Practical round-robin differential-phase-shift quantum key distribution

2017 New J. Phys. 19 033013

(http://iopscience.iop.org/1367-2630/19/3/033013)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
2 November 2016

REVISED
7 February 2017

ACCEPTED FOR PUBLICATION
23 February 2017

PUBLISHED
9 March 2017

PAPER

Practical round-robin differential-phase-shift quantum key distribution

Zhen Zhang, Xiao Yuan, Zhu Cao and Xiongfeng Ma[1]

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, People's Republic of China

[1] Author to whom any correspondence should be addressed.

E-mail: xma@tsinghua.edu.cn

Keywords: quantum key distribution, decoy state, privacy amplification

Abstract

The security of quantum key distribution (QKD) relies on the Heisenberg uncertainty principle, with which legitimate users are able to estimate information leakage by monitoring the disturbance of the transmitted quantum signals. Normally, the disturbance is reflected as bit flip errors in the sifted key; thus, privacy amplification, which removes any leaked information from the key, generally depends on the bit error rate. Recently, a round-robin differential-phase-shift QKD protocol for which privacy amplification does not rely on the bit error rate (Sasaki *et al* 2014 *Nature* **509** 475) was proposed. The amount of leaked information can be bounded by the sender during the state-preparation stage and hence, is independent of the behavior of the unreliable quantum channel. In our work, we apply the tagging technique to the protocol and present a tight bound on the key rate and employ a decoy-state method. The effects of background noise and misalignment are taken into account under practical conditions. Our simulation results show that the protocol can tolerate channel error rates close to 50% within a typical experiment setting. That is, there is a negligible restriction on the error rate in practice.

1. Introduction

Quantum cryptography enables secure information exchange between two remote parties, guaranteed by quantum physics. In particular, quantum key distribution (QKD) [1, 2] offers a means of distributing keys with security that is information-theoretically provable based on the fundamental laws of quantum physics [3–6]. In a typical QKD protocol, a sender, Alice, transmits quantum signals through an untrusted channel to a receiver, Bob, who performs measurements and accumulates raw key data. Alice and Bob aim to share secure identical keys such that an adversary, Eve, cannot obtain information about the keys (up to a small failure probability).

Due to experimental imperfections or eavesdropping, some of the shared sifted keys of Alice and Bob are not identical. Such differences are caused by events known as bit-flip errors. Alice and Bob can run an error correction procedure to make the keys identical. Besides this, owing to eavesdropping, parts of the shared keys may not be secure. The amount of information of the shared keys that is leaked to Eve can be quantified by phase-flip errors [4, 5]. The Heisenberg uncertainty principle tells us that any attempts to eavesdrop on the quantum channel would inevitably cause disturbance in the quantum signals. Alice and Bob can thus quantify, or at least obtain an upper bound on, the phase error rate by monitoring the disturbance, and remove it by performing privacy amplification. Finally, the ratio of the distributed secure key per sifted key bit is given by [5],

$$R = 1 - H(e_{\mathrm{bit}}) - H(e_{\mathrm{ph}}), \tag{1.1}$$

where e_{bit} and e_{ph} are the bit and phase error rates, respectively, and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

In conventional QKD protocols, there exists a fundamental limitation on the error rate. Intuitively, the more disturbance that the adversary introduces (say, indicated by a higher bit error rate), the more information she can obtain. For example, in the BB84 protocol [1], due to its symmetries, the phase error rate can be estimated by

the bit error rate $e_{\rm ph} = e_{\rm bit}$ [5]. In the extreme case, where the bit flip error $e_{\rm bit} \geqslant 11\%$, the final key rate, $R = 1 - 2H(e_{\rm bit})$, drops to 0 according to equation (1.1), which means that no secure key can be achieved. Therefore, the above post-processing procedure works only for the case where the bit error rate is not larger than 11%. Higher error rate thresholds can be obtained by other postprocessing techniques [7], but upper bounds are generally believed to exist [8].

Surprisingly, this is not the case for all QKD protocols. In a recently proposed seminal QKD protocol known as the round-robin differential-phase-shift (RRDPS) [9], the phase error rate can be estimated with a different approach that does not depend on the bit error rate. Instead, the information Eve can acquire is directly bounded by the quantum source, regardless of how she interferes with the quantum signals. In this protocol, Alice encodes her information into the phase of a quantum signal that is in a superposition of L optical modes (say, L sequential pulses). Then, she sends the signal through a (unsafe) quantum channel to Bob, who randomly picks two of the L modes and measures the phase difference between them to gain raw key data. Owing to the randomness of the measurement choices and the coherence of the signal, Eve can only acquire very limited information about the key. As the number of optical modes L increases, the information that Eve can obtain by eavesdropping decreases [9]. With a sufficiently long quantum signal (large L), the phase error rate can be reduced down to 0 and a secure key can be generated even if the bit error rate $e_{\rm bit}$ is close to 50%. Recently, many proof-of-principle experimental demonstrations of the RRDPS protocols have been presented [10–13]. There are also several theoretical follow-ups that considered source flaws in the RRDPS protocol [14] and its extensions to other QKD scenarios [15, 16].

In practical QKD systems, weak coherent pulses are often used as photon sources. In conventional QKD protocols, such as BB84, the multi-photon component from a coherent state cannot lead to any secure keys as it is vulnerable against the photon number-splitting attack [17]. In the RRDPS protocol, when Alice splits the coherent state pulse into L pulses, Bob can generate a secure key even with multi-photon components. For an n-photon input state, the phase error rate can be upper-bounded by $e_{\rm ph}^n \leqslant n/(L-1)$ [9]. With a sufficiently large L, the n-photon state can still positively contribute to the final key rate, according to equation (1.1).

