CHIN. PHYS. LETT. Vol. 28, No. 7 (2011) 070307

Efficient Phase-Encoding Quantum Key Generation with Narrow-Band Single Photons *

YAN Hui(颜辉)[1,2**], ZHU Shi-Liang(朱诗亮)[1], DU Sheng-Wang(杜胜望)[2]

[1]*Laboratory of Quantum Information Technology, ICMP and SPTE, South China Normal University, Guangzhou 510006*

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

(Received 17 February 2011)

We propose an efficient phase-encoding quantum secret key generation scheme with heralded narrow-band single photons. The key information is carried by the phase modulation directly on the single-photon temporal waveform. We show that when the technique is applied to the conventional single photon phase-encoding BB84 and differential phase shift (DPS) quantum key distribution schemes, the key generation efficiencies can be improved by factors of 2 and 3, respectively. For $N(\geq 3)$-period DPS systems, the key generation efficiency can be improved by a factor of N. The technique is suitable for quantum-memory-based long-distance fiber communication systems.

PACS: 03.67.Dd, 42.50.Dv, 03.67.Hk DOI:10.1088/0256-307X/28/7/070307

Quantum key distribution (QKD) is an unconditionally secure method to distribute secret keys between two parties (Alice and Bob). The security of QKD is guaranteed by the principles of quantum mechanics,[1,2] such as noncloning theorem and Heisenberg uncertainty. Since the first QKD experiment using a 32 cm free-space transmission line was reported in 1992,[3] the key distribution distance has continued to increase. With the fiber-based decoy-state BB84 protocol, a photon number splitting (PNS) secure key distribution over 200 km has been achieved.[4] With the differential phase shift (DPS) QKD scheme, the PNS-secure key distribution distance record is also 200 km.[5] The attenuated laser is used as the source in the above schemes. In order to increase the key distribution distance, a quantum memory and quantum repeater are proposed and demonstrated recently.[6] Hence, a single photon, especially a narrowband single photon, is regarded as an attractive source for long distance QKD again besides the attenuated laser.[7] With single photons, phase-encoding BB84 (PE-BB84),[8] and the DPS-QKDs[9–11] are two typical schemes: Alice divides the single photon into two or more time slots and Bob detects the single photon using an unbalanced Mach–Zehnder (M-Z) interferometer, respectively. Because the sequenced single-photon pulses experience the same phase and polarization changes during propagation through the fiber transmission line,[9,10,12] the bit error can easily be corrected at the receiver. However, due to a lack of generating single photons with controllable (phase-amplitude) waveforms, in the conventional single photon PE-BB84 and DPS-QKD schemes, a single photon is split into paths with different lengths and then recombined with passive beam splitters that introduce unavoidable loss. As a result, the generation efficiency decreases as the number of time slots increases. In order to increase the generation efficiency, many methods have been proposed, such as using optical switches or a polarization beam splitter.[13]

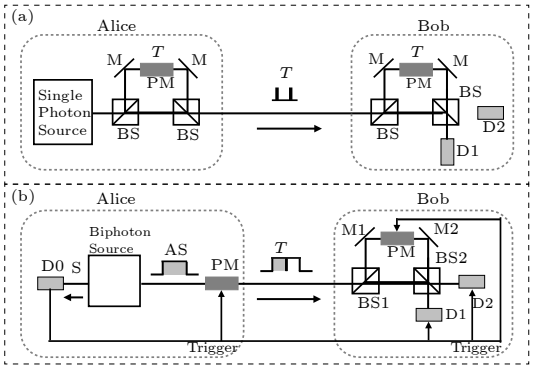

Fig. 1. (a) The conventional phase-encoding BB84 scheme; (b) our proposed phase-encoding BB84 scheme with heralded narrow bandwidth square wave single photons; S: Stokes; AS: anti-Stokes; PM: phase modulator; BS, BS1, BS2: 50% beam splitters; M, M1, M2: mirrors; D, D1, D2: single-photon detectors.

