A security proof of the round-robin differential phase shift quantum key distribution protocol based on the signal disturbance

Toshihiko Sasaki\textsuperscript{1} and Masato Koashi\textsuperscript{1}

\textsuperscript{1}Photon Science Center, School of Engineering, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
E-mail: sasaki@qi.t.u-tokyo.ac.jp

Abstract. The round-robin differential phase shift (RRDPS) quantum key distribution (QKD) protocol is a unique quantum key distribution protocol whose security has not been understood through an information-disturbance trade-off relation, and a sufficient amount of privacy amplification was given independently of signal disturbance. Here, we discuss the security of the RRDPS protocol in the asymptotic regime when a good estimate of the bit error rate is available as a measure of signal disturbance. The uniqueness of the RRDPS protocol shows up as a peculiar form of information-disturbance trade-off curve. When the length of a block of pulses used for encoding and the signal disturbance are both small, it provides a significantly better key rate than that from the original security proof. On the other hand, when the block length is large, the use of the signal disturbance makes little improvement in the key rate. Our analysis will bridge a gap between the RRDPS protocol and the conventional QKD protocols.

Keywords: round-robin differential phase shift quantum key distribution protocol, quantum key distribution, quantum cryptography
1. Introduction

Quantum key distribution (QKD) is an intensively studied field in quantum information theory because of its practical utility and feasibility. It can provide an information-theoretic security in which it is assumed that an eavesdropper (Eve) is only limited by the law of nature, or quantum mechanics. The widely understood idea about why QKD can guarantee the security is that any attempt to read information encoded on a quantum state causes a disturbance. If we base the security on this idea, we have to monitor signal disturbances to detect Eve’s intervention. Recently a new path to guarantee an information-theoretic security was proposed. This implementation is called round-robin differential phase shift QKD, or RRDPS-QKD. The main difference is that it does not need any monitoring of signal disturbance to ensure the security. Although this approach simplifies the security proof and reduces overheads caused by the finite-key effect, it is an interesting question whether we can also understand the RRDPS protocol in the standard way, namely, with the help of monitoring the disturbance in the transmitted signals. In this paper, we prove the security of the RRDPS protocol against general attacks with asymptotic key lengths when it is augmented by a procedure of monitoring the bit error rates. This analysis will gives us a deeper understanding on how the RRDPS protocol is different from or similar to the conventional QKD protocols. It also provides a better key rate for small block sizes and implies the optimality of the original security proof for large block sizes.

2. Protocol

We describe a setup of the RRDPS protocol. The sender Alice prepares an optical pulse train consisting of \(L\) pulses. The optical phase of each pulse is randomly modulated by 0 or \(\pi\). We call these \(L\) pulses a block and \(L\) the block size. Alice applies a common random phase shift \(\delta\) to all pulses in the block. The receiver Bob uses the variable-delay interferometer to measure a relative phase between a randomly chosen pair. A schematic of this interferometer is illustrated in figure 1. The delay of this interferometer is randomly chosen from 1 to \(L - 1\) times the interval of the adjacent pulses. Bob uses photon-number-resolving photon detectors to measure the relative phase of two pulses in the block. At the same time, Bob makes sure the total number of photons in the received block is unity, and otherwise declares a failure of detection. The details of this check process and its variants are given in Appendix A. If the detection has succeeded, Bob sets his pre-sifted key bit as 0 (1) if the relative phase of the detected pair is 0 (\(\pi\)). From the timing of the detection and the amount of the chosen delay, Bob can determine the indices of the detected pair. He discloses the pair of indices over an authenticated public channel. Alice sets her pre-sifted key bit by calculating the relative phase of the announced pair according to her record of the modulations. We refer to the above procedure involving transmission of one block of pulses as a round. After repeating a predetermined number (\(N\)) of rounds, Alice and Bob announce their pre-
**RRDPS based on signal disturbance**

Figure 1. A schematic of a setup for the RRDPS protocol. Alice sends out a train of \( L \) pulses after randomly applying a phase shift, either 0 or \( \pi \) to each pulse with a common random phase offset \( \delta \) by use of the phase modulator (PM). Bob uses the variable-delay interferometer to measure a relative phase between a randomly chosen pair. The amount of the delay is chosen randomly from 1 to \( L - 1 \) times the interval of the adjacent pulses.

sifted key bits of randomly sampled rounds to determine the bit error rate and remove these key bits from each of the pre-sifted keys to define their sifted keys. We call an un-sampled round, in which a sifted key bit is produced, as a sifted round. Alice sends an encrypted syndrome of her sifted key to Bob. Bob reconciles his key to Alice’s key by use of this syndrome. Then, they perform privacy amplification to obtain a correct and secure key with small imperfection.

As for the imperfections of the detectors, we assume that a non-unit quantum efficiency of a detector is modeled by a linear absorber followed by a perfect detector with unit quantum efficiency. We further assume that all the detectors have the same quantum efficiency. Then the inefficiency can be modeled by a common linear absorber placed in front of the interferometer, which can be included in the quantum channel without compromising the security.