When the phase is randomized, a weak coherent state can be treated as a statistical mixture of Fock states, where the photon number follows a Poisson distribution. In the original security analysis [9], the phase error rate for a coherent state source is estimated by upper-bounding the photon number (up to a small failure probability). In this study, we apply the tagging technique, developed by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [18], to assess the phase error rates for different photon number states separately. As a result, we derive a tighter secure key rate bound by reducing the cost in privacy amplification. In addition, we adopt the decoy-state method [19–21], which is widely used in regular QKD systems.

Furthermore, we build a simulation model to analyze the performance of the RRDPS protocol under a practical scenario. We show that, in a practical setting, the maximum transmission distance cannot infinitely increase, even if the phase error rate, $e_{\rm ph}$, drops to zero via the increase of the number of optical mode L. Intuitively, this is due to the fact that the background rate, which is assumed to be a linear function of L, limits the maximum transmission distance. By simulation, we compare three security analysis methods: the one proposed by Sasaki, Yamamoto, and Koashi (SYK) [9], and our new analysis with and without decoy states. The results show the performance improvement by our new analysis methods.

2. Review of the RRDPS protocol

The RRDPS protocol is presented in figure 1. Let us first consider the case wherein Alice uses a single-photon state source. Then the state $|\Psi\rangle_{\mathbf{s}}$ that she prepares is in a superposition of L optical modes,

$$|\Psi_1\rangle_{\mathbf{s}} = \frac{1}{\sqrt{L}} \sum_{k=0}^{L-1} (-1)^{s_k} |k\rangle, \tag{2.1}$$

where $s_k \in \{0, 1\}$ is Alice's encoded key information and $|k\rangle$ denotes the state of the photon appearing in the k-th mode. Alice's L-bit key information, $\mathbf{s} \in \{0, 1\}^L$, is encoded in the phase of each mode, 0 or π. In this study, we use temporal modes as an example of optical modes and hence equation (2.1) forms an L-pulse sequence. In principle, Alice can use optical modes separated by other degrees of freedom, such as spectrum or angular momenta, where our results should be directly applied.

For general states, such as multi-photon states with extra dimensions, Alice can also encode the key information as follows. First, Alice prepares an L-pulse state $|\Psi\rangle$ and L ancillary qubits each in $(|0\rangle + |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Z-basis. Then, she applies the L control operations $U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes (-1)^{\hat{n}}$ on each of the ancillaries as control and the L-pulse state $|\Psi\rangle$ as the target, where $\hat{n}$ is the photon number operator. When the control qubit is $|1\rangle$, all photons in the target light are shifted by a phase π. With this, Alice finally prepares the entangled state

1. Alice prepares a state in the (equal-amplitude) superposition of L (optical) modes and randomly generates a random L-bit sequence, $\mathbf{s} = (s_0, s_1, \ldots, s_{L-1})$.
2. She applies phase modulation, $\{0, \pi\}$, to each optical mode according to $\mathbf{s}$ and obtains the state $|\Psi\rangle_{\mathbf{s}}$. She sends the state to Bob.
3. Bob splits the received signal with a 50/50 beam splitter to obtain two L-pulse trains, generates a random number $r \in \{-L+1, \ldots, -2, -1, 1, 2, \ldots, L-1\}$, and shifts one of the L-pulse trains forward ($r > 0$) or backward ($r < 0$) by r pulses.
4. Bob measures the interference between two L-pulse trains. If he obtains a detection on position i in the unshifted pulse train, corresponding to position j in the shifted pulse train, and $0 \leq j = i+r \leq L-1$, Bob records a raw key bit according to the relative phase $s_B = s_i \oplus s_j$. Otherwise, Bob regards the transmission as a failure.
5. Bob announces $\{i, j\}$ so that Alice can obtain the sifted key, $s_A = s_i \oplus s_j$.

Figure 1. RRDPS protocol [9].

$$
\begin{aligned}
|\Psi\rangle_{\text{Alice}} &= 2^{-L/2} \prod_{k=0}^{L-1} (|0\rangle_k + (-1)^{\hat{n}_k} |1\rangle_k) |\Psi\rangle \\
&= 2^{-L/2} \prod_{k=0}^{L-1} \left(\sum_{s_k \in \{0,1\}} |s_k\rangle_k (-1)^{s_k \hat{n}_k} \right) |\Psi\rangle \\
&= 2^{-L/2} \sum_{\mathbf{s} \in \{0,1\}^L} \left(\prod_{k=0}^{L-1} |s_k\rangle_k (-1)^{s_k \hat{n}_k} \right) |\Psi\rangle,
\end{aligned} \tag{2.2}
$$

where $|s_k\rangle_k$ is the kth ancillary qubit and $\hat{n}_k$ is the photon number operator acting only on the kth pulse. After performing projection measurements on the ancillary qubits in the Z-basis, a specific measurement outcome, $\mathbf{s} = (s_0, s_1, \ldots s_{L-1})$, corresponds to the final output of

$$
|\Psi\rangle_{\mathbf{s}} = \left(\prod_{k=0}^{L-1} (-1)^{s_k \hat{n}_k} \right) |\Psi\rangle. \tag{2.3}
$$

For instance, the state in equation (2.1) corresponds to the case when $|\Psi\rangle$ is a single photon state. The measurement outcomes of the L ancillary qubits in the $\{|0\rangle, |1\rangle\}$ basis can be regarded as random numbers used to construct L bits $\mathbf{s}$ in (figure 1).