In this Letter, we propose another phase-encoding generation method to improve the key creation efficiency in the PE-BB84 and DPS-QKD schemes without using a M-Z interferometer on Alice's site. The motivation comes from the recent narrow-band nonclassical paired photon generation.[14–17] Using spontaneous four-wave mixing and electromagnetically induced transparency in cold atoms, a subnatural linewidth biphoton with a coherence time of

*Supported by the Hong Kong Research Council Project (No HKUST600809), the National Natural Science Foundation of China under Grant No 1097405, the National Basic Research Program of China under Grant Nos 2011CB922104 and 2007CB925204.

**Email: yanhui1981@gmail.com; yanhui@scnu.edu.cn

up to about 1 μs has been demonstrated.[18] Du *et al.*[19] proposed and demonstrated shaping biphoton temporal waveforms by periodically modulating the two classical driven fields. With such a long coherence time and under detecting one of the paired photons, heralded single photons with arbitrary phase-amplitude waveform can be generated with external light modulators.[20,21] It is then possible to eliminate the need for beam splitters in the conventional phase-encoding schemes by using directly phase modulated heralded narrow-band single photons.

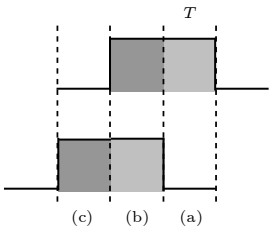

Fig. 2. Time sequence of the phase modulated square wave single photon of the proposed phase-encoding BB84 scheme. The ratio of the click probability in the three time sequences is $(a) : (b) : (c) = 1 : 2 : 1$. T is the phase modulated period (here we take $T = 100$ ns).

We first consider the PE-BB84 scheme and improve its key generation efficiency. Figure 1(a) shows the conventional setup. On Alice's site, a single photon is divided into one short path and one long path with phase modulation (PM) and a time delay of T after the first beam splitter (50%), and then is recombined at the second beam splitter (50%). This effectively splits the single photon as a superposition of two time slots separated by time T. The phase difference between these two time slots is modulated by one of the two nonorthogonal bases $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$ randomly. Bob measures the phase difference with two detectors in either the $\{0, \pi\}$ or the $\{\pi/2, 3\pi/2\}$ basis, using a phase modulator in the long path of an unbalanced M-Z interferometer whose path difference equals that on Alice's site. It is clear that the single photon on Alice's site has 50% probability of leaking out of the system and thus the maximum key sending efficiency is 1/2. On Bob's site, there is no photon loss through the beam splitters. To maximize the used efficiency of the single-photon source, it is better for us to avoid the beam splitters on Alice's site. Our proposed scheme is shown in Fig. 1(b), where Alice's site is modified. In our scheme, with the technique described in Refs. [20,21] and feedback waveform control, Alice makes use of narrow-band biphotons to generate a heralded single anti-Stokes photon with a rectangular shape with a temporal length of 2 T (for example, T=100 ns). This rectangular-shaped single photon then passes through a PM trigged by detection of the Stokes photon and the phase difference is encoded to the two time slots. The detection at Bob's site is similar to that in the conventional scheme [Fig. 1(a)] except that the trigger timing of detecting the Stokes photon is sent from Alice through a classical channel. In this way, there is no photon loss on Alice's site and the key generation efficiency is increased by a factor of 2. Bob could detect one photon at the three time instances with the ratio 1 : 2 : 1, as illustrated in Fig. 2, (a) the first period of the photon passes the short path of the M-Z interferometer; (b) the first period of the photon passes the long path and the second period of the photon passes the short path of the M-Z interferometer; (c) the second period of the photon passes the long path of the M-Z interferometer. In the time instant (b), the phase difference between the two consecutive periods will determine the outputs of the M-Z interferometer and then the click of the detector. When Bob detects a photon at the time instances (a) and (c), he will discard data. When Bob detects a photon at the time instance (b), a secret key bit can be created by comparing his basis with Alice's, similar to the protocol in polarization-based BB84.[3] Because Bob has 1/2 probability in measuring the phase difference and another 1/2 probability in matching the basis, the receiving-key efficiency is 1/4. Therefore accounting for the sending efficiency on Alice's side, the total key creation efficiency is 1/8 for the conventional PE-BB84 scheme, and 1/4 for the improved scheme. The security of the PE-BB84 scheme has been analyzed a lot in the past and is proven to be unconditionally secure.[2,22]

