Single Photon Quantum Cryptography

Alexios Beveratos,* Rosa Brouri, Thierry Gacoin,† André Villing, Jean-Philippe Poizat, and Philippe Grangier

Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, F-91403 Orsay, France

(Received 6 June 2002; published 10 October 2002)

We report the full implementation of a quantum cryptography protocol using a stream of single photon pulses generated by a stable and efficient source operating at room temperature. The single photon pulses are emitted on demand by a single nitrogen-vacancy color center in a diamond nanocrystal. The quantum bit error rate is less that 4.6% and the secure bit rate is 7700 bits/s. The overall performances of our system reaches a domain where single photons have a measurable advantage over an equivalent system based on attenuated light pulses.

DOI: 10.1103/PhysRevLett.89.187901 PACS numbers: 03.67.Dd, 42.50.Dv

Since its initial proposal in 1984 [1] and first experimental demonstration in 1992 [2], quantum key distribution (QKD) has reached maturity through many experimental realizations [3], and it is now commercially available [4]. However, most of the practical realizations of QKD rely on weak coherent pulses (WCP) which are only an approximation of single photon pulses (SPP) that would be desirable in principle. The presence of pulses containing two photons or more in WCPs is an open door to information leakage towards an eavesdropper. In order to remain secure, the WCP schemes require one to attenuate more and more the initial pulse, as the line losses become higher and higher, resulting in either a vanishingly low transmission rate or a loss of security [5,6]. The use of an efficient source of true single photons would therefore considerably improve the performances of existing or future QKD schemes, especially as far as high-loss schemes such as satellite QKD [7] are considered.

In this Letter we present the first complete realization of a quantum cryptographic key distribution based on a pulsed source of true single photons. Our very reliable source of a single photon has been used to send a key over a distance of 50 m in free space at a rate of 7700 secret bits per second including error correction and privacy amplification. Using the published criteria that warrant absolute secrecy of the key against any type of individual attacks [5,6], we will show that our setup reaches the region where a single photon QKD scheme takes a quantitative advantage over a similar system using WCP.

Single photon sources have been extensively studied in recent years and a great variety of approaches has been proposed and implemented [8–13]. Our single photon source is based on the fluorescence of a single nitrogen-vacancy (NV) color center [14] inside a diamond nanocrystal [15,16] at room temperature. This molecularlike system has a lifetime of 23 ns when it is contained in a 40 nm nanocrystal [15]. Its zero-phonon line lies at 637 nm and its room temperature fluorescence spectrum ranges from 637 to 750 nm [17]. This center is intrinsically photostable: no photobleaching has been observed over a week of continuous saturating irradiation of the same center. The nanocrystals are held by a 30 nm thick layer of polymer that has been spin coated on a dielectric mirror [15]. The mirror is initially slightly fluorescing, but this background light is reduced to a negligible value by hours of full power excitation that leads to a complete photobleaching of the dielectric coating, the NV center being unaffected.

The experimental setup is shown in Fig. 1. Alice's station consists of a pulsed single photon source, a photon correlation detection to control the quality of the SPP, and a 4-state polarization encoding scheme. The single photon source is pumped by a homebuilt pulsed laser at a wavelength of 532 nm that delivers 800 ps long pulses of energy 50 pJ with a repetition rate of 5.3 MHz, synchronized on a stable external clock [16]. The green excitation light is focused by a metallographic objective of high numerical aperture ($NA = 0.95$) onto the nanocrystals. The partially polarized fluorescence light (polarization rate of 46%) is collected by the same objective. It is then polarized horizontally by passing through a polymer achromatic half-wave plate and a polarizing cube, spectrally filtered by a long-pass filter (low cutoff 645 nm) that eliminates the reflected laser light and spatially filtered by a confocal setup. In order to control the quality of the SPP, the light can be sent via a movable mirror onto a photon correlation detection scheme consisting of two avalanche photodiodes (APD) in a Hanbury-Brown and Twiss setup.

The total number of polarized photons detected by the two APDs altogether is $N_D^{(a)} = 7 \times 10^4\ \mathrm{s}^{-1}$ for an

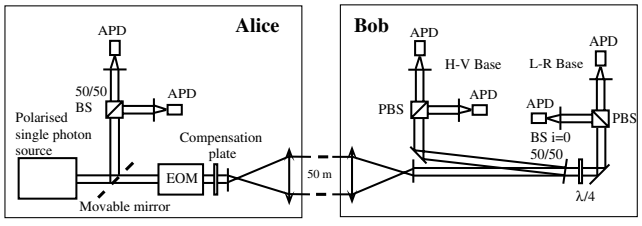

FIG. 1. Experimental setup.