We suppose Alice measures the ancillary qubits after Bob announces (i, j). To obtain $s_i \oplus s_j$, Alice performs a controlled-NOT gate (C-NOT) on the ith and jth ancillary qubits and measures the target in the Z basis. To define the phase error of the target qubit, we can measure it in the X basis. If the qubit is $|+\rangle$, no information is leaked to Eve. The phase error probability is denoted as the probability that the result is $|-\rangle$, which quantifies the leaked information of $s_i \oplus s_j$.

3. Phase error estimation

The schematic for the RRDPS presented in figure 1 is shown in figure 2(a). To estimate how much sifted key information is leaked to Eve, one can consider an equivalent scenario, which is only applied in the security analysis, as shown in figure 2(b). In scenario **b**, Bob first generates a random number $r \in \{-L+1, \cdots, -1, 1, \cdots, L-1\}$. Then, he measures the photon of the received signal and obtains a detection in the ith pulse. Bob calculates $j = i + r \,(\text{mod } L)$ with i and r, and announces the values of i and j. We consider Bob to be a black box with a quantum input and a classical output (i, j) where Eve's interference of the

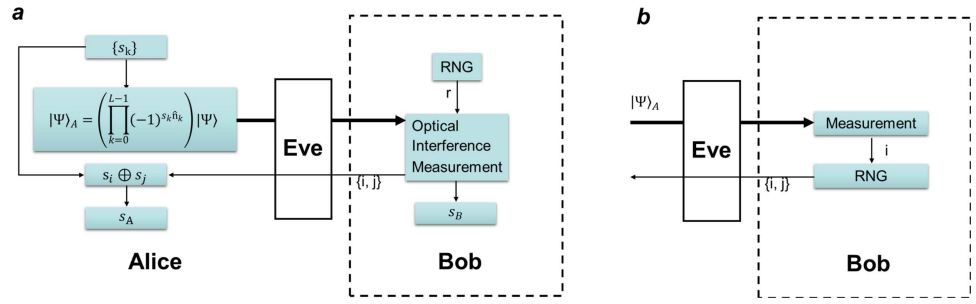

Figure 2. Two scenarios for the RRDPS protocol that are equivalent from Eve's viewpoint. (a) The key distribution procedures are described in figure 1. Bob receives a quantum state and announces (i, j). (b) Bob measures the location of the photon in the received signal to obtain i, and defines $j = i + r$ with randomly generated number $r \in \{-L+1, \cdots, -1, 1, \cdots, L-1\}$.

quantum signal is considered. Since the input and output for the black boxes are identical under both scenarios, one can use scenario figure 2(b) to estimate the phase error rate in scenario figure 2(a).

In scenario **b**, we imagine that Alice performs her measurement after Bob announces his outputs. To get the key bit $s_A = s_i \oplus s_j$, Alice simply applies a C-NOT to the ith and jth ancillary qubits, with the ith qubit as the control and the jth qubit as the target. After that, she measures the j-th qubit in the Z-basis and obtains a sifted key bit, s_A. To estimate the phase error rate, e_{ph}, one can simply measure the jth qubit in the X-basis. If the jth qubit is an eigenstate of the X-basis, the measurement outcome on the Z-basis is fully random that is, no information is leaked to Eve [6]. Hence, the phase error probability of measuring the jth qubit is defined by the probability of finding it in the state $|-\rangle$. As the C-NOT operation will not affect the X-eigenvalues of the jth qubit, which are randomly chosen uniformly from all qubits except the ith one by Bob, the phase error rate can be estimated by the probability of finding any except the ith qubit in the $|-\rangle$ state. Notice that, in equation (2.2), the probability of obtaining $+$ or $-$ is entirely determined by the number of photons contained in the jth pulse. The case of an odd (even) number of photons corresponds to outcome of $|-\rangle$ (resp.$|+\rangle$). Therefore, according to equation (2.3), the phase error rate can be estimated by the probability of finding an odd number of photons in a pulse.

According to equation (2.3), the phase error rate can be upper-bounded by the probability of finding an odd number of photons appearing in a pulse. In the case where $|\Psi\rangle$ is an n-photon state, the maximum possible number of pulses wherein odd numbers of photons appear is n. In the SYK analysis [9], the phase error rate is bounded by

$$e_{\mathrm{ph}}^{n} \leqslant \frac{n}{L-1}. \tag{3.1}$$

4. GLLP analysis

In practice, a phase-randomized weak coherent state photon source is widely used in QKD systems. In the RRDPS protocol, Alice prepares a phase-randomized coherent state pulse with intensity $L\mu$. According to the photon number channel model [20], the state can be regarded as a statistical mixture of n-photon states,

$$\rho = \sum_{n=0}^{\infty} e^{-L\mu} \frac{(L\mu)^n}{n!} |n\rangle\langle n|. \tag{4.1}$$

Then, following the procedures presented in figure 1, this strong pulse is split into L identical small pulses through beam splitters and becomes the initial state $|\Psi\rangle$, which is encoded with key information according to equation (2.3). Note that the intensity of each small pulse, μ, is weak, but $L\mu$ can be large.

For each n-photon term in equation (4.1), the phase error rates can be estimated by equation (3.1). Denote the ratio of the key that needs to be sacrificed for privacy amplification by H_{PA}; by extending the GLLP security analysis [18], the amount of key loss in privacy amplification is given by

$$Q_{L\mu} H_{\mathrm{PA}} = e^{-L\mu} \sum_{n=0}^{\infty} Y_n \frac{(L\mu)^n}{n!} H(e_{\mathrm{ph}}^{n}), \tag{4.2}$$

where $Q_{L\mu} = e^{-L\mu}\sum_{n=0}^{\infty} Y_n (L\mu)^n/n!$ is the overall gain and Y_n denotes the yield of the n-photon state.