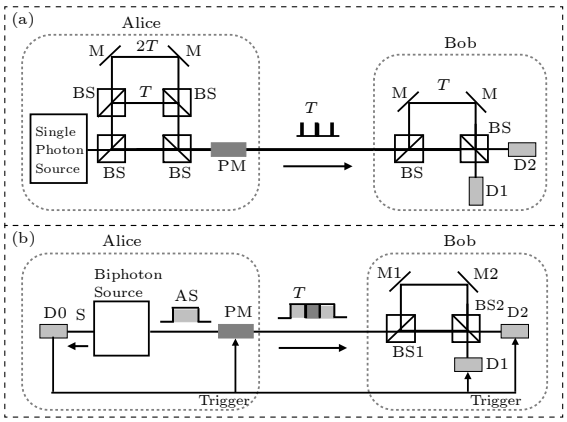

Fig. 3. (a) The currently implemented DPS-QKD scheme; (b) our proposed DPS-QKD scheme with heralded narrow bandwidth square wave single photons; S: Stokes; AS: anti-Stokes; PM: phase modulator; BS, BS1, BS2: 50% beam splitters; M, M1, M2: mirrors; D, D1, D2: single-photon detectors.

Now we turn to the DPS-QKD scheme that has been demonstrated to be one of the most applicable schemes.[8] We show that with a phase-modulated long single photon from a biphoton source, the key creation efficiency of the DPS-QKD scheme could also be improved significantly. Figure 3(a) shows the setup of the conventional DPS-QKD scheme.[8] On Alice's site, the photon from a single photon source is divided into

three paths with time separation T and then recombined by beam splitters. The keys are encoded by preparing the relative phase shift between two consecutive pulses in 0 or π randomly. Bob measures the phase difference using an unbalanced M-Z interferometer setup with a path difference that compensates for the time delay T. Similar to that in PE-BB84, the sending efficiency of a DPS photon is only 1/3 due to the loss of beam splitters. Such a loss can be eliminated in our improved scheme without using beam splitters on Alice's site, as shown in Fig. 3(b). Similar to the improved PE-BB84 system, we divide the long rectangular-shape photon with a temporal length 3 T into 3 time sequences with equal period T. As one does not know the exact arrival time of the single photon within the three time slots, the heralded single photon can be described as a superposition of $|1_a 0_b 0_c\rangle$, $|0_a 1_b 0_c\rangle$, and $|0_a 0_b 1_c\rangle$ (where 1_a represents the photon at time slot a, otherwise it is 0_a). Because the phase of each time slot is randomly modulated by 0 or π, the photon sent from Alice to Bob is in one of the four states: $1/\sqrt{3}(|1_a 0_b 0_c\rangle \pm |0_a 1_b 0_c\rangle \pm |0_a 0_b 1_c\rangle)$ in the present scheme. These four states, which are nonorthogonal with each other and thus cannot be identified by a single measurement, have the same mathematical forms as those in the conventional DPS-QKD scheme.[9,11] Therefore, the unconditional security of the proposed scheme can be proved following the procedure in Refs [9,11]. The detection setup on Bob's site is similar to that in the conventional scheme with the trigger timing sent from Alice through a classical channel by detecting the Stokes photons. It is clear that the single-photon sending efficiency becomes unity in this case and the encoding machine is lossless. In the DPS-QKD configuration, Bob detects a photon at four possible time instances with the ratio 1 : 2 : 2 : 1, as illustrated in Fig. 4: (a) the photon in the first period passes the short path of the M-Z interferometer, (b) the photon in the first period passes the long path and the photon in the second period passes the short path; (c) the photon in the second period passes the long path and the photon in the third period passes the short path; and (d) the photon in the third period passes the long path. In the time instances (b) and (c), the phase difference between the proper consecutive periods will determine the outputs of the M-Z interferometer and then the click of the detector. Bob discards the photons detected at the time instances (a) and (d), and communicates with Alice the time instance when he obtains a photon click only at (b) or (c).[9] With her own modulation pattern, Alice knows which detector clicked on Bob's site and key bits are created and shared by the two parties. The details of the protocol can be seen in Ref. [9]. Here we focus on the key creation efficiency. On Bob's site, photons counted at time instances (b) and (c) fully contribute to the key. The probability of these events is 2/3. Thus, taking into account the sending efficiency on Alice's site, the entire key creation efficiency is 2/9 for the conventional beam-splitter-based DPS-QKD scheme, and 2/3 for our improved scheme. Another feature that should be mentioned is the information capacity after error correction. As described above, the efficiency of obtaining sifted keys in our scheme is 3 times that in the conventional DPS-QKD scheme, while the error rate introduced by the simple intercept/resend attack is 1/4, which is the same as the other scheme. Thus, the new scheme has the larger final information capacity when other parameters hold the same.