As for Alice’s light source, we assume that the probability that it emits an \( L \)-pulse block containing more photons than a fixed threshold photon number \( \nu_{\text{th}} \) is at most \( e_{\text{src}} \). This condition can be certified in an offline test. In the security proof, we do not assume that the photon number distribution of the light source is a Poisson distribution.

3. Security

We will prove the security of the RRDPS protocol by use of the Shor-Preskil argument extended in [13] and the technique in [14]. In this argument, a sufficient amount of the privacy amplification to guarantee the security of Alice’s key is determined by estimating how well the results of a complementary measurement can be predicted.

In order to define a complementary measurement for this protocol, we construct an alternative procedure which is equivalent to the actual setup as follows. In the actual setup, Alice generates a random bit sequence \( s_1, s_2, \ldots, s_L \) and emits the corresponding optical state

\[
e^{i\delta \sum_k \hat{n}_k} \left( \bigotimes_{k=1}^{L} (-1)^{s_k \hat{n}_k} \right) |\Psi\rangle,
\]

where \( \hat{n}_k \) is the number operator of the \( k \)-th pulse and \( |\Psi\rangle \) is the state of the \( L \)-pulse train. Since the common phase shift \( \delta \) is chosen randomly and is never referred to, we can identify the emitted state as the classical
mixture of the states projected to the subspaces with fixed total photon number. The
same distribution of the sequence \( s_1, s_2, \ldots, s_L \) and the corresponding emitted state is
obtained if Alice uses \( L \) auxiliary qubits (denoted by \((A, 1), \ldots, (A, L)\)) and a classical
register (denoted by \( c \)) recording the total photon number to prepare the state
\[
2^{-L/2} \sum_{\nu=0}^{\infty} |\nu\rangle_c \sum_{k=1}^{L} \left( \sum_{s_k \in \{0, 1\}} |s_k\rangle_{A,k} (-1)^{s_k\hat{n}_k} \right) |\Psi\rangle,
\]
and then measures the auxiliary qubits on the \( \{|0\rangle_{A,k}, |1\rangle_{A,k}\} \) bases to determine \( s_k \).
Here, \( \hat{n}_k \) is the projector onto the state whose number of photons in the block is \( \nu \).
We call the \( \{|0\rangle_{A,k}, |1\rangle_{A,k}\} \) basis as \( Z \) basis of the \( k \)-th qubit. We also replace
Alice’s procedure of determining her pre-sifted key bit. In the actual protocol, after
hearing Bob’s announcement of a pair \( \{k, l\} \), Alice determines her pre-sifted key bit by
computing classical XOR \( s_k \oplus s_l \). An equivalent procedure can be constructed as follows.
Instead of measuring each of the auxiliary qubits on \( Z \) basis, we apply a CNOT gate to
the \( k \)-th and \( l \)-th qubits and then measure the target qubit on the \( Z \) basis. Although
the above description of the equivalent procedure is ambiguous about the assignment of
control and target qubits, it will be clarified later.

We define the complementary measurement for this protocol as the \( X \)-basis
measurement on the Alice’s target qubit, where \( X \)-basis measurement is defined as
\( \{|+\rangle, |−\rangle\} \) basis measurement, and \( |\pm\rangle \) is defined as \( (|0\rangle \pm |1\rangle) / \sqrt{2} \). We also define the
\( \{|+\rangle_{A,k}, |−\rangle_{A,k}\} \) basis as \( X \) basis of the \( k \)-th qubit. Note that the state \( |+\rangle_{A,k} \ (|−\rangle_{A,k}) \) corresponds to the case where the \( k \)-th pulse contains an even (odd) number of photons
(see (B.1)). If no photons are emitted in a block, each auxiliary qubit is left in state
\( |+\rangle_{A,k} \), and hence the state of the target qubit is always \( |+\rangle \). This means that the result
of the complementary measurement is predicted with certainty, and it is compatible with
the fact that no information should have leaked on Alice’s sifted key when no photons
were emitted. Based on this observation, we define the occurrence of a “phase error” to
be the case where the complementary measurement results in state \( |−\rangle \).

The use of a laser as a light source implies that there is no deterministic bound
on the total photon number \( \nu \). To handle this, we use the tagging idea [15]. In the
equivalent procedure defined above, (1) implies that Alice can measure the register \( c \)
to learn the emitted total photon number \( \nu \) in each round. We define a round to be
tagged if \( \nu > \nu_{th} \). We pessimistically assume that the full information is leaked for the
tagged rounds. Let \( \delta_{tag} \) be an upper bound on the ratio of the number of tagged and
detected rounds against the total number of detected rounds. Suppose that there is an
upper bound \( \epsilon_{\text{unit}}^{(\text{ph})} (\leq 1/2) \) on the phase error rate in the untagged and detected rounds,
namely, the number of phase error in the untagged and detected rounds against the total
number of the untagged and detected rounds. According to [13, 15], the asymptotic key
rate per block is then given by
\[
G/N = Q(1 - EC - PA),
\]
\[
EC = f_{\text{ECH}}(c),
\]
\[ \text{PA} = \delta_{\text{tag}} + (1 - \delta_{\text{tag}}) h(\bar{e}_{\text{unt}}^{(\text{ph})}), \tag{4} \]

where \( N \) is the total number of the emitted blocks, \( Q \) is the detection rate per block, \( \text{EC} \) is the cost for the error correction, \( \text{PA} \) is the cost for the privacy amplification, \( h(x) \) is the binary entropy function defined as \( -x \log_2 x - (1 - x) \log_2 (1 - x) \), \( e \) is the bit error rate, and \( f_{\text{EC}} \) is determined from the efficiency of the bit error correction. Our main task now is to determine the bound \( \bar{e}_{\text{unt}}^{(\text{ph})} \) under the condition that the observed bit error rate is \( e \) and that the emitted photon number is at most \( \nu_{th} \).