 0031-9007/02/89(18)/187901(4)$20.00

excitation repetition rate of 5.3 MHz. Correcting for the quantum efficiency of the control APDs ($\eta = 0.6$), the number of emitted polarized photons per pulse (before data encoding) is thus 2.2%. The autocorrelation function of the emitted light at saturation, displayed in Fig. 2, shows that the number of photon pairs within a pulse is strongly reduced with respect to Poisson statistics. The normalized area of the central peak is $C(0) = 0.07$, where this area would be unity for WCPs [16]. This means that the number of two-photon pulses of our source is reduced by a factor of $1/C(0) = 14$ compared to a WCP.

The Bennett-Brassard protocol [1] (BB84) is implemented by using the horizontal-vertical (H-V) and circular left-circular right (L-R) basis. These four polarization states are obtained by applying four levels of high voltage on an electro-optical modulator (EOM). The EOM is driven by a homemade module that can switch 500 V in 30 ns to ensure the 5.3 MHz repetition rate of a single photon source. The driving module is fed by sequences of pseudorandom numbers that are produced using a linear feedback shift register in the Fibonacci configuration. In order to minimize polarization errors due to the broad bandwidth of the emitted photons, the EOM is operating very close to the exact zero-path difference (white light fringe). This is obtained by inserting a suitable birefringent plate to compensate for the residual birefringence of the EOM. The source emission rate of 2.2% is reduced down to 1.4% by the transmission of the EOM, measured to be $T_{\mathrm{EOM}} = 0.65$. The corresponding rate of encoded single photons emitted by the Alice station is

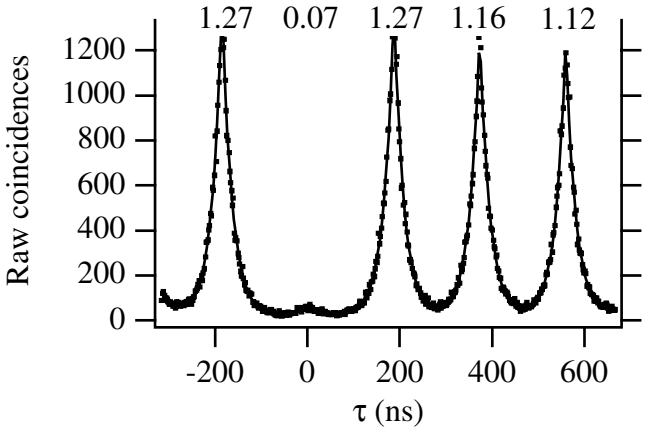

FIG. 2. Autocorrelation function of a single NV center on Alice's side. The raw coincidences are given as a function of the delay between the arrival times of the photons at Alice's correlation detection setup. The exciting laser has a repetition period of 187.5 ns, a pulse width of 0.8 ns, and an average power of 0.2 mW. The count rates are about $3.5 \times 10^4\ \mathrm{s}^{-1}$ on each avalanche photodiode, and the integration time is 166 s. The number above each peak represents its normalized area. The dots are experimental data. The line is an exponential fit for each peak and takes into account the background light.

