PHYSICAL REVIEW A **92**, 060303(R) (2015)

Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws

Akihiro Mizutani,[1,*] Nobuyuki Imoto,[1] and Kiyoshi Tamaki[2]

[1]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*

[2]*NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*

(Received 9 October 2015; published 30 December 2015)

Recently, a new type of quantum key distribution, called the round-robin differential-phase-shift (RRDPS) protocol [T. Sasaki *et al.*, Nature (London) **509**, 475 (2014)], was proposed, where the security can be guaranteed without monitoring any statistics. In this Rapid Communication, we investigate source imperfections and side-channel attacks on the source of this protocol. We show that only three assumptions are needed for the security, and no detailed characterizations of the source or the side-channel attacks are needed. This high robustness is another striking advantage of the RRDPS protocol over other protocols.

DOI: 10.1103/PhysRevA.92.060303 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex

Quantum key distribution (QKD) enables two distant parties (Alice and Bob) to generate a key, which is secret from any eavesdropper (Eve). Since the invention of the first QKD protocol, the Bennett-Brassard 1984 protocol [1], many QKD protocols have been proposed for both discrete variable protocols [2–7] and continuous variable protocols [8,9]. One of the most important tasks in the security proof is to derive an upper bound on the information leakage to Eve. Conventionally, it has been believed that the information leakage can be estimated by monitoring some statistics by Alice and Bob during the quantum communication part of the QKD protocol [10–20]. Recently, a new type of protocol, the round-robin differential-phase-shift (RRDPS) protocol [21], was proposed and surprisingly, the information leakage of this protocol is estimated without any monitoring, but it depends only on the state prepared by Alice. This property leads to some practical advantages, such as the better tolerance on the bit error rate and the fast convergence in the finite key regime [21]. This protocol has attracted intensive attention from theoretical works [22,23], and proof-of-principle experiments have been demonstrated [23–26].

In practice, there are some issues to be addressed to guarantee the security of the RRDPS protocol when it is actually implemented. These issues arise because there is a gap between the properties of the actual devices used in QKD systems and the mathematical model that the security proofs assume, which is also the case for all QKD protocols. Therefore, to bridge this gap is crucial for the implementation security, and many works have been devoted in this direction [17,27–32]. In the case of the RRDPS protocol, all the security analyses including the original proof [21] and the recent works [22,23] have made ideal assumptions on Alice's light source (for instance, phase modulations are assumed to be perfect and any side-channel attacks are excluded). Therefore, to consider the security proof accommodating source flaws is indispensable toward a practical and secure implementation of the RRDPS protocol.

In this Rapid Communication, we extend the security proof of [21] to accommodate the source flaws. Surprisingly, we found that the security can be guaranteed based only on the three assumptions on Alice's source. These assumptions are on the probability of emitting the vacuum state, on the probability that L light pulses contain more than a particular number of photons, and on the independence among the sending states. Importantly, no assumptions on the phase modulation or detailed specifications of imperfections and side-channel attacks on the source are needed. Even with these imperfections and side channels, we show that the RRDPS protocol can distribute the key over longer distances. These results show that the RRDPS protocol is highly robust against the source flaws, which is another striking advantage of this protocol over other protocols.

Before explaining the security of the RRDPS protocol with the flawed sources, we summarize the assumptions we made on the devices. First, as for Alice's side, she employs blocks of L light pulses, and applies phase modulation $\theta_{a_k}^{(k)}$ $(1 \leqslant k \leqslant L)$ to each of the pulses depending on a randomly chosen bit $a_k \in \{0,1\}$. The assumptions on Alice's sending states are summarized as follows.

A1. For every light pulse, the probability of the vacuum emission for the bit value 0(1) is upper and lower bounded by $p_{\mathrm{U},0(1)}(0)$ and $p_{\mathrm{L},0(1)}(0)$, respectively (see Sec. I in the Supplemental Material for the discussions on the estimation of these bounds for some experimental setups [33]).

A2. The L pulses contain in total at most ν_{th} photons except with the probability e_{src}.

A3. There is no quantum and classical correlation among the sending states, and the system that purifies each of the sending states is possessed by Alice.

We emphasize that we do not make any assumptions on phase modulations. Obviously, in order to generate a secret key, $\theta_0^{(k)}$ and $\theta_1^{(k)}$ need to be controlled such that the resulting bit error rate is low enough. However, for the security proof, this precise control over the phase modulation is not needed: our security proof holds not only when the actual value of phase modulations $\{\theta_0^{(k)},\theta_1^{(k)}\}$ do not coincide with $\{0,\pi\}$, but also when Alice has no knowledge about $\theta_0^{(k)}$ and $\theta_1^{(k)}$. Assumption A2 requires that $\Pr[\sum_{k=1}^{L} n_k > \nu_{\mathrm{th}}] \leqslant e_{\mathrm{src}}$ must be satisfied, where n_k denotes the number of photons included in the k^{th} pulse, which would be obtained if we measured it, and the left-hand side represents the probability that the total photon

*mizutani@qi.mp.es.osaka-u.ac.jp

number existing in the L pulses exceeds $\nu_{\rm th}$. We also emphasize that we do not make the single-mode assumption on the pulse, and the mode can depend on the bit value. This includes, for instance, the following cases: (1) the polarization of the pulse depends on the chosen bit value and (2) Eve performs a Trojan-horse attack (THA) [34], where she injects a strong light pulse into Alice's source to obtain some information on the source from the back-reflected pulse.