First, we focus on how the pair \( \{k, l\} \) is determined. Since Bob announces the pair only when he has received only one photon in a block, the positive-operator valued measure (POVM) element \( \hat{P}'_{\{k,l\},s_B} \) of the actual measurement that determines the unordered pair \( \{k, l\} \) and the bit \( s_B \) corresponding to the phase difference is written as

\[ \hat{P}'_{\{k,l\},s_B} = \frac{1}{2(L-1)} \hat{P} \left( \frac{1}{\sqrt{2}} (|k\rangle_B + (-1)^{s_B} |l\rangle_B) \right), \tag{5} \]

where \( \hat{P}(|\psi\rangle) \) is defined as \( |\psi\rangle \langle \psi| \), and \( |k\rangle \) refers to the state of the \( L \) pulses containing one photon in the \( k \)-th pulse and no other photons. Note that the success of detection corresponds to the operator

\[ \sum_{\{k,l\} \in \mathcal{P}, s_B \in \{0,1\}} \hat{P}'_{\{k,l\},s_B} = \frac{1}{2} \sum_{k \in \{1,\cdots,L\}} \hat{P} (|k\rangle_B), \tag{6} \]

where we define \( \mathcal{P} \) as \( \{\{k,l\} \mid k < l, k, l, \in \{1,\cdots,L\}\} \). This equation means that as long as the received block contains one photon in total, Bob’s detection succeeds with probability 1/2 regardless of its state. We can thus rewrite the actual measurement equivalently to the three-step measurement procedure defined as

(i) Bob confirms that there is one photon in the received block via an ideal projection (quantum non-demolition) measurement. If not, the measurement procedure ends with a failure of detection.

(ii) With a probability of 1/2, Bob ends the measurement procedure with a failure of detection.

(iii) Reaching this step implies that the success of detection has been assured. Bob performs the measurement defined by \( \hat{P}_{\{k,l\},s_B} := 2\hat{P}'_{\{k,l\},s_B} \) on the \( L \) pulses to determine an outcome \( (\{k, l\}, s_B) \). He announces the unordered pair \( \{k, l\} \).

In order to assess the security of Alice’s final key, we introduce a virtual protocol in which Bob decides, prior to the step (iii), whether the round is to be sampled or not. Further, when it is not to be sampled, he forgoes the step (iii) of the three-step measurement procedure and instead announces an ordered pair \( (k, l)(k \neq l) \) via a measurement described by the POVM elements

\[ \hat{P}_{(k,l)} = \frac{1}{(L-1)} \hat{P} (|k\rangle_B). \tag{7} \]

This measurement is understood as it determines the index \( k \) of the pulse containing the single photon and randomly chooses the other index \( l \). From the viewpoint of
determining the unordered pair \( \{k, l\} \), this virtual measurement is equivalent to the actual measurement because

\[
\hat{P}(k, l) + \hat{P}(l, k) = \hat{P}(\{k, l\}, 0) + \hat{P}(\{k, l\}, 1).
\]  

(8)

This means that any attack strategy by Eve can be applied to the virtual protocol and leads to the same final state over Alice’s final key and Eve’s quantum system as in the actual protocol. Therefore, the security of the virtual protocol implies that of the actual one. Now we remove the ambiguity about the assignment of control and target qubits for the CNOT gate. We choose the index of the control qubit to be \( k \) when the ordered pair \( (k, l) \) was announced. We can then write the POVM element \( \hat{e}_{(k,l)}^{\text{ph}} \) corresponding to the announcement of \( (k, l) \) and occurrence of a phase error (finding the target qubit in state \( |−\rangle \)) as

\[
\hat{e}_{(k,l)}^{\text{ph}} = \hat{P}(|−\rangle_{A,l}) \hat{P}(k, l),
\]

(9)

where we have used invariance of \( P(|−\rangle_{A,l}) \) under the CNOT gate. We also define the POVM element \( \hat{e}^{\text{ph}} \) corresponding to the occurrence of a phase error as

\[
\hat{e}^{\text{ph}} = \sum_{\{k, l\} \in \mathcal{P}} \hat{e}_{(k,l)}^{\text{ph}} + \hat{e}_{(l,k)}^{\text{ph}}.
\]

(10)