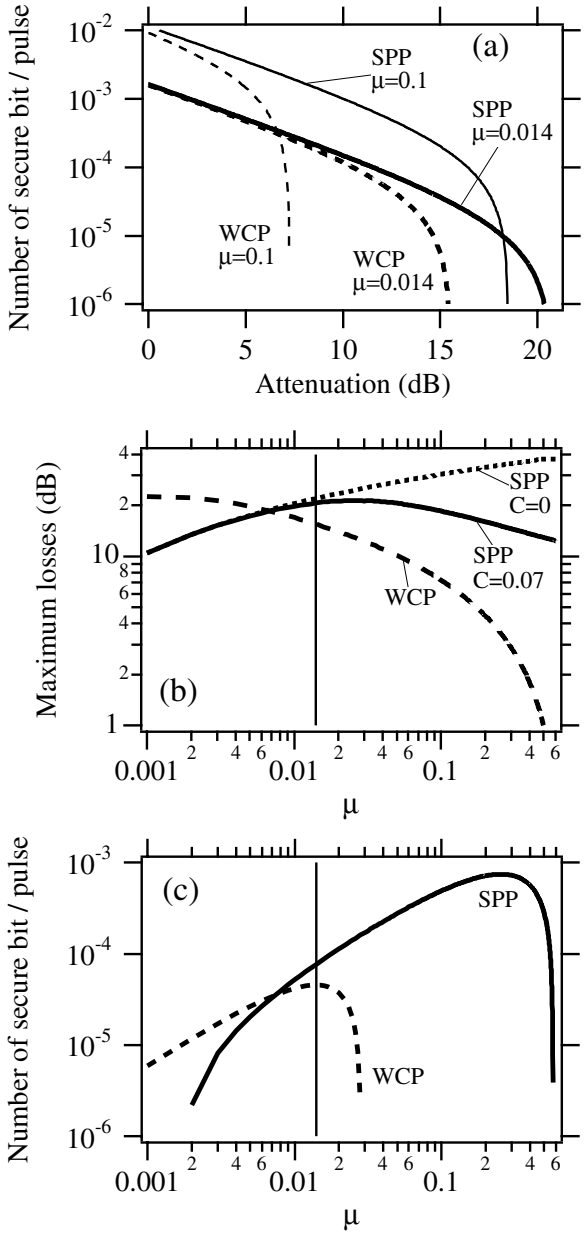

FIG. 3. These plots give theoretical evaluations obtained by using Eq. (1), together with the experimental parameters for our single photon source. (a) Calculated number of secure bit per time detection time gate G as a function of the on-line losses for SPPs and WCPs, for a different average photon number per pulse μ. The SPP traces correspond to our value of the zero time autocorrelation of $C = 0.07$. (b) The maximum allowed on-line losses for secure communication are deduced from (a) and correspond to the attenuation for which $G = 10^{-6}$. This value is plotted as a function of the mean photon number per pulse μ, for a WCP system, for a SPP system with our value of the zero time autocorrelation ($C = 0.07$), and for an ideal SPP system with $C = 0$. The vertical line corresponds to our source, i.e., $\mu = 0.014$. (c) Number of secure bit per detection time gate G as a function of the mean photon number per pulse μ for on-line losses of 12.5 dB. The SPP trace assumes that $C = 0.07$, and the vertical line corresponds to $\mu = 0.014$.

$N^{(a)} = N_D^{(a)} T_{\mathrm{EOM}}/\eta \approx 7.5 \times 10^4\ \mathrm{s}^{-1}$, and the average photon number per pulse is thus $\mu = 0.014$.

The detection at Bob's site lies 50 m away from Alice down a corridor. The single photons are sent via a 2 cm diameter beam so that diffraction effects are negligible. The *H-V* or *L-R* basis is passively selected by a near 0° incidence 50/50 beam splitter that is polarization insensitive. A polymer achromatic quarter-wave plate is inserted in the *L-R* basis arm. In each basis a polarizing beam splitter sends the two polarizations on two APDs. The time arrival of the photons is acquired by a four channel digital oscilloscope on a memory depth of 1×10^6 points per channel and a time resolution of 10 ns. The acquired sequence is hence 10 ms long and it can be repeated at will after the memory of the oscilloscope has been emptied. For the sake of simplicity, the synchronization signal is sent to the oscilloscope using a coaxial cable, but it would be straightforward to use the IR or green laser pulses for the same purpose.

