Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution

Jian-Yu Guan,[1,2] Zhu Cao,[3] Yang Liu,[1,2] Guo-Liang Shen-Tu,[1,2] Jason S. Pelc,[4] M. M. Fejer,[4] Cheng-Zhi Peng,[1,2] Xiongfeng Ma,[3,*] Qiang Zhang,[1,2,†] and Jian-Wei Pan[1,2]

[1]*Department of Modern Physics and National Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[4]*Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA*

(Received 14 January 2015; published 6 May 2015)

In quantum key distribution (QKD), the bit error rate is used to estimate the information leakage and hence determines the amount of privacy amplification—making the final key private by shortening the key. In general, there exists a threshold of the error rate for each scheme, above which no secure key can be generated. This threshold puts a restriction on the environment noises. For example, a widely used QKD protocol, the Bennett-Brassard protocol, cannot tolerate error rates beyond 25%. A new protocol, round-robin differential phase-shifted (RRDPS) QKD, essentially removes this restriction and can in principle tolerate more environment disturbance. Here, we propose and experimentally demonstrate a passive RRDPS QKD scheme. In particular, our 500 MHz passive RRDPS QKD system is able to generate a secure key over 50 km with a bit error rate as high as 29%. This scheme should find its applications in noisy environment conditions.

DOI: 10.1103/PhysRevLett.114.180502 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex

The uncertainty principle guarantees that whenever an eavesdropper, Eve, wants to learn key information in the quantum channel, she would inevitably introduce disturbances, which could be detected by the two authorized parties, Alice and Bob. In reality, the quantum channel may suffer from environment disturbance, which could cause errors and even more vitally conceal Eve's attack.

The amount of leaked key information, which is quantified by a phase error e_p, can be inferred from the channel disturbance, which is quantified by a bit error e_b. The final key rate is given by [1]

$$R \geq 1 - H(e_b) - H(e_p), \tag{1}$$

where $H(e) = -e \log e - (1-e) \log(1-e)$ is the binary Shannon entropy function. The bit error can be directly computed from the experimental data, whereas the phase error needs to be estimated or bounded. In the Bennett-Brassard (BB84) protocol with strong symmetries, one can show that $e_p = e_b$ in the long key length limit. In other protocols, normally there is a relation between the two error rates. In the end, when the error rate e_b goes beyond some threshold level, no secure key can be generated. For example, with the Shor-Preskill security proof [1,2], the BB84 protocol can maximally tolerate 11% error rate. For any security analysis, a simple intercept-and-resend attack [3] shows that the BB84 protocol cannot tolerate more than 25% error rate. This threshold puts a stringent requirement on the system environment, which makes some practical implementations challenging.

Recently, Sasaki, Yamamoto, and Koashi proposed a round-robin differential phase-shift (RRDPS) quantum key distribution (QKD) protocol [4]. The sender Alice encodes a random phase, chosen from $\{0, \pi\}$, on each of L pulses, with an average photon number of μ. Upon receiving the L-pulse block, the receiver Bob implements a single-photon interference with a Mach-Zehnder interferometer (MZI), as shown in Fig. 1(a). The key point is that Bob can randomly adjust the length difference of the two arms of the MZI. After obtaining a detection click, Bob first identifies which two pulses interfere and then announces the corresponding indices i, j to Alice. Alice can derive the relative phase between the two pulses as the raw key, and Bob can record the raw key from the measurement results. The phase error rate e_p depends only on the number of photons in the L-pulse signal and L, not the bit error rate e_b. By setting a large enough L, the phase error rate tends to 0, and hence the scheme can tolerate up to 50% bit error rate according to Eq. (1).

In the protocol, Bob needs to randomly adjust the length difference between the two arms of the MZI, from 1 to $L-1$ pulse periods. Based on the current technology, however, it is challenging to quickly change the length difference of the two arms in a MZI. The main adjust-delay method is to utilize optical switches, which cannot provide both high speed and low insertion loss simultaneously.

