Differential-phase-shift quantum key distribution using heralded narrow-band single photons

Chang Liu,[1] Shanchao Zhang,[1] Luwei Zhao,[1] Peng Chen,[1] C. -H. F. Fung,[2] H. F. Chau,[2] M. M. T. Loy,[1] and Shengwang Du[1,*]

[1]*Department of Physics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China*

[2]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong, China*

[*]*dusw@ust.hk*

http://physics.ust.hk/dusw

Abstract: We demonstrate the first proof of principle differential phase shift (DPS) quantum key distribution (QKD) using narrow-band heralded single photons with amplitude-phase modulations. In the 3-pulse case, we obtain a quantum bit error rate (QBER) as low as 3.06% which meets the unconditional security requirement. As we increase the pulse number up to 15, the key creation efficiency approaches 93.4%, but with a cost of increasing the QBER. Our result suggests that narrow-band single photons maybe a promising source for the DPS-QKD protocol.

OCIS codes: (270.0270) Quantum optics; (270.5568) Quantum cryptography.

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
2. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), 175.
3. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
4. C. H. Bennett, "Quantum ography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124 (1992).
5. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (2000).
6. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).
7. H. -K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
8. K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89**, 037902 (2002).
9. K. Wen, K. Tamaki, and Y. Yamamoto, "Unconditional security of single-photon differential phase shift quantum key distribution," Phys. Rev. Lett. **103**, 170503 (2009).
10. E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A **73**, 012344 (2006).
11. K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A **68**, 022317 (2003).
12. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nat. Photonics **1**, 343–348 (2007).
13. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J. -P. Poizat, and P. Grangier, "Single photon quantum cryptography," Phys. Rev. Lett. **89**, 187901 (2002).

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

14. R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J. -P. Poizat, and P Grangier, "Experimental open-air quantum key distribution with a single-photon source," New J. Phys. **6**, 92 (2004).
15. E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Secure communication: Quantum cryptography with a photon turnstile," Nature **420**, 762 (2002).
16. P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, A. J. Shields, P. Atkinson, and D. A. Ritchie, "Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm," Appl. Phys. Lett. **91**, 161103 (2007).
17. A. Trifonov and A. Zavriyev, "Secure vommunication with a heralded single-photon source," J. Opt. B **7**, S772–S777 (2005).
18. A. Soujaeff, T. Nishioka, T. Hasegawa, S. Takeuchi, T. Tsurumaru, K. Sasaki, and M. Matsui, "Quantum key distribution at 1550 nm using a pulse heralded single photon source," Opt. Express **15**, 726–734 (2007).
19. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5**, 3–28 (1992).
20. A. Kuzmich, W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L. -M. Duan, and H. J. Kimble, "Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles," Nature **423**, 731–734 (2003).
21. S. Du, P. Kolchin, C. Belthangady, G. Y. Yin, and S. E. Harris, "Subnatural linewidth biphotons with controllable temporal length," Phys. Rev. Lett. **100**, 183603 (2008).
22. H. Yan, S. Zhu, and S. Du, "Efficient phase-encoding quantum key generation with narrow-band single photons," Chin. Phys. Lett. **28**, 070307 (2011).
23. S. Du, J. Wen, and M. H. Rubin, "Narrowband biphoton generation near atomic resonance," J. Opt. Soc. Am. B **25**, C98–C108 (2008).
24. S. Zhang, J. F. Chen, C. Liu, S. Zhou, M. M. T. Loy, G. K. L. Wong, and S. Du, "A A dark-line two-dimensional magneto-optical trap of 85Rb atoms with high optical depth," Rev. Sci. Instrum. **83**, 073102 (2012).
25. P. Kolchin, C. Belthangady, S. Du, G. Y. Yin, and S. E. Harris, "Electro-optic modulation of single photons," Phys. Rev. Lett. **101**, 103601 (2008).
26. P. Grangier, G. Roger, and A. Aspect, "Experimental evidence for a photon anticorrelation effect on a beam splitter: A new light on single-photon interferences," Europhys. Lett. **1**, 173–179 (1986).
27. D. Gottesman and H. -K. Lo, "Proof of Security of quantum key distribution with two-way classical communications," IEEE Trans. Inf. Theor. **49**, 457–475 (2003).