Then, the final key rate, similar to equation (1.1), can be rewritten as

$$L \cdot R = Q_{L\mu}[1 - H(e_{\mathrm{bit}}) - H_{\mathrm{PA}}], \tag{4.3}$$

Table 1. Parameters from a typical QKD system [23]. Here, η_d is the detection efficiency, α is the channel loss, e_d is the misalignment error rate, and y_0 is the background rate for each pulse. As there are L pulses, the total background rate should thus be $Y_0 = 1 - (1 - y_0)^L \approx Ly_0$. We discuss the case where the total background rate is independent of L in the discussion section.

Experiment	η_d	e_d	y_0	α
GYS [23]	4.5%	3.3%	1.7×10^{-6}	0.2 dB km^{-1}

where $L \cdot R$ is the final key bit per L-pulse train. Since these trains contain L pulses, the final key rate, R, should be normalized by L. In experiment, the overall gain $Q_{L\mu}$ is an observable, while Y_n is generally an unknown parameter that can be manipulated by Eve. In the following, we show three different approaches to the estimation of H_{PA}.

Let us start with the original SYK analysis [9], where the phase error rate is estimated by equation (3.1). One can set a threshold photon number n_{th}, over which the phase error rate is bounded by 1/2. Since the phase error rate e_{ph}^n increases with the photon number n, one can consider the worst case scenario to be the case where the losses are all contributed from low photon numbers. That is, $Y_n = 1$ for $n > n_{th}$. Also, for all the states with photon numbers less than n_{th}, one has $e_{ph}^n \leqslant e_{ph}^{n_{th}}$. Thus, H_{PA} in equation (4.2) can be upper bounded by

$$Q_{L\mu}H_{PA} \leqslant \left(Q_{L\mu} - \sum_{n>n_{th}} \frac{(L\mu)^n}{n!}e^{-L\mu}\right)H(e_{ph}^{n_{th}}) + \sum_{n>n_{th}} \frac{(L\mu)^n}{n!}e^{-L\mu}H\left(\frac{1}{2}\right), \tag{4.4}$$

where $e_{ph}^{n_{th}}$ is bounded by equation (3.1). In addition, one can optimize over the choice of n_{th} to minimize H_{PA} and hence maximize the final key rate R.

With the tagging technique developed in the GLLP security analysis, we can estimate each privacy-amplification term in equation (4.2) separately. According to equation (3.1), the phase error rate increases with the photon number n. In the worst case scenario, we assume all the losses come from the low-photon number states (with $n < n_{th}$), whereas all of the high-photon number states (with $n > n_{th}$) pass through the channel transparently. Then, H_{PA} in equation (4.3) can be upper-bounded by

$$Q_{L\mu}H_{PA} \leqslant \left(Q_{L\mu} - \sum_{n>n_{th}} \frac{(L\mu)^n}{n!}e^{-L\mu}\right)H(e_{ph}^{n_{th}}) + \sum_{n>n_{th}} \frac{(L\mu)^n}{n!}e^{-L\mu}H(e_{ph}^{n}), \tag{4.5}$$

where $e_{ph}^{n_{th}}$ and e_{ph}^n are bounded by equation (3.1). Here, the threshold photon number, n_{th}, is the critical photon number such that the total, gain $Q_{L\mu}$, can be obtained by contributions from the terms with $n \geqslant n_{th}$. In general, the value of n_{th} calculated in equation (4.5) is different from the optimal n_{th} from the SYK analysis, equation (4.4).

Although the yields Y_n in equation (4.2) cannot be directly measured by experiments, we can use the decoy-state method, by which all the values of Y_n can be accurately estimated with an infinite number of decoy states [20]. In the simulation, we simply use the case where Eve does not interfere with the yields,

$$Y_n = 1 - (1 - Y_0)(1 - \eta)^n, \tag{4.6}$$

where η is the channel transmittance and Y_0 is the background count rate. That is, Y_0 denotes the count rate when Alice sends nothing ($n = 0$).

5. Simulation model and result

With the key rate formula for the RRDPS protocol given in equation (4.3), we can compare the performances of the three different methods of estimating H_{PA} namely, equations (4.4)–(4.6), by means of modeling a practical system [22]. The simulation model is presented in appendix D, and the QKD experimental parameters are listed in table 1. In the simulation, we need to consider all the device imperfections such as misalignment, environmental noise and dark counts.

The performances of the RRDPS protocol with different analytical methods: SYK analysis, new analysis (no-decoy) and new analysis (decoy) are shown in figure 3. Here, we fix L at 32 and optimize μ to obtain the maximum transmission distance. As one can see from figure 3, the improved analysis method enhances the performance, both in terms of the key rate and the maximum transmission distance. The simulation result indicates that the decoy-state method is useful for the RRDPS protocol.

In the conventional BB84 protocol, the decoy state is also utilized to increase the secure key generation rate and the transmission distance. Interestingly, the maximal secure distance of the asymptotic limit of the decoy state BB84 protocol (with infinite decoy states) is also around 140 km [20], with the same set of experimental

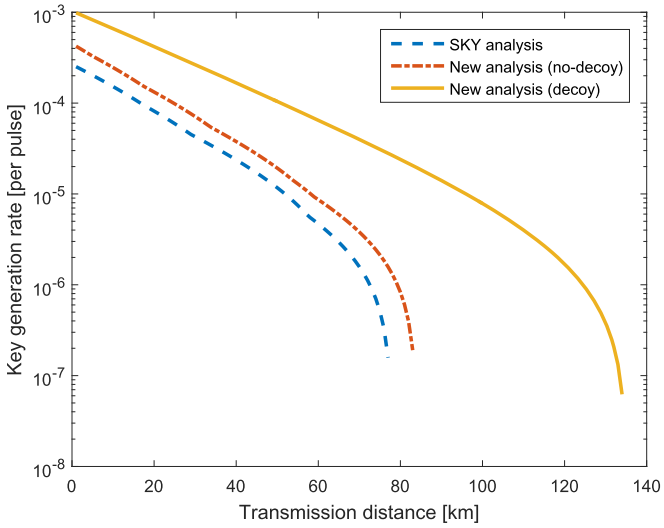

Figure 3. Final key rate for $L = 32$ using a practical QKD model, with parameters listed in table 1.