In order to bound the phase error rate \( e^{\text{ph}}_{\text{unt}} \) in the untagged sifted rounds in the virtual protocol, we utilize the bit error rate in the sample, which is determined commonly in the actual and the virtual protocol. We also use the condition on the total photon number in an untagged round. In accordance with the definition of \( \hat{e}^{\text{ph}} \), we regard the occurrence of a bit error as an outcome of a joint measurement on Alice’s \( L \) qubits and Bob’s \( L \) pulses prior to the step \( \text{[iii]} \). The corresponding POVM element \( \hat{e} \) is given by

\[
\hat{e} = \sum_{\{k, l\} \in \mathcal{P}, s, s_B \in \{0, 1\}} \hat{P} \left( |s\rangle_{A,k} |s \oplus s_B \oplus 1\rangle_{A,l} \right) \hat{P}(\{k, l\}, s_B)
\]

(11)

As for the total photon number, \[4\] dictates that the state of Alice’s \( L \) qubits is confined in a subspace \( \mathcal{H}_{A,\nu} \) when the emitted total photon number is \( \nu \). Let \( \hat{P}(\nu) \) be the projector to \( \mathcal{H}_{A,\nu} \). An asymptotic relation between the phase error rate \( e^{\text{ph}}_{\text{unt}} \) in the untagged sifted rounds and the bit error rate \( e_{\text{unt}} \) in the untagged sampled rounds is then derived by considering the maximum eigenvalue \( \Omega(\nu, \lambda) \) of the operator \( \hat{P}(\nu) (\hat{e}^{\text{ph}} - \lambda \hat{e}) \hat{P}(\nu) \) for \( \nu \leq \nu_{\text{th}} \) and a positive number \( \lambda \). The detailed calculation given in Appendix B leads to the following. In the asymptotic limit, we have

\[
e^{\text{ph}}_{\text{unt}} \leq F(\nu_{\text{th}}, e_{\text{unt}}),
\]

(12)

where \( F(\nu, e) \) is defined as

\[
F(\nu, e) := \inf_{\lambda \geq 0} (\lambda e + \Omega(\nu, \lambda)),
\]

(13)

\[
\Omega(\nu, \lambda) := \max \left( \Omega_{−}(\nu, \lambda), \Omega_{+}(\nu, \lambda) \right),
\]

(14)
Figure 2. The graph of the function $F(\nu, e)$, which also implicitly depends on the block size $L$. (a) For $L = 6$, we vary $\nu$ from 1 to 3. (b) For $L = 64$, we vary $\nu$ from 1 to 32. The value of $F(\nu, e)$ increases as $\nu$ becomes larger.

$$\Omega_-(\nu, \lambda) := \frac{\nu - 1}{L - 1} - \frac{L\lambda + 2}{4(L - 1)} \left(1 - \sqrt{1 - \frac{8(\nu - 1)\lambda}{(L\lambda + 2)^2}}\right), \quad (15)$$

and

$$\Omega_+(\nu, \lambda) := \frac{\nu}{L - 1} - \lambda \frac{L - 1 - \nu}{2(L - 1)}. \quad (16)$$

We illustrate the function $F(\nu, e)$ for the cases $L = 6$ and $L = 64$ in figure 2. As is seen from the figure, each curve for $F(\nu, e)$ with fixed $\nu$ can be well approximated by two straight segments, given by

$$F(\nu, e) \sim \begin{cases} \frac{\nu - 1}{L} \left(1 - \frac{e}{e^*(\nu)}\right) + \frac{\nu}{L - 1} \frac{e}{e^*(\nu)} & 0 \leq e < e^*(\nu) \\ \frac{e}{L - 1} & e \geq e^*(\nu) \end{cases} \quad (17)$$

where $e^*(\nu)$ is defined as $(L - 1 - \nu)/(2(L - 1))$. The function $F(\nu, e)$ takes a constant value when $e$ is large. The value of $\nu/(L - 1)$ reproduces the result of the original security proof [11]. There, the bound was derived by an argument which relies neither on the state of the pulses after Eve’s intervention nor correlations between Alice’s and Bob’s systems. Roughly speaking, Eve cannot learn most of the phases of the $L$ pulses emitted from Alice since those pulses are weak. Moreover, as seen in [7], one of the announced indices is uniformly random no matter what state Eve sends to Bob. These two properties prevent Eve from predicting the phase difference in the announced pair. When $e$ is small, the bound $F(\nu, e)$ becomes lower as $e$ becomes smaller, which is a typical information-disturbance trade-off. Qualitatively, the origin of the trade-off is the same as the original DPS protocol [7]. If Eve reads the relative phase between two successive weak pulses, she disturbs the relative phases of these pulses to the other pulses, increasing the bit error rate. More quantitatively, however, it was also shown [16, 14] that Eve can considerably suppress the increase in the bit error rate by gradually modulating the amplitudes of a sequence of pulses in the DPS protocol. Since the relative
Figure 3. Asymptotic key rate per pulse $G/(LN)$ versus overall transmission $\eta$ for (a) $L = 6$ and (b) $L = 64$. We assume a constant bit error rate of 3%. The upper curve: the key rate when the signal disturbance is monitored. The lower curve: the key rate when the signal disturbance is not monitored.

phases of two distant pulses in this strategy are highly disturbed, it causes a high bit error rate in the RRDPS protocol.