1. Introduction

Security is the heart of a practical communication network. Quantum key distribution (QKD) has drawn much attention in the past decades because of its unconditional security guaranteed by quantum mechanics [1], such as noncloning theorem and Heisenberg uncertainty. Since the first Bennett-Brassard 1984 (BB84) protocol [2], many schemes have been proposed and demonstrated [3–7]. Discrete polarization quantum states have been widely implemented due to its simplicity [2]. However, the fiber length of such a polarization-based QKD system is limited by the birefringence effect that causes the polarization fluctuation on the receiver. This limit can be overcome by differential phase shift (DPS) QKD [8, 9]: Alice divides the single photon into N (≥ 3) time slots and Bob detects the single photon using an unbalanced Mach-Zehnder (M-Z) interferometer. In the absence of eavesdropper, the sequenced single-photon pulses experience the same phase and polarization changes during propagation through the fiber transmission line, thus the bit error can be easily corrected at the receiver. The DPS-QKD also shows tolerance to photon-number-splitting (PNS) attacks [9, 10]. However, to best of our knowledge, all previous DPS-QKD experimental demonstrations were based on weak coherent pulses (WCP) [11, 12] that do not provide the unconditional security of QKD in principle. Single-photon sources have been explored for the BB84 protocol [13–18] since the first QKD experiment in 1992 [19], but their short coherence time makes them difficult for the DPS-QKD protocol, where the key information is carried by the phase difference between the sequential pulses. In the original DPS-QKD proposal [8], a single photon is split into paths with different lengths and then recombined with passive beam splitters that bring unavoidable loss. It is not practical for $N(>3)$-pulse DPS-QKD implementation because the key creation efficiency is proportional to $(N-1)/N^2$ and drops to 0 at a large N limit. Moreover, the phase stabilization

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

between different paths becomes a technological challenge as N increases.

Recently, narrow-band single photons with coherence time up to μs have been generated from cold atoms [20, 21]. Such a long coherence time allows us not only to directly produce single-photon DPS pulses with arbitrary phase pattern, but also to avoid the beam-splitter loss in the original DPS-QKD proposal. As studied by Yan *et al.* [22], the entire key creation efficiency scales as $(N-1)/N$ and approaches 100% at the limit of large N. Therefore, heralded narrow-band single photons with a long coherence time becomes attractive for realizing the single-photon DPS-QKD protocol.

In this paper, we report the first experimental demonstration of polarization-insensitive DPS-QKD protocol using heralded narrow-band single photons, following the suggestion by Yan *et al.* [22]. In the 3-pulse case, we obtain a quantum bit error rate (QBER) as low as 3.06% which meets the unconditional security requirement [9]. The key creation efficiency reaches 66.6% which is 3 times that of the original beam-splitter-based DPS-QKD scheme [22]. Moreover, we extend it to the cases of $N(>3)$ time slots and obtain a high key creation efficiency of 93.4% at N=15. Our polarization-insensitive result implies its potential application for long-distance fiber-based QKD.

2. DPS-QKD Protocol

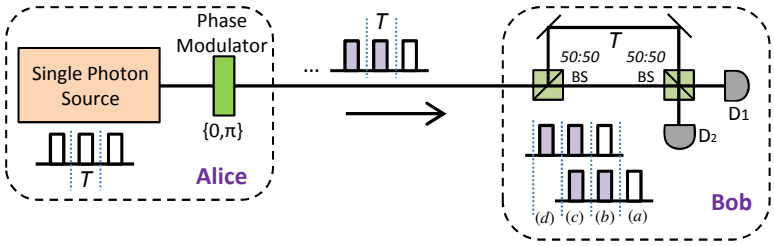

Fig. 1. DPS-QKD scheme with single photons for N=3. T is the modulated time slot period and the time delay between two paths of interferometer; D_1,D_2 are two single-photon detectors.