In this Letter, we propose an alternative scheme that passively chooses two pulses to interfere with the same bit error tolerability. When Bob receives a block from Alice, he

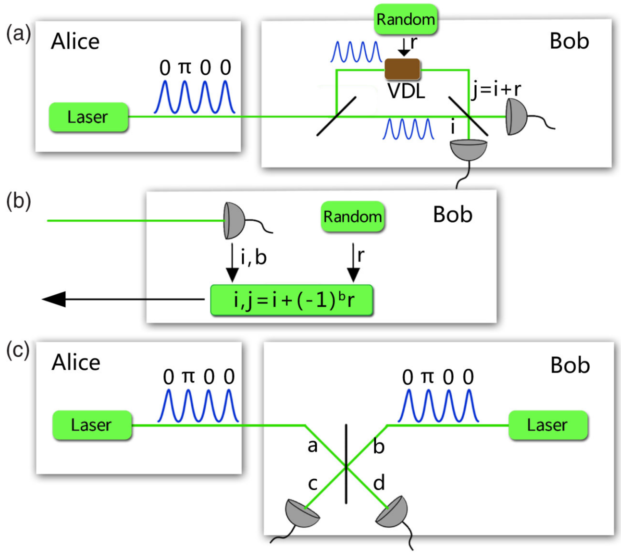

FIG. 1 (color online). (a) Original RRDPS scheme [4]. VDL stands for variable delay line. Bob splits the received signals into two paths and applies a variable delay r to one of the paths. (b) Equivalent model. Bob obtains a click at position i, generates two random numbers $r\in\{1,\ldots,L-1\}$ and $b\in\{0,1\}$ to obtain $j=i+(-1)^b r$, and publicly announces i and j to Alice. (c) Passive RRDPS scheme. Bob uses a local laser to generate an L-pulse reference, which interferes with Alice's L-pulse signal. Bob then records the coincidence clicks.

prepares a local L-pulse reference in plain phases; i.e., all phases are encoded at phase 0. This L-pulse reference interferes with the L-pulse signal sent by Alice on a beam splitter, as shown in Fig. 1(c). For each block, Bob records the status of his two detectors with time stamps i and j.

If Bob's reference is in phase with Alice's signal, the whole setup is essentially a huge MZI. Any detection signal at time slot i will tell the phase difference between i and the phase reference. Then the encoding bit value can be revealed to Bob. Here, Bob requires a phase reference from Alice, which may require complicated frequency comb technology [5].

The phase reference is not a necessary requirement for our scheme, though. If Bob's phase reference is random comparing to Alice's signal, the interference is no longer a Mach-Zehnder type but a Hong-Ou-Mandel type [6]. Let us consider a simple case when both Alice and Bob each has exactly one photon in their L-pulse trains. The states of Alice and Bob can be represented by

$$\frac{1}{\sqrt{L}}\sum_{i=1}^{L}(-1)^{s_i}a_i^\dagger|0\rangle, \qquad \frac{1}{\sqrt{L}}\sum_{i=1}^{L}b_i^\dagger|0\rangle, \tag{2}$$

respectively, where $s_i\in\{0,1\}$ designates the phase of Alice's ith pulse. Since there are two photons in a block, one from Alice and one from Bob, Bob would obtain at most two detection clicks. He postselects to choose the block where there are exactly two detections and announces their positions i and j (if $i=j$, the detection result is discarded). The raw key is the relative phase between these two pulses in the L-pulse signal. Alice can derive this phase difference from her record.

After the interference and Bob's postselection, the quantum state at the two detectors becomes one of

$$\begin{aligned}&[1-(-1)^{s_i+s_j}]d_i^\dagger c_j^\dagger|0\rangle, \qquad &&[1-(-1)^{s_i+s_j}]c_i^\dagger d_j^\dagger|0\rangle,\\ &[1+(-1)^{s_i+s_j}]c_i^\dagger c_j^\dagger|0\rangle, \qquad &&[1+(-1)^{s_i+s_j}]d_i^\dagger d_j^\dagger|0\rangle,\end{aligned} \tag{3}$$

where $c_i^\dagger$ and $d_i^\dagger$ are the creation operators at the two detectors, respectively, as shown in Fig. 1(c). This means if Alice's pulses i and j have the same phase, i.e., $s_i=s_j$, the two clicks should be triggered by the same detector, while if Alice's pulses i and j have different phases, the two clicks should be triggered by different detectors. Thus Bob, can derive the relative phase by comparing the measurement results of the ith and jth pulses.