From the assumption of the independence among the sending states described in A3, the $k^{\rm th}$ sending state is expressed as a partial trace over the system $\mathrm{A_n}$ of the following state

$$|\Psi_{a_k,k}\rangle_{\mathrm{A_n,B}} = \sum_w \sqrt{c^{(k)}_{w,a_k}}\hat{U}^{(k)}_{a_k}|w^{(k)}_{a_k}\rangle_{\mathrm{A_n}}|\varphi^{(k)}_{w,a_k}\rangle_{\mathrm{B}},$$

where $c^{(k)}_{w,a_k}$ are non-negative real numbers satisfying $\sum_w c^{(k)}_{w,a_k} = 1$, $\hat{U}^{(k)}_{a_k}$ is an arbitrary unitary operator on the system $\mathrm{A_n}$, $\{|w^{(k)}_{a_k}\rangle_{\mathrm{A_n}}\}_w$ are orthonormal bases of the ancilla system, and $\{|\varphi^{(k)}_{w,a_k}\rangle_{\mathrm{B}}\}_w$ are orthonormal bases to diagonalize the density operator of the sending state

$$\hat{\rho}^{(k)}_{a_k} := \mathrm{tr}_{\mathrm{A_n}}|\Psi_{a_k,k}\rangle\langle\Psi_{a_k,k}|_{\mathrm{A_n,B}}. \tag{1}$$

Note that the system $\mathrm{A_n}$ that purifies each of the sending states is possessed by Alice. Then, for each trial, Alice sends $\otimes_{k=1}^{L}\hat{\rho}^{(k)}_{a_k}$ to Bob over the quantum channel. Note that in the original protocol [21], Alice sends $\otimes_{k=1}^{L}e^{i\pi a_k\hat{n}_k}|\Psi\rangle$ in each trial, where $\hat{n}_k$ is the number operator for the $k^{\rm th}$ pulse, and $|\Psi\rangle$ is the L-pulse state (contains at most $\nu_{\rm th}$ photons) before performing a perfect phase modulation ($e^{i\pi a_k\hat{n}_k}$).

As for the assumptions on Bob's side, they are the same as those made in the original security proof [21], that is, Bob uses detectors that can discriminate among the vacuum, a single photon, and multi photons, and Bob has a random number generator (RNG). Using devices with these assumptions, we describe Bob's actual procedures in what follows. Note that Bob's actual procedures are the same as those in the original protocol [21]. Bob first splits L incoming pulses into two trains of pulses, and shifts backwards only one train by r that is chosen randomly from $\{1,\ldots,L-1\}$. Then Bob lets each of the first $L-r$ pulses in the shifted train interfere with each of the last $L-r$ pulses in the other train with a 50:50 beam splitter, and performs a photon measurement with the two detectors. Each of these detectors corresponds to the bit value of 0 and 1, respectively. Bob takes note of the bit value when he observes a single photon in the original L pulses in total, otherwise he discards the data. Also, he records in which time slot he obtained the single photon, and he announces this time slot and r over the classical channel. From this information, Alice obtains a sifted key $a_{k_{\rm d}} \oplus a_{k_{\rm d}+r}$, where $k_{\rm d}$ denotes the time slot of the single-photon detection. Bob repeats this process for many blocks containing L pulses.

Under the assumptions listed above, we prove the security of the RRDPS protocol with the source flaws. We note that, for simplicity of the analysis, we consider that the number of blocks containing L pulses sent is asymptotically large. In the proof, we construct a virtual protocol that cannot be distinguished from the actual protocol from Eve's viewpoint. In this virtual protocol, Alice first prepares her virtual qubit virA, ancilla qubits, and system B in the following state:

$$|\Phi\rangle_{\mathrm{virA,A_n,B}} = 2^{-L/2}\bigotimes_{k=1}^{L}\sum_{a_k=0,1}|a_k\rangle_{\mathrm{virA}}|\Psi_{a_k,k}\rangle_{\mathrm{A_n,B}}, \tag{2}$$

and sends only system B to Bob over the quantum channel. Here, this state is in the tensor product due to the assumption A3, and we define $\{|0\rangle,|1\rangle\}$ as the Z basis state.

