Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source

Qin Wang,[1,2,*] Wei Chen,[1] Guilherme Xavier,[2] Marcin Swillo,[2] Tao Zhang,[1] Sebastien Sauge,[2] Maria Tengner,[2] Zheng-Fu Han,[1] Guang-Can Guo,[1] and Anders Karlsson[2]

[1]*Department of Physics, Key Laboratory of Quantum Information, CAS, USTC, 230026, Hefei, China*
[2]*Department of Microelectronics and Applied Physics, Royal Institute of Technology (KTH), Electrum 229, SE-164 40 Kista, Sweden*

(Received 4 November 2007; published 5 March 2008)

We have experimentally demonstrated a decoy-state quantum key distribution scheme (QKD) with a heralded single-photon source based on parametric down-conversion. We used a one-way Bennett-Brassard 1984 protocol with a four states and one-detector phase-coding scheme, which is immune to recently proposed time-shift attacks, photon-number splitting attacks, and can also be proven to be secure against Trojan horse attacks and any other standard individual or coherent attacks. In principle, the setup can tolerate the highest losses or it can give the highest secure key generation rate under fixed losses compared with other practical schemes. This makes it a quite promising candidate for future quantum key distribution systems.

DOI: 10.1103/PhysRevLett.100.090501 PACS numbers: 03.67.Dd, 03.67.Hk, 42.65.Yj

Since the Bennett-Brassard 1984 (BB84) protocol [1] was put forward, quantum key distribution (QKD) has attracted more and more attention from the worldwide scientific research community, since its unconditional security can be ensured by the theory of quantum mechanics [1–5]. However, the ''in principle'' unconditional security has always been threatened by imperfect realistic systems, such as nonideal single-photon sources (SPS), large channel losses and imperfect single-photon detectors. Luckily, some security proofs have also been given under those imperfect experimental conditions [6–12].

Hitherto, an attenuated laser, i.e., a weak coherent state (WCS) is often used instead of an ideal single-photon source in present quantum key distributions. Unfortunately, there are at least two drawbacks with this kind of source. One is the large vacuum state component, which results in a limited secure transmission distance. The other is a significant ratio between the multiphoton and single-photon probabilities, which opens a back door for a photon-number splitting (PNS) attack [7,8,13]. In order to maintain the security, one has to attenuate the laser into a very weak intensity, which inevitably results in a very low key generation rate. Fortunately, the so called decoy-state method has come to the rescue, as it can significantly improve the performance of QKD in practical systems [14–19].

Alternatively, a turnstile single-photon source or a heralded single-photon source (HSPS) can be used instead of an ideal single-photon source. Already, several promising implementations of such sources have been demonstrated, some based on color centers emission [20–22], some based on quantum-dot emission (QD) [23,24], and some based on parametric-down-conversion (PDC) processes [25–27]. In fact, a true single-photon source can never be made in practice, such devices can only produce states with a sub-Poissonian distributed photon count. Vacuum and multiphoton components still exist. Therefore, the decoy-state method is still needed in a QKD implementation using a heralded single-photon source. Here, we apply both HSPS and the decoy-state method in our QKD experiment. To our knowledge, this is the first time the two components have been combined in a true QKD experiment. The combination drastically increase the maximum tolerable channel losses or the secure key generation rates under fixed losses compared with WCS.

The main idea of the decoy-state method is to randomly send out signals among several different intensities, which allows one to estimate the behavior of the vacuum, the single-photon and the multiphoton components individually. As a result, an eavesdropper's presence will be detected. In our experiment, we use a three-intensity decoy-state method [15,18,28], and our source is a HSPS with sub-Poissonian distribution emitting from a PDC process. By applying the same characterization method as in [25], we can get the photon-number distributions of our source shown in Table I:

Here p_0, p_1, and p_2 represent the probabilities of vacuum, single-photon and multiphoton components individually; P_{cor} is the correlation rate of photon pairs, i.e., the probability of generating a heralded photon whenever a heralding one has been detected; $g^{(2)}(0)$ is the normalized second-order correlation function of the field at zero time delay. Because of a continuous-wave laser being used as the pump, the multiphoton probability is very low, in fact, it can be as low as 2% of the multiphoton probability in a weak coherent source having the same single-photon probability. Clearly, our source has a substantial sub-Poissonian distribution.