In the DPS-QKD configuration [8], a single photon is divided into $N(\geq 3)$ time slots with equal period T at Alice's site. The keys are encoded by preparing the relative phase shift between consecutive pulses in 0 or π randomly. Bob detects the incoming photon using an unbalanced M-Z interferometer setup with a path time delay difference equal to the period T. Here we describe the DPS-QKD protocol using single photons by taking the example at $N=3$, as illustrated in Fig. 1. The detection at Bob's site occurs in four possible time instances: (a) a photon in the first period passes through the short path; (b) a photon in the first period passes through the long path and a photon in the second period passes through the short path; (c) a photon in the second period passes through the long path and a photon in the third period passes through the short path; (d) a photon in the third period passes through the long path. Two detectors (D_1 and D_2) at the output ports of Bob's interferometer clicks for 0 or π phase difference based on Alice's modulation. Once a photon is detected, Bob records the time and which detector clicks. If the detectors click at the (b) or (c) time instances, Bob tells Alice only the information of time instances through a classical channel; otherwise, Bob discards the photon. Using the time-instance information and her phase encoding records, Alice knows which detector clicked at Bob's site. Defining the clicks at D_1 and D_2 as "0" and "1" respectively, Alice and Bob can obtain a confidential bit string as a sharing key. The photon sent from Alice to Bob is one of the following four states: $(|1_1 0_2 0_3\rangle \pm |0_1 1_2 0_3\rangle \pm |0_1 0_2 1_3\rangle)/\sqrt{3}$ (where $1_{i=1,2,3}$ represents the

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

photon at time slot *i*). As nonorthogonal with each other, the four states cannot be perfectly identified by a single measurement based on noncloning theorem [1], which guarantees the security of the scheme. The DPS-QKD protocol has been proven to be unconditionally secure with a QBER not greater than 4.12% [9].

3. Experimental setup and photon source characterization

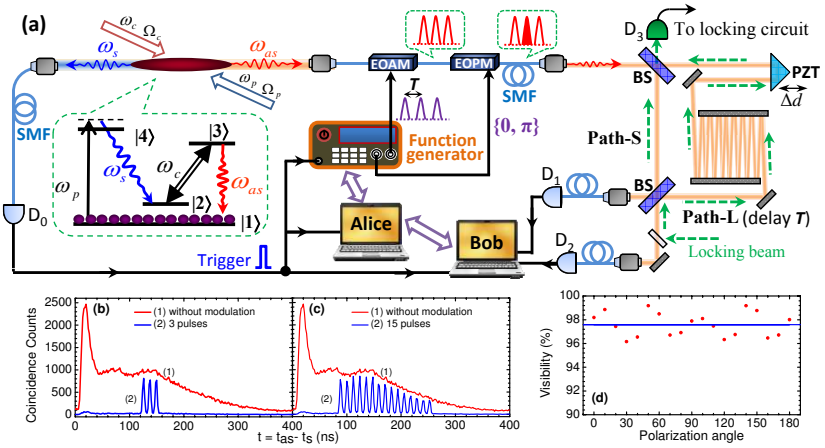

Fig. 2. (a) Experimental setup for narrow-band heralded single-photon generation and DPS quantum key distribution. The relevant ^{85}Rb atomic energy levels are $|1\rangle = |5S_{1/2}, F = 2\rangle$, $|2\rangle = |5S_{1/2}, F = 3\rangle$, $|3\rangle = |5P_{1/2}, F = 3\rangle$, and $|4\rangle = |5P_{3/2}, F = 3\rangle$. (b) and (c) show Stokes-anti-Stokes two-photon coincidence counts measured for 300 s with a time bin of 2 ns. The plot (1) is the heralded single-photon waveform without modulation. The plots (2) are the heralded single photons with 3- and 15-pulse modulations. (d) The visibility of the M-Z interferometer at detector D_1 with incident photons at different polarization angles.