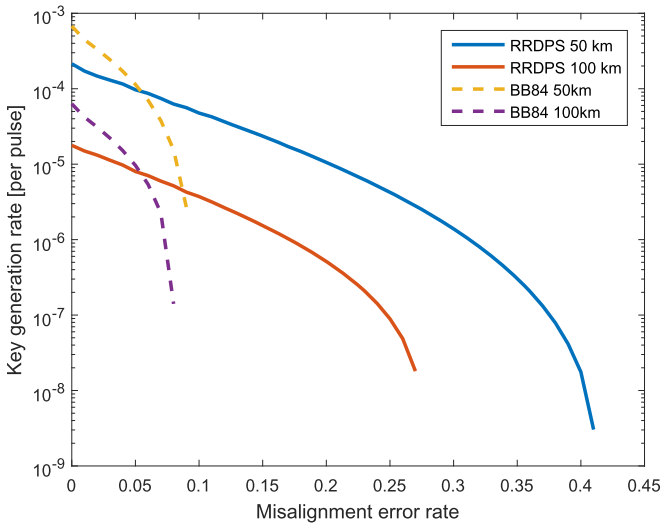

Figure 4. The optimized final key rate via the misalignment error rate.

parameters. In the simulation, we compare the BB84 and RRDPS protocols. The result shows that the RRDPS protocol tolerates the misalignment error better (see figure 4). Here, we compare the two protocols under two typical cases, for which transmission distances are, 50 km and 100 km, respectively. As shown in figure 4, the final key rates of the RRDPS protocol are higher than those in the BB84 protocol when the misalignment error rate are greater than 7%. In the 50 km case, the RRDPS protocol can tolerate a misalignment error rate of more than 40%; in the 100 km case, secure key can be generated even if the misalignment error rate is equal to 25% which is a hard upper bound of the BB84 protocol because of the intercept-and-resend attack [1, 8].

We next briefly compare the RRDPS protocol with the measurement-device-independent QKD (MDIQKD) [24, 25] protocol. The MDIQKD protocol has been demonstrated over 200 km [26–29] and in field test [30]. While the MDIQKD protocol enjoys the advantage of being secure against any detection loopholes, the RRDPS protocol is able to tolerate higher error rate. In the short distances, similar to the BB84 protocol, the RRDPS protocol should yield a higher key rate than the MDIQKD protocol. We expect two protocols should find suitable applications in different practical scenarios.

6. Discussion

In the original security analysis [9], the signal going to Bob's detection box is assumed to be single photon states. Also, the detectors used by Bob are assumed to be single-photon detectors (or photon number resolving detectors). In practice, these requirements are challenging with current technology. Instead, normally coherent state sources and threshold detectors are used. Thus, there is a gap between the security analysis and the implementation. A similar problem also exists for other QKD schemes [31]. The solution there is to apply the squashing model [32–34] to Bob's measurement. As a result, the signal Bob receives can be regarded as a qubit state in the security analysis. However, the squashing model cannot be directly applied here, since the single-photon state received by Bob is a qudit with a dimension of 2^L. Thus, it is an interesting future project to work a squashing model for the general qudit case.

The upper bound of the phase error with n-photons given in equation (3.1) is only a rough estimation. An interesting future work is to find a tighter upper bound of the phase error rate and combine it with the GLLP tagging idea and the decoy-state method. In appendix B, we discuss an ideal case where the input n-photons are considered to be independent. We show that the phase error estimation can be improved such that it becomes $1/2$ only in the limit of infinite photon numbers while the original phase error becomes $1/2$ when $n \geqslant L/2 + 1$. Although such an ideal scenario may become vulnerable in practice, the result may still shed light on a better upper bound to the phase error rate with multi-photons.

In practice, the parameter L may not be chosen freely. When L increases, the (relative) phase maintenance may becomes challenging. That is, it is reasonable to assume that the misalignment parameter grows with increasing L. Supposing that we ignore this practical issue for the moment and optimize the parameter L, our simulation result shows that with a large L (optimal value around 10^4 for the two no-decoy cases), three curves in figure 3 can reach a maximal secure distance of 140 km. In the decoy state case, the result is very stable under different values of L. In fact, with $L = 32$, the performance is already very close to the optimal L case. From this perspective, the decoy-state method makes the RRDPS protocol easier to implement in practice. Note that a practical decoy-state method based on our result is recently published [35].

In the simulation, we assume that the total background count rate (Ly_0) in an L-pulse block would linearly increase with L. One can also consider a scenario where the background noise, Y_0, has a fixed value, independent of L. Under this assumption, as shown in appendix C, we prove that the maximum transmission distance can infinitely increase, and that the optimal value of L linearly increases with the inverse of the channel transmittance, $L \propto 1/\eta$. This is not surprising, since the phase error rate approaches 0 as L increases, which allows the bit error rate (if it is independent of L) to grow arbitrarily close to $1/2$.

Furthermore, we show in appendix D that the RRDPS protocol can tolerate the misalignment error, e_{d}, up to 50%. Intuitively, this can be explained by the fact that the misalignment error (e_{d}) is independent of L, and it is similar to the case where the background noise, Y_0, is independent of L. Thus, we conjecture that the RRDPS is able to tolerate errors that are independent of L.