The total number of photons detected by Bob is $N_D^{(b)} = 3.93 \times 10^4\ \mathrm{s}^{-1}$. The dark counts on Bob's APDs with no signal at the input are $(d_H, d_V, d_L, d_R) = (150, 180, 380, 160)\ \mathrm{s}^{-1}$. This includes APD's dark counts and background noise due to ambient light that is carefully shielded using dark screens and pinholes. Considering the 23 ns lifetime of the NV center, a post selection of pulses within a 50 ns gate selects approximatively $\eta_g = 90\%$ of all single photons and keeps only $\beta_g = 27\%$ of the background counts. After basis reconciliation, the raw bit rate is then $N_r = \eta_g N_D^{(b)}/2 = 1.77 \times 10^4\ \mathrm{s}^{-1}$. Taking into account the detection gate, the fraction of dark counts versus useful photons during a detection gate is therefore $p_{\mathrm{dark}} = \beta_g \sum_{i=H,V,L,R} d_i/[\eta_g N_D^{(b)}] = 0.7\%$. The static polarization error rates are measured while Alice codes each one of the four polarizations, and they are $p_{\mathrm{pol}}^{\mathrm{HV}} = 1.2\%$ in the *H-V* basis and $p_{\mathrm{pol}}^{\mathrm{LR}} = 3.2\%$ in the *L-R* basis, owing to the slight imperfection brought by the achromatic wave plate (dark counts have been subtracted in these values). One can thus estimate the quantum bit error rate (QBER) to be $e = (p_{\mathrm{dark}} + p_{\mathrm{pol}}^{\mathrm{HV}} + p_{\mathrm{pol}}^{\mathrm{LR}})/2 = 2.6\%$. By comparing the full key that Bob received to the one that Alice sent, the measured QBER is found to be $e = 4.6\% \pm 1\%$. The difference with the previous value is attributed to the fact that static polarization errors are a lower bound to the real dynamic errors, owing to the nonideal shape of the electric pulses driving the EOM.

The complete secret key transmission was achieved by carrying out error correction and privacy amplification using the public domain software QUCRYPT designed by Salvail [18]. This leads to an average of 77 secret bits shared by Alice and Bob in a 10 ms sequence.

We now compare the performance of our single photon BB84 setup with QKD schemes using WCPs [7,19]. The comparison is carried out by taking the detection efficiency and the dark counts of Bob in the present setup. For WCP we assume a detection gate of 2 ns that is typical for recent experiments [7,19]. The quantities that are compared are the maximum allowed on-line losses and the secret bit rate. Since QKD is supposed to offer unconditional security, it is assumed that a potential eavesdropper (Eve) has an unlimited technological power to carry out individual attacks within the rules of quantum mechanics. Eve can then access all the information leakage caused by the quantum bit error rate e and by the multiphoton pulses [5]. In the case of WCP with an average number μ of photons per pulse at Alice's station ($\mu \ll 1$), the probability of a multiphoton pulse is given by $S_m^{\mathrm{WCP}} = \mu^2/2$. The only way to reduce the fraction of multiphoton pulses in WCP is therefore to reduce the bit rate by working with smaller μ. To the contrary, SPP offers the possibility of achieving a vanishing ratio of multiphoton pulses without any tradeoff on the filling of the pulses. In the present experiment the probability of a multiphoton pulse is reduced to $S_m^{\mathrm{SPP}} = C(0)\mu^2/2$ with $C(0) = 0.07$.

The important figure to be evaluated is the number of secure bits per pulse (G) after error correction and privacy amplification. This quantity is given by [6]

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

The quantity p_{exp} is the probability that Bob has a click on his detectors (including possible dark counts) during a detection gate, and S_m is the probability of a multiphoton photon pulse just at the output of Alice's station. The function $f[e]$ depends on the algorithm that is used for the error correction. The Shannon limit gives $f[e] = 1$ for any e, which is the value taken in Fig. 3. For the best known algorithm, $f[e] = 1.16$ for $e \leq 5\%$ (this value of $f[e]$ is used here). In our setup, the parameters are $(p_{\mathrm{exp}}, S_m, e) = (7.4 \times 10^{-3}, 7 \times 10^{-6}, 4.6 \times 10^{-2})$ so that $G = 1.68 \times 10^{-3}$. The number of secure bits per second given by Eq. (1) is thus $N_{\mathrm{QKD}} = 8900\ \mathrm{s}^{-1}$, which is reasonably close to our experimental value of $7700\ \mathrm{s}^{-1}$.

As can be seen in Fig. 3, our SPP quantum cryptographic system has a quantitative advantage over the best existing WCP systems. When any type of individual attacks, without any technological limitations, are taken into account, our SPP system can deliver an absolutely secure secret key at a higher bit rate and offers the possibility of transmitting this key over longer distances. Our quantum cryptographic setup compares also favorably with QKD experiments using pairs of entangled photons [20], with a significantly higher secure bit rate in our case (though this may depend on various other practical limitations). Moreover, several relatively simple

improvements could give SPP-QKD protocols an even greater advantage. In particular, inserting the emitter in a microcavity [21] is within experimental reach. This may be helpful to increase the collection efficiency, and therefore the secret bit rate, and also to narrow the emission spectrum, and thus to reduce polarization errors.