We demonstrate the DPS-QKD scheme with narrow-band heralded single photons whose amplitude and phase are modulated. The experimental setup is illustrated in Fig. 2(a). We generate narrow-band photon pairs using spontaneous four-wave mixing [23] in a two-dimensional (2D) ^{85}Rb magneto-optical trap (MOT) [24], where the atoms are optically pumped into the ground state $|1\rangle$. The atomic cloud in the MOT has a length of 1.5 cm and a temperature of about 100 μK. In presence of counter-propagating pump (ω_p, 780 nm) and coupling (ω_c, 795 nm) laser beams, the phase-matched Stokes (ω_s, 780 nm) and anti-Stokes (ω_{as}, 795 nm) photon pairs are generated [21] and coupled into two opposing single-mode fibers (SMF) [21]. The pump and coupling beams, with the same collimated beam diameter of 1.6 mm, are aligned at a 3° angle with respect to the Stokes-anti-Stokes axis. The pump laser is blue detuned by 60 MHz from the transition $|1\rangle \rightarrow |4\rangle$ and the coupling laser is on resonance with the transition $|2\rangle \rightarrow |3\rangle$. Detecting a Stokes photon at the single-photon detector D_0 (PerkinElmer SPCM-AQ4C) heralds the generation of its paired anti-Stokes photon and synchronizes the timing for the entire experimental system. The anti-Stokes photons are successively sent through an electro-optical amplitude modulator (EOAM, fiber-based,10 GHz, EOspace) and an electro-optical phase modulator (EOPM, fiber-based, 10 GHz, EOspace), which are driven by a two-channel arbitrary waveform generator (Tektronix AFG 3252). In this way, we produce heralded single anti-Stokes photons with the waveform consisting of N time slots [25] and modulate the phase difference of 0 or π between two adjacent sequential pulses.

Then we couple the modulated anti-Stokes photons into a 3-meter-long SMF and send them

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

to a 1-bit delayed free-space unbalanced M-Z interferometer at Bob's site. The purpose of choosing the free-space setup is for polarization insensitive operation which will be demonstrated later. The 1-bit delay between long path (Path-L) and short path (Path-S) is fulfilled by reflecting single photons 8 times between two parallel mirrors in the long path. In order to eliminate the path length fluctuation caused by air flow in Path-L, the parallel mirrors are hermetically sealed in an aluminum container with two high-transmission windows. Moreover, a reference beam (795 nm) is fed into the interferometer in the reverse direction and detects the phase difference between the Path-L and Path-S with detector D_3 during the MOT loading stage. With a PZT-mounted prism inserted into the Path-L, we can actively lock the M-Z interferometer for a complete constructive or destructive interference. Coincidence counts between D_0 and the two single-photon detectors (D_1 and D_2, PerkinElmer SPCM-AQRH-16-FC) at the output ports of the interferometer are recorded by a time-to-digital converter (Fast Comtec P7888) with 2 ns bin width. The experiment runs at a repetition rate of 600 Hz with a 30% time window for the DPS-QKD experiment.

Before demonstrating the DPS-QKD, we characterize the single-photon source. In all measurements, the parameters for single-photon generation are fixed. We set the pump and coupling laser powers 35 μW and 1.6 mW respectively. The optical depth at the anti-Stokes transition is about 45. With the EOAM operating at its maximum transmission, the unmodulated Stokes-anti-Stokes coincidence counts for 300 s run time is shown as the plot(1) (red curve) in the Fig. 2(b) and (c). The heralded single photon has a temporal length of about 350 ns. The experimentally detected photon pair rate is about 375 pair/s. After taking into account the two-photon detection efficiency of 2.27% [including the photon detector quantum efficiencies (50% each), fiber-fiber coupling efficiencies at MOT (70%), EOM transmissions (50% each), fiber connection efficiency (81%), and filter transmissions (80% each)], it corresponds to 16520 pair/s produced from the source. Using the EOMs, we modulate the single photon into 3 time slots, which is illustrated as plot(2) (blue curve) in the Fig. 2(b). The full width at half maximum of the pulse is 5 ns , and the time interval T is 12 ns. In this 3-pulse modulation case, the utilization efficiency, defined as the ratio of modulated photon rate to the unmodulated photon rate, is only about 7.1%. We notice, as the interferometer in Bob's configuration is 1-bit delay, the interference of probability amplitudes only occurs between two adjacent time slots. As long as the difference between adjacent pulses is sufficiently small, it is not necessary to generate identical probability amplitudes across all the pulses for $N > 3$. Therefore, to utilize single photons efficiently, we produce N pulses following the slowly varying envelope of the unmodulated single-photon waveform, as shown in Fig. 2(c). Although it leads to a certain cost of increasing QBER, the utilization efficiency is significantly improved when N reaches a large value, such as N =15 which is shown as plot(2) (blue color) in Fig. 2(c). The utilization efficiency for N=15 reaches about 20.2%. We further implement two passive polarization-independent beam splitters (BS1, BS2) to reduce the polarization sensitivity of the M-Z interferometer on the receiver. The measured visibility of interference fringes as a function of incident polarization angle is displayed in Fig. 2(d). The red dots represent the experiment data, while the blue line is the average visibility of 97.6%. Thus our optical detection setup at Bob's side is insensitive to the polarization change which is crucial for long-distance fiber-based QKD.