In this study, we make use a phase-randomized coherent state as input. In experiments, the continually phase-randomization requires the phase uniformly distributed from 0 to 2π, which is generally hard to implement. Instead, the discrete phase-randomization can be applied to approximate exact phase-randomization [36]. We leave such an extension to future research.

Acknowledgments

We thank Q Zhao and J Ma for helpful discussions. This study was supported by the National Natural Science Foundation of China Grants No. 11674193.

Appendix A. Simulation model

Here, we adopt a widely used simulation model for QKD [22]. Use $L\mu$ to denote the intensity of the source; η to be the overall transmittance; Y_n and e_n to be the yield (the probability of obtaining a successful detection) and the error rate, respectively, with n denoting the number of photons Alice sends. Without Eve's interference, Y_n and e_n are given by [22]

$$\begin{aligned} Y_n &= 1 - (1 - Y_0)(1 - \eta)^n, \\ e_n Y_n &= e_0 Y_0 + e_d (1 - Y_0)[1 - (1 - \eta)^n], \end{aligned} \tag{A.1}$$

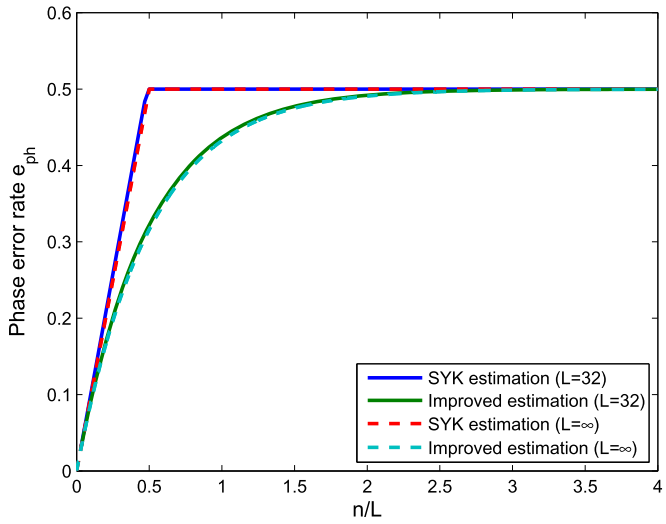

Figure B1. Comparison between two different estimates of e_{ph}^{n} with $L = 32$ and $L = \infty$, in the case where Eve does not change the photon-number statistics. The SYK analysis method is given in equation (3.1). The improved method is given in equation (B.1).

where the value of e_0 is equal to 0.5. Then the overall gain and QBER are given by

$$Q_{L\mu} = \sum Y_n \frac{(L\mu)^n}{n!} e^{-L\mu} = Y_0 + (1 - Y_0)(1 - e^{-\eta L\mu}),$$
$$E_{L\mu} Q_{L\mu} = \sum e_n Y_n \frac{(L\mu)^n}{n!} e^{-L\mu} = e_0 Y_0 + e_d (1 - Y_0)(1 - e^{-\eta L\mu}). \quad \text{(A.2)}$$

In simulation, we consider two different scenarios, an idealized one and a practical one. In the idealized case, we consider that the background noise, $Y_0 = y_0$, is independent of L. In the practical condition, Bob is required to obtain L detections and the background noise, Y_0, becomes $1 - (1 - y_0)^L$.

We show in appendix C that the maximal transmission distances of the RRDPS protocol behave differently under each of these two scenarios. In the idealized case, we show that the maximal transmission distance of the RRDPS protocol can be infinite. In the practical case, we show that there exists a limit on the transmission distance (loss).

Appendix B. Potential improvement for phase error rate estimation

In this section, we consider phase error estimation with an n-photon state as a comparison to the estimation given in equation (3.1). Here, we consider an ideal scenario that the n photons are independent. Note that the n photons are indeed independent when Alice prepares the state. Thus, the ideal scenario considered here only assumes that the quantum channel preserves this independency, for example, the beam splitting channel model.

In such a case, we can consider that each photon independently appears in each pulse with an equal probability of $p = 1/L$. One can imagine that Alice first prepares an n-photon state and allows it to pass through many beam splitters to form an L-pulse sequence. We refer to [11, 37] for the details of experimental implementations. When considering the case where Eve's operation in the quantum channel does not change the photon-number statistics, the phase error rate estimation can be improved over the original one [9],

$$e_{\mathrm{ph}}^{n} = \sum_{k \in \mathrm{odd}} \binom{n}{k} p^k (1 - p)^{n-k} = \frac{1 - (1 - 2p)^n}{2}. \quad \text{(B.1)}$$

The key point here is that in the RRDPS protocol, the phase error rate of each pulse is determined by the preparation of quantum state, but not by Eve's interaction. Thus, Alice and Bob do not need to accept the worst case scenario; instead, they can accurately derive the phase error rate in the state-preparation stage. This is the essential reason why the phase error rate in the RRDPS protocol is independent of the bit error rate.

Before we apply the new phase error estimation method to the QKD scheme, let us first compare the SYK result in equation (3.1) with the new one in equation (B.1) in figure B1. One can see that the improved method does give a tighter bound on the phase error rate, e_{ph}^{n}, for an n-photon state source. We expect that the key rate will be improved by employing the improved scheme, and this is confirmed in later simulations.