Using the same method as in [28–30], and taking statistical fluctuation into account, we can derive a lower bound of the counting rate of single-photon states (Y_1^L)

TABLE I. The measured photon-number distributions of our HSPS under different triggering frequencies.

	Trigger frequency (after time chopper, kHz)	Intensity (mean photons per gate, 25 ns	p_0	p_1	p_2	$g^2(0)$	P_{cor}
μ	200	0.588×10^{-3}	0.726 95	0.272 88	1.6005×10^{-4}	4.56×10^{-3}	0.272 67
μ	650	5.532×10^{-3}	0.698 10	0.300 29	1.6556×10^{-3}	3.53×10^{-2}	0.298 09

and an upper bound of the quantum bit-error rate of single-photon states (e_1^U) as:

$$Y_1^L = \frac{p'_2(\mu')Q_\mu^L - p_2(\mu)Q_{\mu'}^U - Y_0^U[p_0(\mu)p'_2(\mu') - p'_0(\mu')p_2(\mu)]}{p_1(\mu)p'_2(\mu') - p'_1(\mu')p_2(\mu)}, \tag{1}$$

$$e_1^U = \frac{Q_{\mu'}E_{\mu'}^U - e_0 Y_0^L p'_0(\mu')}{Y_1^L p'_1(\mu')}; \tag{2}$$

where e_0 and Y_0 are the quantum bit-error rate and counting rate of vacuum state; μ (μ') is the mean photon number per time slot (what we used is 2.5 ns in our experiment); N_μ, $N_{\mu'}$ and N_0 are the numbers of heralding pulses (i.e. the numbers of opening the gate of InGaAs detector) for different intensities (μ, μ', μ_0) respectively; Q_μ ($Q_{\mu'}$) and E_μ ($E_{\mu'}$) are the overall counting rate and the quantum bit-error rate for signal μ (μ') individually; and $Q_\mu^L \equiv Q_\mu(1 - \frac{10}{\sqrt{N_\mu Q_\mu}})$; $Q_{\mu'}^U \equiv Q_{\mu'}(1 + \frac{10}{\sqrt{N_{\mu'} Q_{\mu'}}})$; $Q_{\mu'}E_{\mu'}^U \equiv Q_{\mu'}E_{\mu'}(1 + \frac{10}{\sqrt{N_{\mu'} Q_{\mu'} E_{\mu'}}})$; $Y_0^L \equiv (1 - \frac{10}{\sqrt{N_0 Y_0}})$; $Y_0^U \equiv (1 + \frac{10}{\sqrt{N_0 Y_0}})$ [31];

Furthermore, after error correction and privacy amplification, we can get the final key generation rate from the signal (μ') [12,32]:

$$R \geq q\{-Q_{\mu'} f(E_{\mu'}) H_2(E_{\mu'}) + Q_0 + Q_1^L[1 - H_2(e_1^U)]\}, \tag{3}$$

where the factor of q ($=\frac{1}{2}$) comes from the cost of basis mismatch in the Bennett-Brassard 1984 (BB84) protocol, (or it is $\frac{1}{4}$ when a one-detector scheme is used); $f(E_{\mu'})$ is a factor for the cost of error correction given existing error correction systems in practice; We use $f = 1.22$ here [8]; $Q_0 \equiv Y_0 p'_0(\mu')$; $Q_1^L \equiv Y_1^L p'_1(\mu')$; $H_2(x)$ is the binary Shannon information function, given by: $H_2(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$.

As shown in Fig. 1, using the BB84 protocol and under the same experimental conditions, i.e., the same dark count rate (0.8×10^{-5}/gate), the same detection efficiency (7.5%), and the same misalignment of the system ($e_{\mathrm{detector}} \sim 2.5\%$), we compare our HSPS based decoy-state scheme to several other schemes, including HSPS without decoy states, WCS with or without decoy states, and also the ideal single-photon source case. (Based on decoy states, we can give accurate estimations of Y_1^L and e_1^U as in our Eqs. (1) and (2) in the case of HSPS or as in Eq. (2) of Ref. [33] in the case of WCS; however, without decoy states, we have to do some pessimistic assumptions as in Eq. (4.1) of Ref. [34].) As can be seen, our scheme gets the maximum tolerable losses or the highest key generation rate under fixed losses among all these practical schemes. Moreover, if a better HSPS (with 70% correlated photon pairs, as reported in [35]) is used, its performance comes close to the ideal single-photon source.