4. DPS-QKD Experimental demonstration

We now follow the DPS-QKD protocol to distribute secure keys between Alice and Bob. At N = 3, we test all four possible phase modulation patterns: (0, 0, 0), (π, 0, 0), (0, π, 0) and (0, 0, π). For each fixed encoding pattern, we record the coincidence counts for 300 s run time between the detector D_0 and the detectors D_1 and D_2. After the measurement, Bob discards the photons detected during the first and last time instances [(a) and (d) in Fig. 1], and compares

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

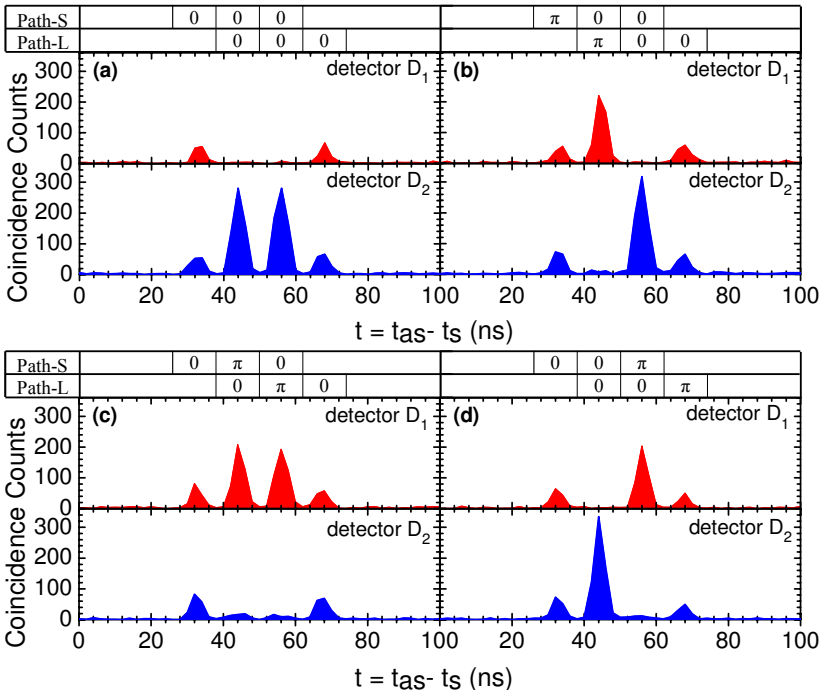

Fig. 3. Photon counts at the two output ports of M-Z interferometer at N=3 in the following modulation patterns: (a) (0, 0, 0), (b) (π, 0, 0), (c) (0, π, 0), and (d) (0, 0, π).