As shown in figure B1, when the total photon number n of the L-pulse quantum signal increases beyond the value of L, the phase error rate, e_{ph}^{n}, exponentially approaches to $1/2$ quickly, that is,

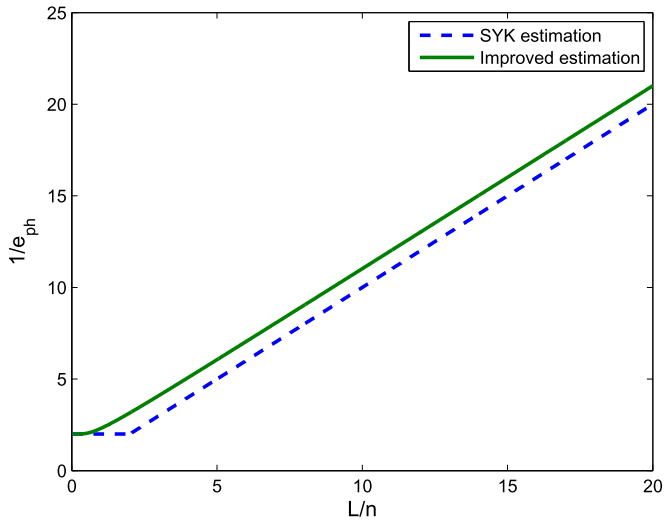

Figure B2. Comparison of two different estimates of $1/e_{\mathrm{ph}}^{n}$ as a function L/n. The SYK analysis method is given in equation (3.1); the new method is given in equation (B.1). When the SYK analysis method is applied, the optimized value of the mean photon number is around 0.05. In this case, the value of L/n is around 20.

$$e_{\mathrm{ph}}^{n} \approx \frac{1}{2} - e^{-2n/L}, \tag{B.2}$$

where the ratio n/L can be interpreted as the mean photon number of each pulse. On the other hand, when n is much smaller than L, e_{ph}^{n} can be approximated as

$$\begin{aligned}\frac{1}{e_{\mathrm{ph}}^{n}} &= \frac{2}{1-\left(1-\frac{2}{L}\right)^{n}} \\ &\approx \frac{2}{1-\left(1-\frac{2n}{L}+\frac{2n^{2}}{L^{2}}\right)} - \frac{L}{n} + \frac{L}{n} \\ &\approx \frac{L}{n}\left(\frac{1}{1-\frac{n}{L}} - 1\right) + \frac{L}{n} \\ &\approx 1 + \frac{L}{n}.\end{aligned} \tag{B.3}$$

It is not hard to see that the phase error decreases along with the mean photon number of each pulse. In fact, in the entire regime of n and L, the phase error rate, e_{ph}^{n}, mainly depends on the average photon number per pulse, n/L, as seen in equation (B.3). In the meantime, we can see from figure B2 that the new estimation method defined in equation (B.1) is always better than the original SYK method defined in equation (3.1). Although the ideal case considered here is not the worst case scenario in practice, the improvement here indicates a better potential theoretical bound to the phase error estimation with multi-photon states.

Appendix C. Maximal transmission distance

To calculate the maximal transmission loss, we consider the asymptotic case where the values of L and $L\mu$ are very large. Since the total photon number of the state prepared by Alice follows a Poisson distribution, the photon number can be well-approximated by $L\mu$. In this case, the cost of privacy amplification is close to a fixed value. A secure key can be generated in the case where the final key rate, R, in equation (1.1) is bigger than 0:

$$1 - H(e_{\mathrm{bit}}) - H(e_{\mathrm{ph}}) \geqslant 0. \tag{C.1}$$

According to equations (3.1) and (C.1), the threshold value of the bit-flip error rate, c, is

$$c = H^{-1}[1 - H(e_{\rm ph})] = H^{-1}\left[1 - H\left(\frac{L\mu}{L-1}\right)\right] \approx H^{-1}[1 - H(\mu)]. \tag{C.2}$$

Based on the simulation model in equation (A.2), the bit-flip error rate is given by

$$e_{\rm bit} = \frac{E_{L\mu}Q_{L\mu}}{Q_{L\mu}} = e_{\rm d} + \frac{(0.5 - e_{\rm d})Y_0}{Y_0 + (1 - Y_0)(1 - e^{-\eta L\mu})}, \tag{C.3}$$

which is a decreasing function of the overall transmittance η. Since the bit error rate $e_{\rm bit}$ is upper-bounded by c, as given in equation (C.2), the minimal overall transmittance $\eta_{\rm min}$, in the case where Alice and Bob can communicate securely, can be calculated accordingly. Considering $e_{\rm bit} \leqslant c$, equation (C.3) can be rewritten as

$$1 - e^{-\eta_{\rm min}L\mu} = \left(\frac{0.5 - e_{\rm d}}{c - e_{\rm d}} - 1\right)\frac{Y_0}{1 - Y_0}. \tag{C.4}$$

Suppose that $\eta_{\rm min}$ is small, the term $1 - e^{-\eta_{\rm min}L\mu}$ can be well-approximated by $\eta_{\rm min}L\mu$. Then, the minimized $\eta_{\rm min}$ can be approximated by

$$\eta_{\rm min} \approx \frac{1}{L}\left[\frac{1}{\mu}\left(\frac{0.5 - e_{\rm d}}{c - e_{\rm d}} - 1\right)\right]\frac{Y_0}{1 - Y_0}. \tag{C.5}$$

Notice that, the relationship between the transmission loss Tl (dB) and the overall transmittance η is defined by

$$Tl = -10\log_{10}\eta, \tag{C.6}$$

and the relationship between the transmission distance D (km) and the overall transmittance η is

$$D = \frac{Tl}{\alpha} = -50\log_{10}\eta, \tag{C.7}$$

where the channel loss α is 0.2 dB km^{-1}, as we adopted in table 1. In general, the transmission distance D increases as the overall transmittance η decreases.

