **IT-22** 644
[2] Bennett C H and Brassard G 1984 *Proc. Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* p 175
[3] Gisin N, Robordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[5] Townsend P 1994 *Electron. Lett.* **30** 809
[6] Ribordy G, Brendel J, Gautier J-D, Gisin N and Zbinden H 2001 *Phys. Rev.* A **63** 012309
[7] Kosaka H, Tomita A, Nambu Y, Kimura T and Nakamura K 2003 *Electron. Lett.* **39** 1199
[8] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 *New J. Phys.* **4** 43
[9] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 *New J. Phys.* **4** 82
[10] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P M and Rarity J G 2003 *Nature* **419** 450
[11] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[12] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[13] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J-P and Grangier P 2002 *Phys. Rev. Lett.* **89** 187901
[14] Waks E, Inoue K, Santori C, Fattal D, Vučković J, Solomon G and Yamamoto Y 2002 *Nature* **420** 762
[15] Nielsen P M, Schori C, Sorensen J L, Salvail L, Damgard I and Polzik E 2001 *J. Mod. Opt.* **48** 192; online at http://www.cki.au.dk/experiment/qcrypto/doc
[16] Imamoglu A and Yamamoto Y 1994 *Phys. Rev. Lett.* **72** 210
[17] De Martini F, Di Giuseppe G and Marrocco M 1996 *Phys. Rev. Lett.* **76** 900
[18] Brouri R, Beveratos A, Poizat J-P and Grangier P 2000 *Phys. Rev.* A **62** 063814
[19] Brunel C, Lounis B, Tamarat P and Orrit M 1999 *Phys. Rev. Lett.* **83** 2722
[20] Lounis B and Moerner W E 2000 *Nature* **407** 491
[21] Treussart F, Alléaume R, Le Floc'h V, Xiao L T, Courty J-M and Roch J-F 2002 *Phys. Rev. Lett.* **89** 093601
[22] Alléaume R, Treussart F, Courty J M and Roch J F 2004 *New J. Phys.* **6** in press
[23] Kuhn A, Hennrich M and Rempe G 2002 *Phys. Rev. Lett.* **89** 067901
[24] Beveratos A, Kühn S, Brouri R, Gacoin T, Poizat J P and Grangier P 2002 *Eur. Phys. J.* D **18** 191
[25] Michler P, Kiraz A, Becker C, Schoenfeld W V, Petroff P M, Zhang L, Hu E and Imamoğlu A 2000 *Science* **290** 2282
[26] Santori C, Pelton M, Solomon G, Dale Y and Yamamoto Y 2001 *Phys. Rev. Lett.* **86** 1502
[27] Moreau E, Robert I, Gérard J-M, Abram I, Manin L and Thierry-Mieg V 2001 *Appl. Phys. Lett.* **79** 2865
[28] Santori C, Fattal D, Vučković J, Solomon G and Yamamoto Y 2002 *Nature* **419** 594
[29] Pelton M, Santori C, Vučković J, Zhang B, Solomon G, Plant J and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 233602
[30] Hours J, Varoutsis S, Gallart M, Bloch J, Robert-Philip I, Cavanna A, Abram I, Laruelle F and Gérard J-M 2003 *Appl. Phys. Lett.* **82** 2206
[31] Vučković J, Fattal D, Santori C, Solomon G and Yamamoto Y 2003 *Appl. Phys. Lett.* **82** 3596

[32] 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 *Science* **295** 102
[33] Kurtsiefer C, Mayer S, Zarda P and Weinfurter H 2000 *Phys. Rev. Lett.* **85** 290
[34] Brouri R, Beveratos A, Poizat J-P and Grangier P 2000 *Opt. Lett.* **25** 1294
[35] Beveratos A, Brouri R, Gacoin T, Poizat J-P and Grangier P 2001 *Phys. Rev.* A **64** 061802
[36] Dumeige Y, Treussart F, Alléaume R, Gacoin T, Roch J-F and Grangier P 2004 *J. Lumin.* in press
[37] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Inform. Theory* **41** 1915
[38] Brassard G and Salvail L 1994 *Advances in Cryptology—EUROCRYPT '93* ed T Helleseth (*Lecture Notes in Computer Science* vol 765) (Berlin: Springer) p 410
[39] Curty M and Lütkenhaus N 2003 *Preprint* quant-ph/0311066
[40] Acin A, Gisin N and Scarani V 2004 *Phys. Rev.* A **69** 012309
[41] Gaebel T, Popa I, Gruber A, Domhan M, Jelezko F and Wrachtrup J 2004 *Preprint* quant-ph/0402213