Our experimental setup (implemented at KTH with joint equipment from KTH and USTC) is shown in Fig. 2. We use a 532 nm continuous-wave (cw) laser to pump a periodically poled $LiNbO_3$ (PPLN) crystal of 50 mm length, to generate nondegenerate correlated photon pairs (with 809 and 1555 nm wavelengths); After triggering one photon at 809 nm, with gating time at 2.5 ns and gating frequency at 650 kHz, we can get a HSPS with a narrow bandwidth (0.8 nm FWHM), which has about 30% single-photon probability as shown in Table I [25]. The heralded photon is transmitted from Alice to Bob through 25 km of spooled SMF-28 fiber (attenuation: 0.2 dB/km), incorpo-

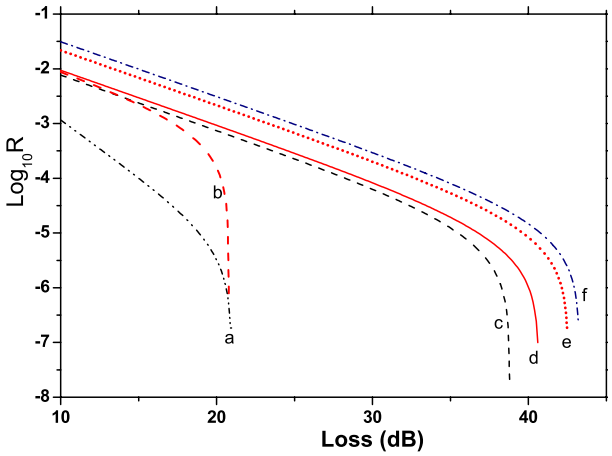

FIG. 1 (color online). The key generation rate vs the total losses comparing several different schemes. The numerical simulations are done in the case of: (a) with WCS and without decoy-state method; (b) with HSPS and without decoy-state method; (c) with WCS based decoy-state method (with optimal values of μ' at each points and an infinite number of decoy states); (d) with HSPS based decoy-state method with $P_{\mathrm{cor}} = 30\%$ (with $\mu' = 5.53 \times 10^{-3}$ and $\mu = 5.88 \times 10^{-4}$, these parameters come from our experiment below, after numerical simulation, we also find the key rate is stable with moderate changing the value of μ' or μ); (e) with HSPS based decoy-state method with $P_{\mathrm{cor}} = 70\%$(with $\mu' = 5.53 \times 10^{-3}$ and $\mu = 5.88 \times 10^{-4}$); (f) with the ideal SPS. (Note: Without taking statistical fluctuation into account in all these lines.)

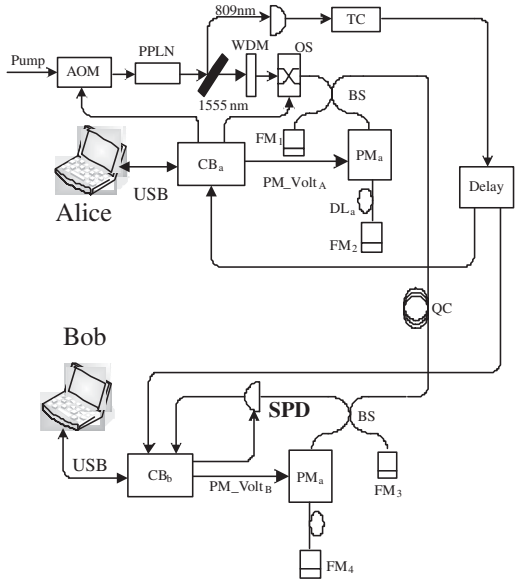

FIG. 2. The experimental setup of our quantum key transmission system. PPLN: periodically-poled $LiNbO_3$, AOM: acousto-optical-modulator, WDM: wavelength-division multiplexing, OS: optical switch, TC: time chopper, BS: beam-splitter, FM: Faraday Mirror, PM: phase modulator, DL: delay line, QC: quantum channel, SPD: single-photon detector, CB: control board.

rating a one-way Faraday-Michelson (*F-M*) QKD system [36]. We use a four-state and one-detector phase-coding scheme, which is immune to time-shift attacks [37,38], faked-state attacks [39], Trojan horse attacks [40], and can also been proven to be secure against any other standard individual or coherent attacks.