The remaining problem is to bound $\delta_{\text{tag}}$ and $e_{\text{unt}}$. From the definition of $e_{\text{src}}$, the expected total number of the tagged rounds is at most $Ne_{\text{src}}$. If we recall Bob’s three-step measurement procedure, we see that half of the rounds lead to detection failure at step (iii). In the asymptotic limit, it means

$$\delta_{\text{tag}} \leq \frac{e_{\text{src}}}{2Q}.$$  

As for $e_{\text{unt}}$, we use the fact that a fraction $(1 - \delta_{\text{tag}})$ of the sampled rounds should be untagged in the asymptotic limit. Then, we have $e_{\text{unt}}(1 - \delta_{\text{tag}}) \leq e$, namely,

$$e_{\text{unt}} \leq \frac{e}{1 - \delta_{\text{tag}}}. \quad (19)$$

Combining these bounds with (4), we obtain a sufficient amount of the privacy amplification as

$$PA = \frac{e_{\text{src}}}{2Q} + \left(1 - \frac{e_{\text{src}}}{2Q}\right) h \left(F\left(\nu_{\text{th}}, \frac{e}{1 - \frac{e_{\text{src}}}{2Q}}\right)\right). \quad (20)$$

4. Secure key rate

In order to examine how the performance of the RRDPS protocol is improved by use of the bit error rate, we calculate the secure key generation rate based on the following model. We assume that the dark countings are negligible and set $e = 0.03$ and $f_{EC} = 1.1$. We also assume that the measurement results are the same as those calculated with the source emitting coherent states. It means that $Q$ and $e_{\text{src}}$ is written as

$$Q = \frac{L\mu\eta}{2} \exp\left(-\frac{L\mu\eta}{2}\right) \quad (21)$$
and
\[ e_{\text{src}} = 1 - \exp(-L\mu) \sum_{\nu=0}^{\nu_{\text{th}}} \frac{(L\mu)^\nu}{\nu!}, \]  
(22)

where \( \mu \) is the average photon number of a pulse and \( \eta \) is the overall transmission rate. In figure 3, we plot the key rate per pulse \( G/(LN) \) as a function of the overall transmission rate \( \eta \) for \( L = 6 \) and \( L = 64 \). We optimized the values of \( \nu_{\text{th}} \) and \( \mu \) for each \( \eta \). We also plotted the key rate when the amount of privacy amplification is independent of the bit error rate, which is given by (20) with \( F(\nu, e) \) replaced by \( \nu_{\text{th}}/(L - 1) \). These graphs confirm that we can improve the key rate by use of signal disturbance. On the other hand, the amount of improvement decreases as the block size becomes larger. This behavior can be ascribed to the gap between \( F(\nu, 0) \) and \( F(\nu, 0.5) \), namely, how the ability of Eve to cause a phase error depends on whether her attack is restricted to a low bit error rate or not. In the limit of no bit errors, what Eve can do is to leave one of the \( \nu \) emitted photons untouched and pass on to Bob. She gathers information from the remaining \( \nu - 1 \) photons, while she has no control over which indices will be announce by Bob because the photon passed on to Bob is coherent over entire pulses and hence there is no correlation to the other systems. This explains the value of \( F(\nu, 0) = (\nu - 1)/L \). When we remove the restriction on the bit error, Eve can use all of the \( \nu \) photons to gather information. She can also have a partial influence on the announced indices. As seen from (7), she has the power of veto on one value and the range of index \( l \) spans \( L - 1 \) values. This results in \( F(\nu, 0.5) = \nu/(L - 1) \). When the block size becomes large, both values behaves as \( \nu/L \), leading to a small difference in Eve’s ability.

5. Summary

In this paper, we proved the security of the RRDPS protocol against general attacks in the asymptotic regime from the standard viewpoint that Eve’s intervention is estimated from the signal disturbance. The key ingredient of the security proof was to determine the relation between the bit error rate and the phase error rate, where the latter represents the lack of ability to predict an observable complementary to the sifted key. As in the other protocols such as the BB84 protocol, the phase error rate decreases as the signal disturbance approaches to zero. On the other hand, beyond a threshold value of the bit error rate, the phase error ceases to depend on the bit error rate, which gives an alternative explanation for the original RRDPS protocol in terms of information-disturbance relation. We have seen an improvement in the key rate compared to that obtained with no monitoring of the signal disturbance. The difference is prominent for a small value of the block size \( L \), whereas it decreases with \( L \). The reason for this behavior is that the leading \( O(L^{-1}) \) term of the phase error rate is the same regardless of whether the bit error is restricted or not. This indicates that the original RRDPS protocol for a large block size is almost optimal even though it does not use the information available from monitoring disturbance.
**Figure A1.** (a): A setup for counting the total photon number deterministically. An optical shutter is placed just before the variable-delay interferometer. It is closed during the arrival timings of the idle pulses. (b): A measurement setup using threshold detectors. An optical shutter is placed just before the variable delay. When the shutter is closed for the whole block, the double count rate of this setup can bound the rate of rounds where there are two or more photons in the block received by Bob. The optical shutter is also used for avoiding the mixing with the next block.