his detection events with Alice's encoded pattern through a classical communication channel. The measured coincidence counts are displayed in Fig. 3, where the corresponding fixed phase modulation pattern is shown above in the overhead table. The QBERs for pattern (0, 0, 0), (π, 0, 0), (0, π, 0) and (0, 0, π) are 2.98%, 4.48%, 10.67% and 6.18% respectively. Comparing the error rate of the four patterns, we find that a phase change always results in a higher error rate. This is mainly caused by the limited 240 MHz bandwidth of our arbitrary waveform generator. As a result, the step waveforms sent to the EOPM have finite rise and fall times of 2.5 ns. During this rise (or fall) time, phase shift is neither 0 nor π, resulting in the imperfect destructive interference at the outputs of M-Z interferometer. The error rates are expected to be reduced significantly if we use a faster waveform generator to control the phase shift more precisely. An alternative way to reduce QBER is to exclude these error events from the detection time window. We can set the single-photon detection at the middle of each interference time slot, only within a small data window which does not include the rise and fall times of phase modulation. We confirm this by reducing the detection time window to 2 ns, and obtain a QBER as low as 3.06%, which is below the threshold for unconditional security in the DPS-QKD scheme. In the experiment, the measured photon-counting rate of shaped N=3 pulses is 12 count/s and the key creation efficiency is 66.6%. With the 5 dB transmission line loss, the final sifted secure key rates for 12-ns data window and 2-ns data window are 3.8 bit/s and 1.7 bit/s.

With the ability to directly modulate single-photon temporal waveform into $N(>3)$ time slots, we also perform the operations of QKD in different $N(>3)$ cases. The number of possible phase modulation patterns increases exponentially with N. As an example, Fig. 4 shows the measured results for the following four phase patterns at N=15: (a) (0, 0, 0, π, π, 0, π, π, 0, 0, 0, π, π, π, 0), (b) (0, 0, 0, π, π, 0, π, π, 0, π, π, 0, 0, π, 0), (c) (π, 0, 0, 0, 0, π, π, 0, 0, π, π, 0, 0,

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

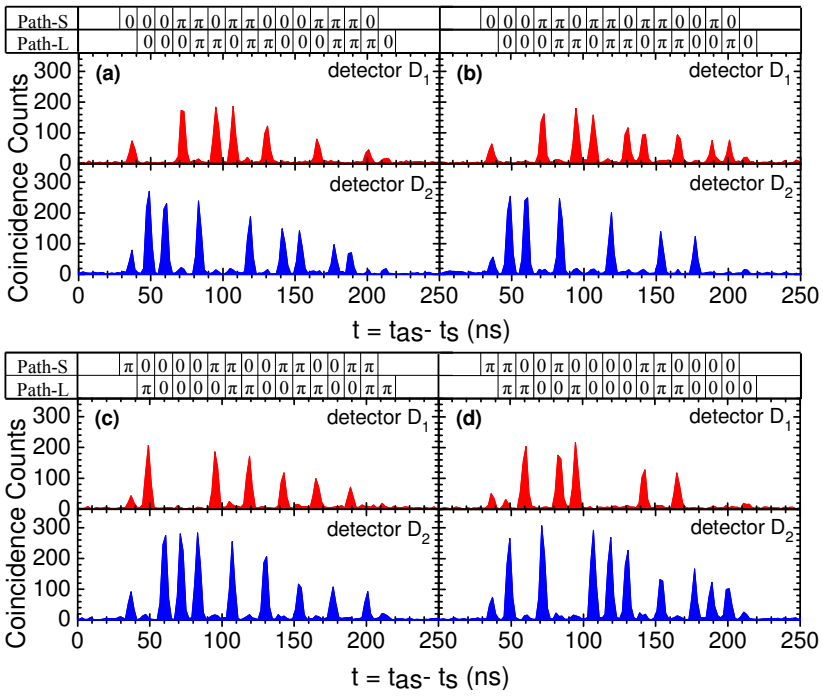

Fig. 4. Photon counts at the two output ports of the M-Z interferometer at N=15 in the following modulation patterns: (a) (0, 0, 0, π, π, 0, π, π, 0, 0, 0, π, π, π, 0), (b) (0, 0, 0, π, π, 0, π, π, 0, π, π, 0, 0, π, 0), (c) (π, 0, 0, 0, 0, π, π, 0, 0, π, π, 0, 0, π, π), and (d) (π, π, 0, 0, π, 0, 0, 0, 0, π, π, 0, 0, 0, 0).

π, π), and (d) (π, π, 0, 0, π, 0, 0, 0, 0, π, π, 0, 0, 0, 0). These patterns are generated based on pseudo-random process in a computer. In this case, with the full detection window (12 ns), the key generation rate is 18.4 bit/s with a QBER of 9.41%. As we reduce the detection window to 2 ns, the key generation rate becomes 4.4 bit/s and the QBER is 6.69%. As compared with N=3, the key creation efficiency reaches 93.4%.