C.1. L-independent Y_0

In an idealized case, where the background noise $Y_0 = y_0$ is independent of L, secure transmission loss can be arbitrarily large with increasing L. That is, a secure key can be transmitted through arbitrarily large distance. Under this condition, $L\eta$, only depends on μ, as shown equation (C.5). We can therefore optimize the parameter μ to minimize $L\eta$, which is found to be around 0.06 when using the experimental parameters in table 1. Under this optimal μ, the overall transmittance is a linear function of $1/L$, which can be infinitely small if L is sufficiently large.

We can also estimate the final key rate in the case that is very close to the maximal transmission distance. For instance, we consider the regime where the transmission distance is 0.1 km less than the maximal distance. In this regime, the optimal $L\eta$ can be considered to have a fixed value. Combined with the optimal value of μ, the parameter $L\eta\mu$ is a fixed value. According to equations (A.2) and (C.3), $Q_{L\mu}$, $e_{\rm bit}$, and $E_{L\mu}Q_{L\mu}$, determined by $L\eta\mu$, are constants. The phase error rate $e_{\rm ph}$ is determined by the parameter μ. Thus, we can see that the right-hand side of the equation (4.3) is a constant, and the final key rate R is a linear function of $1/L$ (or η).

C.2. L-dependent Y_0

Under a practical condition, the total background rate Y_0 also depends on L. Suppose the state Alice that prepared is a vacuum, the probability that Bob still obtains a successful detection in each pulse is a nonzero value, y_0, due to the background noise. Since there are L pulses, the total background contribution Y_0 is defined by the probability of a successful detection event with the vacuum input, which can be given by $1 - (1 - y_0)^L$.

From equations (C.5) and (C.9), the overall transmittance is given by

$$\eta \approx \frac{1}{L}\left[\frac{1}{\mu}\left(\frac{0.5 - e_{\rm d}}{c - e_{\rm d}} - 1\right)\right]\frac{1 - (1 - y_0)^L}{(1 - y_0)^L} \geqslant \left[\frac{1}{\mu}\left(\frac{0.5 - e_{\rm d}}{c - e_{\rm d}} - 1\right)\right]y_0, \tag{C.8}$$

where the second step can be derived by

$$\frac{Y_0}{1 - Y_0} = \frac{1 - (1 - y_0)^L}{(1 - y_0)^L} \geqslant \left(\frac{1}{1 - y_0}\right)^L - 1 \geqslant (1 + y_0)^L - 1 \geqslant Ly_0. \tag{C.9}$$

Table D1. RRDPS with a bit error rate close to 0.5. The experimental parameters are listed in table 1, except $\eta_d = 90\%$ and $Y_0 = 1 - (1 - y_0)^L$ (without approximation). Here, we employ our new analysis method with decoy states.

Distance	L	$L\mu$	e_d	e_{bit}	R
1 km	220 000	0.77	0.485	0.4923	2.265×10^{-10}

For any reasonable μ, it can be concluded from equation (C.8) that the lower bound of the overall transmittance is a fixed value independent of L. Therefore, the transmission distance cannot reach infinity under this practical condition. Note that the bound of equation (C.8) is not tight.

Appendix D. Tolerable bit error rate

In the main context, we have shown that the RRDPS protocol can tolerate a bit-flip error rate e_{bit} close to 0.5 when the phase error rate e_{ph} tends to 0. Here we give a simulation example to show that, under a practical condition, the RRDPS protocol can generate a secure key when $e_{bit} = 0.4923$. The result is shown in table D1. One can see that the RRDPS protocol can tolerate the bit-flip error well.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3
[3] Mayers D 2001 *J. ACM* **48** 351–406
[4] Lo H K and Chau H F 1999 *Science* **283** 2050–6
[5] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441–4
[6] Koashi M 2009 *New J. Phys.* **11** 045018
[7] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theory* **49** 457–75
[8] Curty M, Lewenstein M and Lütkenhaus N 2004 *Phys. Rev. Lett.* **92** 217903
[9] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475–8
[10] Guan J Y, Cao Z, Liu Y, Shen-Tu G L, Pelc J S, Fejer M M, Peng C Z, Ma X, Zhang Q and Pan J W 2015 *Phys. Rev. Lett.* **114** 180502
[11] Takesue H, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827–31
[12] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832–6
[13] Li Y H *et al* 2016 *Phys. Rev.* A **93** 030302
[14] Mizutani A, Imoto N and Tamaki K 2015 *Phys. Rev.* A **92** 060303
[15] Yin H L, Fu Y, Mao Y and Chen Z B 2016 *Phys. Rev.* A **93** 022330
[16] Chau H F, Wong C, Wang Q and Huang T 2016 arXiv:1608.08329
[17] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330–3
[18] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[19] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[20] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[21] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[22] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[23] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762–4
[24] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[25] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[26] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[27] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
[28] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[29] Tang Y L *et al* 2014 *Phys. Rev. Lett.* **113** 190501
[30] Tang Y L *et al* 2014 *IEEE J. Sel. Top. Quantum Electron.* **21** 6600407
[31] Ma X, Fung C H F and Lo H K 2007 *Phys. Rev.* A **76** 012307
[32] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Phys. Rev. Lett.* **101** 093601
[33] Fung C H F, Chau H F and Lo H K 2011 *Phys. Rev.* A **84** 020303
[34] Gittsovich O, Beaudry N J, Narasimhachar V, Alvarez R R, Moroder T and Lütkenhaus N 2014 *Phys. Rev.* A **89** 012325
[35] Zhang Y Y, Bao W S, Zhou C, Li H W, Wang Y and Jiang M S 2016 *Opt. Express* **24** 20763–73
[36] Cao Z, Zhang Z, Lo H K and Ma X 2015 *New J. Phys.* **17** 053014
[37] Fröhlich B and Yuan Z 2015 *Nat. Photon.* **9** 781–2