**Acknowledgments**

We thank K. Tamaki for helpful discussions. This work was funded in part by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan), Photon Frontier Network Program (Ministry of Education, Culture, Sports, Science and Technology).

**Appendix A.**

In order to count the total photon number by using the photon number resolving detectors after the delayed interferometer, we need a careful implementation to avoid crosstalk between adjacent blocks. One simple way is to define blocks such that each block is followed by $L - 1$ idle pulses before the next block starts. As in figure A1(a), Bob places an optical shutter in front of his apparatus and close it during the arrival timings of the idle pulses. All photons in a block are then reach a detector at one of $2L - 1$ timings dedicated solely for the block. In this scheme, the insertion of idle pulses almost halves the efficiency of the protocol. In order to avoid the separation of blocks, Bob can prepare two copies of variable interferometers and use a switch to redirect every other incoming block to each interferometer.

There is another way to handle this problem, which allows the use of threshold detectors (distinguishing only the vacuum from one or more photons) instead of the photon number resolving detectors, which was adopted in the demonstration [17] of the RRDPS protocol with a passive configuration. Instead of actually learning the photon number in each block, we use the idea of tagging, namely, the property that each multi-photon block can be tagged in principle without affecting the measurements in the protocol. To obtain an upper bound on the number of tagged rounds, Bob places an optical shutter just before the variable delay as in figure A1(b). For a randomly sampled block, he throws away all the pulses in the delayed arm, and records the occurrence of coincidence detections in the entire block. This is equivalent to a conventional setup [18, 19], which can be used for bounding the probability of multiple photons in the
signal. In this scheme, it is not necessary to separate the blocks apart because the optical shutter can be used for avoiding the mixing with the next block by throwing away the pulses that are to be delayed beyond the block duration.

Appendix B.

We first identify the subspace $\mathcal{H}_{A,\nu}$ of Alice’s $L$ qubits and the corresponding projection $\hat{P}^{(\nu)}$. The initial state in (1) can be rewritten in terms of the $X$ basis of the qubits as

$$\sum_{\nu=0}^{\infty} |\nu\rangle_c \otimes_{k=1}^{L} \left( \sum_{s \in \{+,–\}} |\pm_s\rangle_{A,k} \frac{1}{2} (1 \pm s \frac{\hat{n}_k}{2}) \right) |\Psi\rangle. \quad (B.1)$$

The operator $\frac{1}{2} (1 \pm s (-1)^{\hat{n}_k})$ is a projection onto the subspace in which the $k$-th pulse includes even (or odd) number of photons. Let us write the $X$-basis states of Alice’s $L$ qubits as $\hat{H} \otimes L |a\rangle_A$, where $a$ is the array of bit values $a_k$, $|a\rangle_A$ represents $\otimes_{k=1}^{L} |a_k\rangle_{A,k}$, and $\hat{H}$ is the Hadamard operator. Let $|a\rangle$ be $\sum_{k=1}^{L} \delta_{a_k,1}$. The correlation in (B.1) implies that when the qubits are found in state $\hat{H} \otimes L |a\rangle_A$, the total emitted photon number $\nu$ satisfies $\nu \geq |a|$ and has the same parity as that of $|a\rangle$. Hence, given $\nu$, the state of the qubits should be contained in subspace $\mathcal{H}_{A,\nu}$ defined by the projection

$$\hat{P}^{(\nu)} := \sum_{|a| \in \mathfrak{N}_\nu} \hat{P} \left( \hat{H} \otimes L |a\rangle_A \right), \quad (B.2)$$

with $\mathfrak{N}_\nu := \{ \nu - 2k \mid k \in \mathbb{Z}, k \geq 0, \nu - 2k \geq 0 \}$.

For a non-negative number $\lambda$, let us define $\Omega(\nu, \lambda)$ as the largest eigenvalue of the operator $\hat{P}^{(\nu)} (\hat{\epsilon}^{(\text{ph})} - \lambda \hat{\epsilon}) \hat{P}^{(\nu)}$, which satisfies

$$\hat{P}^{(\nu)} (\hat{\epsilon}^{(\text{ph})} - \lambda \hat{\epsilon}) \hat{P}^{(\nu)} \leq \Omega(\nu, \lambda) \hat{P}^{(\nu)}. \quad (B.3)$$

Let us consider one of the untagged rounds, which means $\nu \leq \nu_{\text{th}}$, and let $\hat{\rho}_{\text{unt}}$ be the state of Alice’s $L$ qubits and Bob’s $L$ pulses prior to the step (iii). From its construction, $\hat{\rho}_{\text{unt}}$ satisfies $\hat{P}^{(\nu)} \hat{\rho}_{\text{unt}} \hat{P}^{(\nu)} = \hat{\rho}_{\text{unt}}$. By multiplying (B.3) by $\hat{\rho}_{\text{unt}}$ and taking the trace, we find

$$\text{Tr} \left( \hat{\rho}_{\text{unt}} \hat{\epsilon}^{(\text{ph})} \right) \leq \lambda \text{Tr}(\hat{\rho}_{\text{unt}} \hat{\epsilon}) + \max_{\nu \leq \nu_{\text{th}}} \Omega(\nu, \lambda). \quad (B.4)$$

This inequality implies that for any $\epsilon(>0)$, the probability of violating the inequality

$$\epsilon_{\text{unt}}^{(\text{ph})} \leq \lambda \epsilon_{\text{unt}} + \max_{\nu \leq \nu_{\text{th}}} \Omega(\nu, \lambda) + \epsilon \quad (B.5)$$

for the measured values decreases exponentially as the number of the untagged and detected rounds becomes larger. One way to prove this statement is to define a sequence regarded as a martingale and use Azuma’s inequality [20].