In order to avoid the large insertion loss of presently available optical amplitude modulators (AM, >3 dB), we use a fiber pig-tailed optical switch (OS, 0.6 dB loss) at the arm of signal (1555 nm), and place an acousto-optic-modulator (AOM) before the pump light, by controlling both of them in our program (changing between μ and μ' with AOM, and changing between μ and μ_0 with OS), we can randomly generate signals at 1555 nm wavelength among the three intensities: $[\mu', \mu, \mu_0] = [5.532 \times 10^{-3}, 0.588 \times 10^{-3}, 0.577 \times 10^{-5}]$, [here, μ is the mean photon number per gate, i.e., 2.5 ns, and because of an imperfect isolation ratio of the optical switch (~20 dB), we cannot use a real vacuum state for μ_0, which will decrease the estimate of Y_1, hence give a lower value of R], and the ratio between them is about 10:4:1. Meanwhile, we set a time chopper (see detail in Ref. [41]) in the triggering signal, on one hand to easily synchronize the signals at 1555 nm, on the other hand to keep the dark count rate for the three intensities at almost the same level. In addition, in order to get a higher visibility in the *F-M* interferometers (>95%, without removing any dark counts), we use a wavelength-division multiplexing filter (WDM) to further narrow the bandwidth of the signal photons (0.4 nm FWHM).

In our QKD system, we adopted a scan and transmission mode [36,41], which makes it quite stable for several hours of continuous measurements. For example, during a typical measurement of 200 min, (with effective transmission time about 70 min, the scan and responding time are considerably longer than the transmission time because of the low coincidence count rate), with a total of 1.5×10^9 triggering pulses, the detection efficiency is about 7.5%, the vacuum state counting rate is about 0.8×10^{-5}/gate, (we attribute 0.7×10^{-5} coming from dark counts, and 0.1×10^{-5} coming from the leakage of the optical switch and the misalignment of the system), the counting rate, $Q_{\mu'}$ (Q_μ) and average quantum bit-error rate (QBER), $E_{\mu'}$ (E_μ) are about 6.64×10^{-5} (6.38×10^{-5}) and 6.88% (6.43%), respectively, and we can get about 30.90×10^3 bits sifted key from total 84.60×10^3 coincidence counts after a total loss of 36 dB. Finally, we can deduce out 3.77×10^3 secure key, which agrees well with the theoretical value as shown in Fig. 3 (using the simulating model in [18,28,29]).

The final key rate is lower than in other systems, because there are large losses in our QKD system, including the insertion losses of the WDM filter and the optical switch, the inefficient InGaAs detector, and most importantly, the *F-M* interferometer, for the signal photons have to go through each phase modulator (PM) twice, and have to suffer losses from two beam-splitters. In all, the total losses are about 31 dB. In fact, these losses can be decreased substantially. First, the narrow bandwidth filter should be placed before the heralding detector instead of before the transmission line. This will not only avoid the loss of signal photons, but also improve the quality of correlated photon pairs (70% in [35]); Second, to use a low-loss *M-Z* interferometer (as used in [42]) instead of our present *F-M*

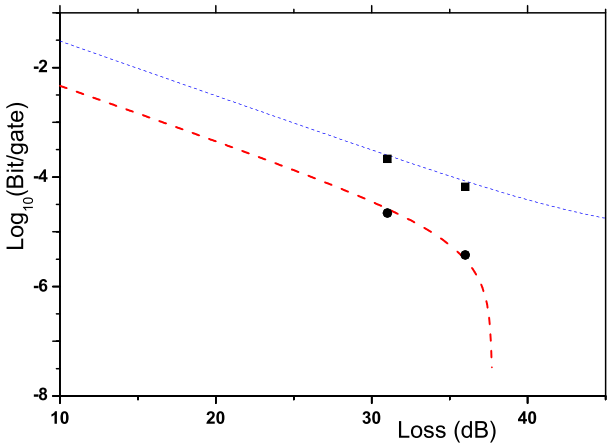

FIG. 3 (color online). Comparing the theoretical values and experimental results in coincidence counting rate and the final secure key rate. The dotted line and dashed line represent theoretical counting rate for the signal photons (μ') and final secure key rate (taking statistical fluctuation into account) individually. The dots and squares are the corresponding experimental results at the total loss of 31 and 36 dB.