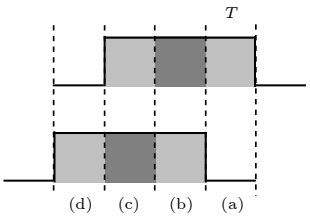

Fig. 4. Time sequence of the phase modulated square wave photon of our proposed DPS-QKD scheme. The ratio of the click probability in the four time sequences is $(a) : (b) : (c) : (d) = 1 : 2 : 2 : 1$. T is the phase modulated period (here we take $T = 100$ ns).

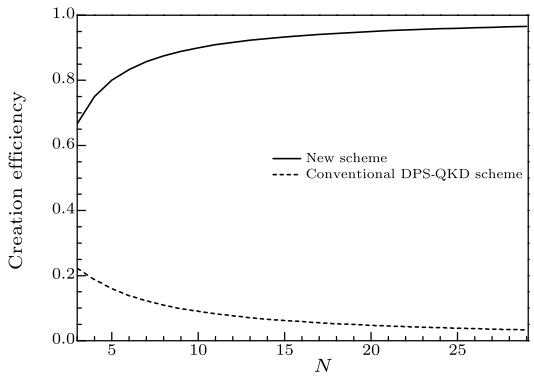

Fig. 5. The key creation efficiency with different N for our proposed scheme and the conventional DPS-QKD scheme (with passive BS).

As proposed by Inoue *et al.*,[9,23] the above DPS-QKD scheme with $N = 3$ time slots can be extended to the $N(> 3$ cases where the key receiving efficiency scales as $(N-1)/N$ and approaches 1 at a large N limit. However, in the conventional setup with passive beam splitters on Alice's site, the single-photon sending efficiency decreases at a larger N because it scales as $1/N$. As a result, the total key creation efficiency becomes $(N-1)/N^2$ and decreases to zero at the limit of large N. If we use heralded narrow-band single photons with proper phase-amplitude modulations, the sending efficiency on Alice's site will always be 1 and will not depend on N. Thus, in our proposed technique, the total key creation efficiency is proportional to $(N-1)/N$ and indeed reaches unity

at large N limit. Figure 5 shows the difference in the total creation efficiencies as a function of N between the proposed and the conventional DPS-QKD schemes for comparison.

In addition, besides the key creation efficiency, the secure key rate (SKR) is another important parameter to characterize a practical QKD system. Compared with the conventional single photon schemes, there are several more parameters that will limit the SKR in our scheme: first, the generation rate and the temporal length of the heralded single photon; with 300 ns temporal length photons, the SKR will be limited to about 3 MHz; using faster phase modulator (>30 GHz) allows us to reduce the temporal length from 300 ns to several ns or even shorter;[24] the generation rate can be increased if we shorten the temporal length of the single photon,[24] or using a spontaneous parametric down-conversion heralded single photon source. Secondly, the time jitter of the detector, with the time jitter of 100 ps, the detector will bring a error rate of 1% if $T = 10$ ns. Thirdly, the shape of the square wave single photon after a long distance transmission, especially the rising and falling edges, this shortage can be conquered if we let the temporal length of the single-photon slightly longer than NT (the effective signal length); the propagation losses in the optical fiber cables are larger for the 780 nm narrow-band single photons, as we proposed. Fortunately, the generation of telecom wavelength narrow-band photons has already been demonstrated in experiment.[25]