Next, we determine the function $\Omega(\nu, \lambda)$. We introduce a unitary operator $\hat{U}$ by the relation

$$\hat{U} \hat{H} \otimes L |a\rangle_A |k\rangle_B = \hat{H} \otimes L |a'\rangle_A |k\rangle_B, \quad (B.6)$$
where \( a' \) is defined by \( a'_t = a_t \oplus \delta_{t,k} \) for each element. In terms of this unitary, the operators \( \hat{P}^{(\nu)}, \hat{e}, \) and \( \hat{e}^{(ph)} \) are transformed as

\[
\hat{U}^\dagger \hat{P}^{(\nu)} \hat{U} = \sum_{|a|=\nu-1,\nu-3,...} \hat{P} \left( \hat{H}^{\otimes L} |a\rangle_A \right) + \sum_{|a|=\nu+1} \sum_{k=1}^L \hat{P} \left( \hat{H}^{\otimes L} |a\rangle_A \right) \hat{P} (|k\rangle_B) \delta_{ak,1},
\]

(B.7)

\[
\hat{U}^\dagger \hat{e} \hat{U} = \sum_{\{k,l\} \in \Psi} \frac{1}{L-1} \hat{P} \left( \frac{1}{\sqrt{2}} (|k\rangle_B - |l\rangle_B) \right),
\]

(B.8)

\[
\hat{U}^\dagger \hat{e}^{(ph)} \hat{U} = \hat{e}^{(ph)} = \frac{1}{L-1} \sum_{a \in \Omega} \hat{P} \left( \hat{H}^{\otimes L} |a\rangle_A \right) \sum_{k=1}^L \hat{P} (|k\rangle_B) ((|a| - 1) \delta_{ak,1} + |a| \delta_{ak,0}),
\]

(B.9)

where \( \Omega \) is defined as \( \{0,1\}^L \).

Since all the transformed operators commute with \( \hat{P} \left( \hat{H}^{\otimes L} |a\rangle_A \right) \), we have a direct-sum decomposition

\[
\hat{U}^\dagger \hat{P}^{(\nu)} (\hat{e}^{(ph)} - \lambda \hat{e}) \hat{P}^{(\nu)} \hat{U} = \sum_{|a|=\nu+1,\nu-1,\nu-3,...} \hat{P} \left( \hat{H}^{\otimes L} |a\rangle_A \right) \otimes \hat{\Lambda}(\nu, \lambda, a).
\]

(B.10)

Due to the symmetry over the permutation of the index, the largest eigenvalue of \( \hat{\Lambda}(\nu, \lambda, a) \) depends only on \( |a| \), which we denote by \( \Omega(\nu, \lambda, |a|) \). Equation (B.10) implies that \( \Omega(\nu, \lambda) \) is equal to the maximum of \( \Omega(\nu, \lambda, |a|) \) over \( |a| = \nu + 1, \nu - 1, \nu - 3, \ldots \).

For evaluation of \( \Omega(\nu, \lambda, |a|) \), it suffices to consider sequences in the form of \( a = (1, \ldots, 1, 0, \ldots, 0) \). The matrix representation of operator \( \hat{\Lambda}(\nu, \lambda, a) \) is conveniently described by the following matrices. Define \( d \)-dimensional matrices \( M_1^{(d)} \) and \( M_2^{(d,m)} \) by

\[
\forall i, j, (M_1^{(d)})_{ij} = 1
\]

(B.11)

and

\[
\forall i, j, (M_2^{(d,m)})_{ij} = \begin{cases} 1 & i = j \leq m \\ 0 & \text{otherwise} \end{cases}
\]

(B.12)

We also define \( 1^{(d)} \) as the identity matrix. From (B.7), (B.8), and (B.9), the nonzero part of \( \hat{\Lambda}(\nu, \lambda, a) \) is represented as

\[
\frac{\lambda}{2(L-1)} M_1^{(L)} - \frac{1}{L-1} M_2^{(L,|a|)} + \frac{2|a| - L\lambda}{2(L-1)} 1^{(L)}
\]

(B.13)

for \( |a| = \nu - 1, \nu - 3, \ldots \), and

\[
\frac{\lambda}{2(L-1)} M_1^{(|a|)} + \frac{2(|a| - 1) - \lambda L}{2(L-1)} 1^{(|a|)}
\]

(B.14)

for \( |a| = \nu + 1 \). In order to obtain their eigenvalues, we use the next proposition.