interferometer, as the former can have about 6 dB less loss; Thirdly, to use a better detector at 1555 nm, with a lower dark count rate ($\sim 10^{-6}$) or a higher detection efficiency (10%–15%); Fourthly, if a two-detector scheme is used, another 3 dB is gained. All in all, with present technology, it is realistic to decrease the loss by 15–18 dB in this QKD system, which is quite considerable for a long distance transmission (>100 km).

Despite of these deficiencies mentioned above, this experiment is still sufficient to prove, in principle, that our HSPS based decoy-state scheme can tolerate the highest losses among all practical schemes, which also means the highest secure key generation rate under fixed losses. Therefore, it is a good candidate for future quantum key distribution systems.

The authors thank Professor X. B. Wang (Tsinghua Univ.) and Dr. C. H. F. Fung (Univ. of Toronto) for useful discussions, and Professor G. Björk for valuable comments, and also thank ACREO AB for the splicing machine used, thank M. Chacinski and M. Yan for technical assistance. This work was funded by the EU through the QAP (Qubit Applications-015848) project, and the SECOQC project (No. FP6-2002-IST-1-506813), the Swedish Science Research Council, the Swedish Foundation for Strategic Research, the ECOC Foundation; and partly funded by the National Science Foundation of China under Grant No. 60537020 and No. 60621064, Chinese Academy of Sciences and International Partnership Project. G. B. Xavier thanks the Brazilian agencies CAPES and CNPq for financial support.

*qinw@kth.se

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] D. Mayers, J. ACM **48**, 351 (2001).
[5] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).
[6] D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1998), p. 503.
[7] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[9] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, J. Mod. Opt. **48**, 2009 (2001).
[10] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[11] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[12] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[13] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[14] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[15] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[16] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[17] X. B. Wang, Phys. Rev. A **72**, 012322 (2005).
[18] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005).
[19] X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).
[20] A. Beveratos *et al.*, Phys. Rev. Lett. **89**, 187901 (2002).
[21] E. Waks *et al.*, Nature (London) **420**, 762 (2002).
[22] R. Alleaume *et al.*, New J. Phys. **6**, 92 (2004).
[23] S. Kako, *et al.*, Nat. Mater. **5**, 887 (2006).
[24] K. Sebald *et al.*, Appl. Phys. Lett.. **81**, 2920 (2002).
[25] M. Tengner and D. Ljunggren, arXiv:quant-ph/0706.2985v1.
[26] H. D. Riedmatten *et al.*, J. Mod. Opt. **51**, 1637 (2004).
[27] S. Mori, J. Söderholm, N. Namekata, and S. Inoue, Opt. Commun. **264**, 156 (2006).
[28] Q. Wang, X. B. Wang, and G. C. Guo, Phys. Rev. A **75**, 012312 (2007).
[29] Q. Wang, X. B. Wang, G. Björk, and A. Karlsson, Europhys. Lett. **79**, 40001 (2007).
[30] Q. Wang and A. Karlsson, Phys. Rev. A **76**, 014309 (2007).
[31] We estimated e_1 and Y_1 very conservatively as within 10 standard deviations, which promises a confidence interval for statistical fluctuations of less than 1×10^{-23}.
[32] M. Koashi, arXiv:quant-ph/0609180v1.
[33] Y. Zhao, B. Qi, X. F. Ma, H. K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[34] X. F. Ma, arXiv:quant-ph/0503057v1.
[35] A. Zavriyev and A. Trifonov, in *Proceedings of single photon workshop 2007* (Turin, Italy, 2007).
[36] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005); Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, Appl. Phys. Lett. **86**, 221103 (2005).
[37] B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, Quantum Inf. Comput. **7**, 073 (2007).
[38] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, H. K. Lo, arXiv:quant-ph/0704.3253.
[39] V. Makarov and J. Skaar arXiv:quant-ph/0702262.
[40] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[41] Qin Wang *et al.* (to be published).
[42] P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, and A. J. Shields, Appl. Phys. Lett. **91**, 161103 (2007).