5. Discussion and conclusion

5.1. Discussion

The unconditional security of single-photon DPS-QKD protocol is guaranteed by the quantum nature of the single photons [9]. In order to analyze the principle unconditional security of key distributions, we characterize the quality of heralded single photons by measuring its conditional autocorrelation function $g_c^{(2)} = (N_{012}N_0)/(N_{01}N_{02})$ [26], where N_0 is the Stokes counts at D_0, N_{01} and N_{02} are the twofold coincidence counts, and N_{012} is the threefold coincidence counts. An ideal coherent light source gives $g_c^{(2)} = 1$, while a pure single-photon source has $g_c^{(2)} = 0$ and a two-photon source has $g_c^{(2)} = 0.5$. Therefore $g_c^{(2)} < 0.5$ suggests the near-single-photon character. With the coincidence window including all the N time slots, we obtain the $g_c^{(2)}$ for different N cases shown in Fig. 5(a). The measured $g_c^{(2)}$ ranges from 0.2 to 0.33, which is well below the two-photon threshold. The multi-photon probability is as least reduced by a factor of $1/g_c^{(2)}$ comparing with a WCP source at the same rate, suggesting an improved security in the key distribution process.

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

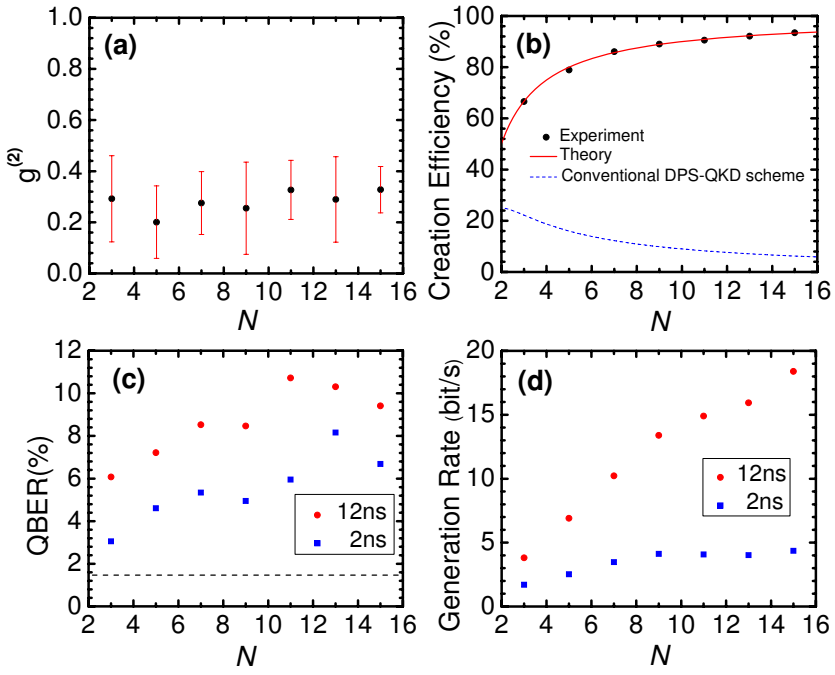

Fig. 5. The DPS-QKD characterization at different N: (a) the second-order correlation $g^{(2)}$ of the heralded anti-Stokes photons, (b) the key creation efficiency, (c) the average QBER, and (d) the key generation rate. The black dashed line in (c) is the QBER baseline (about 1.5%) caused by the detector dark counts.

If one takes the original proposed beam-splitter-based DPS-QKD scheme [8], Alice has only an efficiency of $1/N$ in sending a photon successfully. At Bob's side, photons at the first time slot in the short path and the last time slot in the long path do not contribute to the key and thus the maximum key detection efficiency of a single photon is $(N-1)/N$. Therefore the total key creation efficiency of the conventional scheme scales as $(N-1)/N^2$ which decreases to zero at the limit of large N [the blue dashed line in Fig. 5(b)]. In our experimental setup, the sending efficiency at Alice's site is always 1 and thus the key creation efficiency scales as $(N-1)/N$ which approaches 1 at the limit of large N. Figure 5(b) shows the difference between our experiment scheme and conventional DPS-QKD scheme in the key creation efficiency as a function of N. The experimental data (black dot) agrees well with the theory (red solid line).