For the security analysis, we show that in the single-photon case, our protocol is equivalent to an intermediate model shown in Fig. 1(b) [4], which is then equivalent to the RRDPS protocol. Thus, the phase error e_p is also bounded by $1/(L-1)$ as in RRDPS. Bob postselects the block where two clicks happen at i and j, but he cannot distinguish whether the photon causing the click belongs to the signal (Alice) or to the reference (Bob). Suppose Bob's photon is at i; the other case is similar. Since the L-pulse reference of Bob has a symmetry among all pulses, the $L-1$ possible positions of Bob's photon i (excluding the position of Alice's photon j) have the same weight. Bob has passively chosen a random shift $r=j-i$ between the clicks i and j, which is equivalent to the active shift in the raw model, as shown in Fig. 1(a). We give a strict proof of this equivalence in Supplemental Material [7], by showing that, for any single-photon input to Bob, the output, which is the distribution of the detection event (i,j), remains the same for both our protocol and the raw model.

In practice, a single-photon state source is often replaced by a weak laser pulse, which can be described by a coherent state. Alice generates a coherent-state pulse, randomizes its phase, and divides it into a series of weaker coherent-state pulses using, say, beam splitters. Alice can also generate the pulse train directly, say, by modulating a continuous-wave laser, with the same phase, which we call overall phase. This state preparation is the same for Bob. When the overall phase is randomized, it is shown that the state of the whole pulse train can be described by a statistical mixture of Fock states, whose photon number follows a Poisson distribution [8]. Similar to the single-photon case, Alice's key information is encoded into the relative phases between pulses.

In this coherent-state scenario, it is possible to have multiphoton components in both Alice and Bob's respective pulse trains, which will invariably alter Bob's postprocessing strategy. If Bob gets two or more detector clicks in a block, he randomly chooses two time stamps i and j of detector clicks and announces them. Otherwise, he discards the result. In this way, Bob can figure out the phase difference between i and j as in the single-photon protocol. By dividing into cases, one can bound e_p for the coherent-state protocol. Detailed analysis can be found in Supplemental Material [7].

Meanwhile, the multiphoton components may cause a large inherent bit error rate. Imagine the case where Alice sends nothing (or photons are lost in the channel) and Bob sends 2-photon state; it might result in a false conclusive detection event. The bit error rate in this case is clearly 50%. Since the probability of two single photons from each side (which does not have any inherent error) is the same as the probability of multiphoton from one arm and nothing from the other, the total inherent bit error rate will be 25%.

Our passive RRDPS scheme has three possible types of implementations: the single-photon case, the phase-locked weak coherent state, and the phase-randomized weak coherent sate. The third case is the most practical, which does not needs any fancy phase-locking technology, single-photon source, or high-speed optical switches. We then provide a proof-of-principle experiment demonstration for the third case.

The experiment setup is shown in Fig. 2. On Alice's side, a tunable extra cavity diode laser with a central wavelength of 1550.14 nm and a linewidth of 50 kHz is modulated into a pulse train with a repetition frequency 500 MHz. A beam splitter (BS) is used to separate the pulse train into two beams: one is for Alice's encoding, and the other one is sent to Bob as a reference. Alice encodes random $\{0, \pi\}$ phase into each individual pulse of the pulse train with a 10-GHz-fast modulator, driven by a pulse pattern generator. The pulse pattern generator's random signal is generated beforehand by a quantum random number generator. Before sending the pulse train to the channel, Alice attenuates the average photon number per pulse into 0.004. The signal light goes through the channel of a fiber spool to Bob.

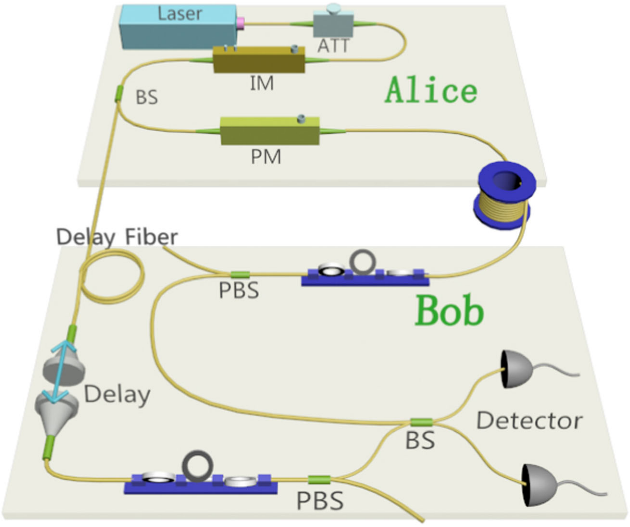

FIG. 2 (color online). Experiment setup. ATT, attenuator; IM, intensity modulator; BS, polarization maintaining beam splitter; PM, phase modulator; Delay, optical adjustable delay line; PC, polarization controller; PBS, polarization beam splitter (single mode to polarization maintaining). The attenuation on Bob's side is realized by a polarization controller and a polarization beam splitter.