In summary, we have proposed a highly efficient phase-encoding quantum key generation scheme by using heralded narrow-band single photons with phase modulation. While implemented to the single photon PE-BB84 protocol, the entire key creation efficiency can be increased by a factor of 2. For the single photon DPS-QKD scheme with $N = 3$, the key creation efficiency can be increased by a factor of 3. We further show that in the conventional single photon scheme, the entire key creation efficiency decreases as we increase N and reaches zero at large N limit due to the beam splitter loss on Alice's site. In our proposed technique, the creation efficiency scales as $(N-1)/N$ and reaches unity at large N. The overall maximum efficiency may be limited only by shaping loss of the initial temporal waveform of heralded single photons emitted from their source, the quantum detection efficiencies, and propagation loss. The nearly rectangular-shaped subnatural linewidth biphotons[18] are ideal for this application with a reshaping loss of less than 20%. In addition, the narrow band photons can be directly integrated with the quantum memory and quantum repeater, so the described technique will be suitable for quantum-memory-based long-distance fiber transmission systems.

The authors thank He G P and Wang X B for helpful discussion.

References

[1] Gisin N et al 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V et al 2009 *Rev. Mod. Phys.* **81** 1301
[3] Bennett C H and Brassard G 1984 *Proc. IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India) (New York: IEEE) p 175
[4] Liu Yang et al 2010 *Opt. Express* **18** 8587
Rosenberg D et al 2009 *New J. Phys.* **11** 045009
Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
Lo H K et al 2005 *Phys. Rev. Lett.* **94** 230504
Yin Z Q et al 2008 *Chin. Phys. Lett.* **25** 3547
Wang W Y et al 2007 *Chin. Phys. Lett.* **24** 1463
[5] Takesue H et al 2007 *Nature Photon.* **1** 343
[6] Tanji H et al 2009 *Phys. Rev. Lett.* **103** 043601
Duan L M et al 2001 *Nature* **414** 413
Jiang L et al 2007 *Phys. Rev.* A **76** 012301
Chen Z B et al 2007 *Phys. Rev.* A **76** 022329
Mei F et al 2010 *Phys. Rev.* A **82** 052315
[7] Waks E et al 2002 *Nature* **420** 762 Beveratos A et al 2002 *Phys. Rev. Lett.* **89** 187901
[8] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121 Marand C and Townsend P D 1995 *Opt. Lett.* **20** 1695
[9] Inoue K et al 2002 *Phys. Rev. Lett.* **89** 037902
[10] Inoue K et al 2003 *Phys. Rev.* A **68** 022317
[11] Wen K et al 2009 *Phys. Rev. Lett.* **103** 170503
[12] Chen X et al 2004 *Appl. Phys. Lett.* **85**, 1648
[13] Adachi et al 2009 *New J. Phys.* **11** 113033
Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133
Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[14] Balic V et al 2005 *Phys. Rev. Lett.* **94** 183601
Kolchin P et al 2006 *Phys. Rev. Lett.* **97** 113602
Liu X B et al 2008 *Chin. Phys. Lett.* **25** 3856
Liu W T et al 2006 *Chin. Phys. Lett.* **23** 287
[15] Thompson J K et al 2006 *Science* **313** 74
[16] van der Wal C H et al 2003 *Science* **301** 196
[17] Kuzmich A et al 2003 *Nature* **423** 731
[18] Du S W et al 2008 *Phys. Rev. Lett.* **100** 183603
[19] Du S et al 2009 *Phys. Rev.* A **79** 043811
Chen J F et al 2010 *Phys. Rev. Lett.* **104** 183604
[20] Klchin P et al 2008 *Phys. Rev. Lett.* **101** 103601
[21] Specht H P et al 2009 *Nature Photon.* **3** 469
[22] Mayers D 1996 *Advances in Cryptology: Proceedings of Crypto96, Lecture Notes in Computer Science* (Berlin: Springer-Verlag) vol 1109 p 343
Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[23] Zhou C et al 2003 *Appl. Phys. Lett.* **83** 1692
[24] Chen J F et al 2010 *Phys. Rev. Lett.* **104** 223602
[25] Chaneliere T et al 2006 *Phys. Rev. Lett.* **96** 093604