The average QBERs for 12-ns and 2-ns coincidence windows at different N are shown in Fig. 5(c). For 12-ns coincidence window, we notice the QBERs for all N are higher than 6%. The QBER tends to increase with increasing the pulse number N. Two main reasons may account for this. The first is the finite rise and fall times (2.5 ns) of the step phase modulation which degrades the MZ inference, as described in Sec. 4. We confirm this at N=3 with 12-ns coincidence window in which the average QBER is 6.08% as shown in Fig. 5(c). However, when we only count the pattern (0, 0, 0) [Fig. 3(a)], the QBER is only 2.98%. The higher average QBER of 6.08% results from other phase modulated patterns. The larger N, the more frequently the phase change occurs, and the higher the average QBER is. Therefore, we expect implementing a faster waveform generator with shorter rise and fall times will significantly reduce the QBER. For example, at N=3 with 12-ns coincidence window, the average QBER can approach to 2.98% that is below the threshold required for the unconditional security. One can

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

also reduce the QBER by shortening the coincidence window to 2 ns from which the rise and fall times are excluded, as shown as the blue solid square data points in Fig. 5(c). The QBER at N=3 for the 2-ns coincidence window becomes 3.06%, which is well below the required value of 4.12% for the unconditional security. The second source of QBER is the accidental noise coincidence counts. As shown in Fig. 1(c), the heralded single photon waveform shows a decayed tail. As we increase N, the averaged single-photon (signal) to background (noise) ratio decreases. These increasing noise counts contribute directly to the QBER. The noise coincidence counts are mainly contributed from the uncorrelated photons from stray lights and the detector dark counts. In our setup running at 30% duty cycle, the dark counts for detectors D_0, D_1, and D_2 are 300 count/s, 6 count/s, and 6 count/s, respectively. The accidental coincidence counts from these dark counts cause a QBER of about 1.5%, as shown as the black dashed baseline in Fig. 5(c). If we take better single photon detectors with fewer dark counts (particularly D_0 in our setup) to eliminate this dark-count-induced QBER, the unconditional security of DPS-QKD demonstrated in this work can extend N up to 9.

Finally, we plot the experimental key generation rate as a function of N in Fig. 5(d). It is clear that the key generation rate increases with the increase of N. A larger N offers a higher utilization efficiency of a single photon and a higher final key creation rate. Under the security condition, the product of the QBER and the key generation rate maybe an appropriate figure of merit for the QKD system and it can be used to optimize the value of N.

5.2. Conclusion

As a conclusion, we have demonstrated the DPS-QKD using a narrow-band heralded single-photon source for the first time. For $N = 3$, we obtain a QBER of 3.06% with a 2-ns photon counting window [Fig. 5(c)], which meets the requirement of unconditional security. We also conduct the experiment with $N(>3)$ time slots, and the measurement of key creation efficiency agrees well with the theory, showing a significant improvement compared with conventional DPS-QKD scheme. The dependence of conditional autocorrelation $g_c^{(2)}$, QBER, key creation efficiency and generation rate on the pulse number N are studied systematically. Note that even though the QBER values for the cases with $N>3$ are higher than the known security threshold of 4.12% [9], use of a faster waveform generator for step phase modulation and detectors with fewer dark counts can extend the unconditional security to N=9. Meanwhile, the use of more sophisticated classical postprocessing techniques such as two-way classical communications [27] may be able to raise the tolerable QBER. Then, some of the cases with $N>3$ already demonstrated in this experiment may become secure, further showing the advantage of this scheme. However, this improvement has yet to be proven. Our results suggest the potential application of narrow-band single-photon source in quantum key generation and distribution. Our polarization insensitive setup is suitable for fiber-based long distance QKD systems.

Acknowledgements

The authors thank H.-K. Lo for helpful discussion and J.F. Chen for making the PZT-locking circuit. The work was supported by the Hong Kong Research Grants Council (No. HKU8/CRF/11G).

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013