On Bob's side, he first attenuates his reference pulse intensity into an average photon number $\mu = 0.004$ per pulse and then interferes with the signal pulse on a BS. Before the BS, a tunable fiber delay line and some fixed fiber delay are used to guarantee that the two pulse trains arrive at the BS simultaneously. Meanwhile, two polarization controllers and polarization beam splitters are used to make the two beams' polarizations identical.

The output ports of the BS are led to two up-conversion single-photon detectors. The up-conversion detector uses sum-frequency generation in a periodically poled lithium niobate with a 1.94 μm pump beam to convert the telecom-band photons to 860 nm, where they are detected by a silicon single-photon detector. This scheme benefits from the high detection efficiency and short dead time of the silicon detector, and the long-wave pump technology [9] as well as the volume Bragg gratings help to reduce the noise dramatically [10]. The detectors used in our experiment both have efficiencies larger than 14%, a dead time less than 80 ns, and a dark count of 500 Hz.

We utilize a time digital converter (TDC) to record the detection signal. The TDC has a timing resolution of 160 ps and is synchronized with the pulse pattern generator by sharing the same clock. The TDC will time tag and memorize all the events and sent to a PC for analysis.

The final key rate formula is similar to the BB84 protocol [1]:

$$K = N(1 - H_{PA} - H_{EC}), \tag{4}$$

where N stands for the length of the shifted key and $H_{EC} = fH(e_b)$ accounts for the cost of error correction. Here, denote e_b to be the bit error rate and f to be the error correction efficiency. For simplicity, we use $f = 1$ in the following postprocessing.

The privacy amplification cost is $H_{PA} = H(e_p)\times(1 + 1.98\sqrt{s/N})$, where e_p is the phase error rate and the second factor accounts for finite key effects. Here s comes from the security parameter 2^{-s}, a typical value of which is 100. To estimate the phase error rate, we set a proper photon number threshold v_{th}, which is a parameter to be optimized. For an L-pulse signal containing more than v_{th} photons, we assume these photons as tagged and the corresponding $e_p = 1/2$; that is, Eve can get all information about them. For a signal containing less than v_{th} photons, we can effectively bound the leaked information by estimating its phase error rate (see part II of Supplemental Material [7]). Let $e_{src}(v_{\mathrm{th}}) = \Pr(n > v_{\mathrm{th}})$

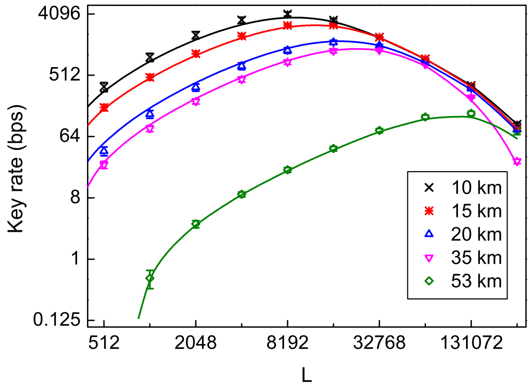

FIG. 3 (color online). The dependence of the key rate on the block size L at various distances. For each distance, we repeat the experiment 10 times and take the standard deviations in 10 trials as the error bar.

be the probability of this, where n is the photon number of the L-pulse signal. The phase error is calculated by

$$e_p = \frac{e_{src}}{Q} + \left(1 - \frac{e_{src}}{Q}\right)\frac{1 - (\frac{L-3}{L-1})^{v_{\rm th}}}{4} + \frac{\frac{m}{M}}{2(1-\frac{m}{M})}, \qquad (5)$$

where Q is the gain of the experiment given by N_{em}/N. Here N_{em} is the total number of blocks, N is the number of blocks after Bob's postselection, m is the total number of photon counts of one detector, and M is the total number of pulses.