**Proposition 1.**

\[
\det \left( \alpha M_1^{(d)} + \beta M_2^{(d,m)} + \gamma 1^{(d)} \right) = \gamma^{d-m-1}(\gamma + \beta)^{m-1}(\gamma^2 + (\beta + da)\gamma + (d - m)\alpha\beta)
\]

(B.15)
(Proof of proposition [1]) The normalized vectors defined as
\[ m^{-1/2}(1, e^{2\pi i k/m}, \ldots, e^{2\pi i (m-1)/m}, 0, \ldots, 0) \quad (k = 1, \ldots, m - 1) \] (B.16)
and the normalized vectors defined as
\[(d - m)^{-1/2}(0, \ldots, 0, 1, e^{2\pi i k/(d - m)}, \ldots, e^{2\pi i (d - m - 1)/(d - m)}) \quad (k = 1, \ldots, d - m - 1) \] (B.17)
are the eigenvectors with the eigenvalues \( \beta + \gamma \) and \( \gamma \). The remaining space is spanned by the two normalized vectors \( m^{-1/2}(1, \ldots, 0, \ldots, 0) \) and \( (d - m)^{-1/2}(0, \ldots, 0, 1, \ldots, 1) \).

By directly calculating the determinant, we obtain (B.15). □

By use of proposition [1] we obtain the largest eigenvalues of (B.13) and (B.14) as
\[
\Omega_-(\nu, \lambda) := \max_{|a| = \nu - 1, \nu - 3, \ldots} \Omega(\nu, \lambda, |a|) = \Omega(\nu, \lambda, \nu - 1) = \frac{\nu - 1}{L - 1} - \frac{L\lambda + 2}{4(L - 1)} \left(1 - \sqrt{1 - \frac{8(\nu - 1)\lambda}{(L\lambda + 2)^2}}\right)
\] (B.18)
and
\[
\Omega_+(\nu, \lambda) := \Omega(\nu, \lambda, \nu + 1) = \frac{\nu}{L - 1} - \lambda \frac{L - 1 - \nu}{2(L - 1)},
\] (B.19)
respectively. Thus, the function \( \Omega(\nu, \lambda) \) is given by
\[
\Omega(\nu, \lambda) = \max (\Omega_-(\nu, \lambda), \Omega_+(\nu, \lambda)).
\] (B.20)

From the explicit expressions of \( \Omega(\nu, \lambda) \), we find that \( \Omega(\nu, \lambda) \) is an increasing function for \( \nu \). It means
\[
\max_{\nu \leq \nu_{th}} \Omega(\nu, \lambda) = \Omega(\nu_{th}, \lambda).
\] (B.21)
Combined with (13), it ensures that for any \( \epsilon > 0 \), there exists \( \lambda \geq 0 \) such that
\[
\lambda e_{unt} + \max_{\nu \leq \nu_{th}} \Omega(\nu, \lambda) \leq F(\nu_{th}, e_{unt}) + \epsilon.
\] (B.22)
With (B.5), we see that the probability of violating
\[
e_{unt}^{(ph)} \leq F(\nu_{th}, e_{unt}) + 2\epsilon
\] (B.23)
vanishes in the asymptotic limit. This statement is the precise meaning of (12).

References

[1] 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, page 175, New York, 1984. Bangalore, India, IEEE Press.
[2] Artur K. Ekert. Quantum cryptography based on bell’s theorem. Phys. Rev. Lett., 67:661–663, Aug 1991.
[3] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68:3121–3124, May 1992.
[4] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett., 81:3018–3021, Oct 1998.
RRDPS based on signal disturbance

[5] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[6] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108–194108, 2005.

[7] K. Inoue, E. Waks, and Y. Yamamoto. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A*, 68:022317, Aug 2003.

[8] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[9] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Z. Phys.*, 43:172–198, 1927.

[10] Masanao Ozawa. Uncertainty relations for noise and disturbance in generalized quantum measurements. *Ann. Phys.*, 311(2):350 – 416, 2004.

[11] Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475–478, 2014.

[12] Toshimori Honjo and Kyo Inoue. Differential-phase-shift quantum key distribution with an extended degree of freedom. *Opt. Lett.*, 31(4):522–524, Feb 2006.

[13] M Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009.

[14] Kiyoshi Tamaki, Masato Koashi, and Go Kato. Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization. *arXiv:1208.1995*, 2012.

[15] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect device. *Quant. Inf. Comp.*, 4:325, 2004.

[16] Toyohiro Tsurumaru. Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol. *Phys. Rev. A*, 75:062319, Jun 2007.

[17] Hiroki Takesue, Toshihiko Sasaki, Kiyoshi Tamaki, and Masato Koashi. Experimental quantum key distribution without monitoring signal disturbance. *Nat Photon*, 9(12):827–831, Dec 2015.

[18] R. Hanbury Brown and R. Q. Twiss. A test of a new type of stellar interferometer on sirius. *Nature*, 178(4541):1046–1048, Nov 1956.

[19] Roy J. Glauber. Coherent and incoherent states of the radiation field. *Phys. Rev.*, 131:2766–2788, Sep 1963.

[20] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal, Second Series*, 19(3):357–367, 1967.