As a conclusion, we have demonstrated the first complete single photon quantum key distribution setup by using a very reliable room temperature single photon source. Despite the fairly broad spectrum of the single photons, a 4-states polarization encoding and decoding was implemented with low error rate (4.6%), and transmission over 50 m in air was successfully achieved with a secure bit rate of $N_{\mathrm{QKD}} = 7700\ \mathrm{s}^{-1}$. These results show that single photon QKD is a realistic candidate for long distance quantum cryptography, such as surface-to-satellite QKD.

We thank John Rarity for very fruitful discussions, Louis Salvail and Martial Tarizzo for helping us with the "QUCRYPT" software [18], Hervé Rigneault for providing us with the back reflecting mirror, Alain Aide and Frédéric Moron for the electronics, Robert Pansu for the loan of the time to amplitude converter, Stéphane Esnouf for the diamond irradiation, and Marie-Françoise Ravet for the diamond annealing. This work is part of the "S4P" project supported by the European Union IST/ FET/ QIPC Program.

*Email address: alexios.beveratos@iota.u-psud.fr
†Present address: Laboratoire de Physique de la Matière Condensée, Ecole Polytechnique, F-91128 Palaiseau, France.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, Piscataway, NJ, 1984), p. 175.
[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[4] id Quantique SA, http://www.idquantique.com
[5] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[6] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[7] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Phys. Rev. Lett. **84**, 5652 (2000).
[8] F. de Martini, G. di Guiseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).
[9] R. Brouri, A. Beveratos, J.-Ph. Poizat, and P. Grangier, Phys. Rev. A **62**, 063817 (2000).
[10] Th. Basché, W. E. Moerner, M. Orrit, and H. Talon, Phys. Rev. Lett. **69**, 1516 (1992); C. Brunel, B. Lounis, Ph. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999); L. Fleury, J. M. Segura, G. Zumofen, B. Hecht, and U. P. Wild, Phys. Rev. Lett. **84**, 1148 (2000); B. Lounis and W. E. Moerner, Nature (London) **407**, 491 (2000); F. Treussart, A. Clouqueur, C. Grossman, and J.-F. Roch, Opt. Lett. **26**, 1504 (2001).
[11] P. Michler, A. Imamoğlu, M. D. Mason, P. J. Carson, G. F. Strouse, and S. K. Buratto, Nature (London) **406**, 968 (2000).
[12] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoğlu, Science **290**, 2282 (2000); C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, Phys. Rev. Lett. **86**, 1502 (2001); V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen T. Tsegaye, E. Goobar, M.-E. Pistol, L. Samuelson, and G. Björk, Appl. Phys. Lett. **78**, 2476 (2001); E. Moreau, I. Robert, J.-M. Gérard, I. Abram, L. Manin, and V. Thierry-Mieg, Appl. Phys. Lett. **79**, 2865 (2001).
[13] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999); Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, Science **295**, 102 (2002).
[14] R. Brouri, A. Beveratos, J.-Ph. Poizat, and P. Grangier, Opt. Lett. **25**, 1294 (2000); C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).
[15] A. Beveratos, R. Brouri, T. Gacoin, J.-Ph. Poizat, and Ph. Grangier, Phys. Rev. A **64**, 061802(R) (2001).
[16] A. Beveratos, S. Kühn, R. Brouri, T. Gacoin, J.-Ph. Poizat, and P. Grangier, Eur. Phys. J. D **18**, 191 (2002).
[17] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup, and C. von Borczyskowki, Science **276**, 2012 (1997).
[18] P. M. Nielsen, C. Schori, J. L. Sorensen, L. Salvail, I. Damgard, and E. Polzik, J. Mod. Opt. **48**, 1921 (2001); http://www.cki.au.dk/experiment/qrypto/doc/
[19] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, quant-ph/0203118.
[20] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000); D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, *ibid.* **84**, 4733 (2000); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *ibid.* **84**, 4737 (2000); G. Ribordy, J. Brendel, J. D. Gautier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2001).
[21] J. M. Gérard, B. Sermage, B. Gayral, B. Legrand, E. Costard, and V. Thierry-Mieg, Phys. Rev. Lett. **81**, 1110 (1998).