The three additive terms in the phase error correspond to the probability of more than $v_{\rm th}$ photons, the probability of less than $v_{\rm th}$ photons, and the probability that two or more photons simultaneously enter the same detector at the same time stamp. Note that one factor 2 in the denominator of $[1-(L-3/L-1)^{v_{\rm th}}]/4$ is because the phase error rate is 0 when the two clicks that Bob announces are both from the signal or both from the reference, and this probability is at least as large as the probability that one such click comes from the signal and the other from the reference. By choosing a proper value of $v_{\rm th}$, one can minimize the cost of privacy amplification. The detailed discussion is referred to Supplemental Material [7].

The final key rate depends on the block length L. Given the laser intensity of every pulse and the transmission distance, there exists an optimal L for the key rate. On Alice's side, instead of setting a fixed L, we modulate the cw laser to form a continuous sequential pulse train, like the DPS QKD experiment [11,12]. During the postprocessing step, we can choose an optimal L by maximizing the final key rate, as shown in Fig. 3.

The experimental parameters with the optimal L are listed in Table I.

The above analysis does not consider the dead time. We discount its effect by postselecting: Immediately after one detector click, we effectively disable the other detector within one dead time period by postselecting out this period. The exact treatment is referred to Supplemental Material [7].

TABLE I. List of optimal L, $v_{\rm th}$, e_b, and e_{ph} for various distances.

d (km)	μ	Optimal L	$v_{\rm th}$	e_b	e_{ph}
10	0.004	8192	57	0.275	0.003 59
15	0.004	16 384	99	0.271	0.003 11
20	0.004	16 384	100	0.283	0.003 12
35	0.004	32 768	179	0.276	0.002 78
53	0.004	131 072	625	0.312	0.002 40

In summary, we demonstrate a passive scheme to substitute the original RRDPS protocol, and our system can distill a secure key with a bit error rate of 28% in the lab. With our scheme, one can easily achieve a large number L (say, $L = 2^{14}$) of pulse trains in the experiment. In the original scheme, the pulse train length L needs to be optimized before the experiment, which requires a precise calibration of the system. In our scheme, on the other hand, the parameter L can be decided during postprocessing step, which has an advantage in the case with large environment fluctuations.

The inherent error can be removed by a postselecting technique [13] combined with the recently developed discrete-phase-randomization scheme for the coherent states [14]. In principle, with certain modifications, such a technique can be used in our scheme. This is an interesting prospective research project. Meanwhile, the inherent error can be removed by using a phase-locked coherent state. Note that if Alice sends a strong laser pulse to Bob as reference and Bob directly uses it as for interference, Eve may implement a man-in-the-middle attack. One solution to remove this potential threat is to utilize frequency-comb-based frequency distribution technology [15].

In the future, a field test of the passive RRDPS scheme with two independent lasers can be realized by the technology developed in a recent QKD experiment [16]. With low-jitter and high-efficiency single-photon detectors [17], a much higher secure key rate with a 10 GHz clock rate system [11] can be achieved.

The authors thank Yan-Lin Tang, Xiao Yuan, and Zhen Zhang for enlightening discussions. This research has been supported by the National Basic Research Program (under Grants No. 2011CB921300, No. 2013CB336800, and No. 2011CBA00300), the National Natural Science Foundation of China, the Chinese Academy of Science, and the Shandong Institute of Quantum Science and Technology Co., Limited.

[*] xma@tsinghua.edu.cn
[†] qiangzh@ustc.edu.cn

[1] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[4] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).

[5] R. K. Shelton, L.-S. Ma, H. C. Kapteyn, M. M. Murnane, J. L. Hall, and J. Ye, Science **293**, 1286 (2001).

[6] C. Hong, Z. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

[7] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.114.180502 for the details of the safety proof and postprocessing issues.

[8] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[9] J. S. Pelc, L. Ma, C. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, and M. Fejer, Opt. Express **19**, 21445 (2011).

[10] G.-L. Shentu, J. S. Pelc, X.-D. Wang, Q.-C. Sun, M.-Y. Zheng, M. M. Fejer, Q. Zhang, and J.-W. Pan, Opt. Express **21**, 13986 (2013).

[11] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).

[12] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).

[13] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[14] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, arXiv:1410.3217v1.

[15] K. Predehl *et al.*, Science **336**, 441 (2012).

[16] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, IEEE J. Sel. Top. Quantum Electron. **21**, 6600407 (2015).

[17] F. Marsili *et al.*, Nat. Photonics **7**, 210 (2013).