Next, we explain Bob's measurement procedures for the virtual protocol. As explained above, in the actual protocol, Bob performs an interference measurement on $i^{\rm th}(1\leqslant i\leqslant L)$ and $j^{\rm th}(1\leqslant j\leqslant L)$ pulses, where a difference of i and j is randomly chosen by Bob's RNG (i.e., $|i-j|=r$). In the virtual protocol, however, Bob does not perform such an interference measurement, but performs the measurement to determine which pulse contains a single photon among the incoming L pulses. In this virtual measurement, the index i is determined by the location of the single photon ($1\leqslant i\leqslant L$), and the other index j is determined as

$$j = i + (-1)^b r (\mathrm{mod}\, L), \tag{3}$$

where r is randomly chosen from the RNG, and b is randomly chosen from 0 or 1 by Bob. After obtaining the pair $\{i,j\}$, he announces $\{i,j\}$ to Alice over the classical channel. Note that Eve has perfect control over i because she can freely choose which pulse contains a single photon, but she cannot control j at all because j contains the randomness Bob locally chooses. The reason why Bob can choose j as Eq. (3) is that the probability distributions of obtaining i and j if Bob postselects the successful detection event (i.e., only a single photon is detected from the L pulses) are exactly the same for both actual and virtual protocols for any eavesdropping [21]. This means that the classical information available to Eve is the same between the two protocols. Therefore, combined with the equivalence between the virtual and actual protocols in Alice's side, we are allowed to discuss the security based on the virtual protocol. In the virtual protocol, Alice keeps all the L virtual qubits and the ancilla qubits when Bob obtains the successful detection.

The quantity we use to measure the leaked information is the so-called phase error rate [35], which is related to the smooth max-entropy [17,36]. With the phase error rate $e_{\rm ph}$, the key rate per transmission of one pulse is expressed as [37]

$$R = Q[1 - f_{\rm EC}h(e_{\rm b}) - h(e_{\rm ph})]/L, \tag{4}$$

where Q denotes the single-photon detection probability in Bob's measurement, $f_{\rm EC}$ is an error correction efficiency, and $e_{\rm b}$ denotes the bit error rate in the protocol and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ as the binary entropy function. Here, $h(e_{\rm ph})$ represents the fraction of bits to be shortened in the privacy amplification step. Once the sifted bits are shortened according to this fraction, the phase error information that Eve used to have becomes totally useless for her guessing the generated key.

Our goal below is to estimate the upper bound on the phase error rate. For the estimation, we need to define the phase error rate, but before we give its definition, it is convenient to rewrite

Eq. (2) as

$$|\Phi\rangle_{\mathrm{virA,A_n,B}} = 2^{-L}\bigotimes_{k=1}^{L}\Big[\sqrt{2+d_k}|+\rangle_{\mathrm{virA}}|\Phi_k^{+}\rangle_{\mathrm{A_n,B}} + \sqrt{2-d_k}|-\rangle_{\mathrm{virA}}|\Phi_k^{-}\rangle_{\mathrm{A_n,B}}\Big],$$

where we define $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ as the X basis state,

$$d_k = \sum_{w,w'}\sqrt{c_{w,0}^{(k)}c_{w',1}^{(k)}}\big(\langle w_1^{\prime(k)}|\hat{U}_1^{(k)\dagger}\hat{U}_0^{(k)}|w_0^{(k)}\rangle_{\mathrm{A_n}} \times \langle\varphi_{w',1}^{(k)}|\varphi_{w,0}^{(k)}\rangle_{\mathrm{B}} + \mathrm{c.c.}\big),$$

and

$$\big|\Phi_k^{\pm}\big\rangle_{\mathrm{A_n,B}} = (|\Psi_{0,k}\rangle_{\mathrm{A_n,B}} \pm |\Psi_{1,k}\rangle_{\mathrm{A_n,B}})/\sqrt{2\pm d_k}.$$

Here, c.c. stands for complex conjugate. The key parameter in the security proof is the vacuum emission probability of $|\Phi_k^{\pm}\rangle_{\mathrm{A_n,B}}$, which is defined by $p_{\pm}^{(k)}(0)$ and given by (see Sec. II in the Supplemental Material for details)

$$p_{\pm}^{(k)}(0) = \frac{\big(\sqrt{p_0^{(k)}(0)} \pm \sqrt{p_1^{(k)}(0)}\big)^2}{2\pm d_k}. \tag{5}$$

Here $p_0^{(k)}(0)$ and $p_1^{(k)}(0)$ denote the vacuum emission probabilities of $|\Psi_{0,k}\rangle_{\mathrm{A_n,B}}$ and $|\Psi_{1,k}\rangle_{\mathrm{A_n,B}}$, respectively. In the virtual protocol, Alice's task is to guess the outcome of the X basis measurement on the j^{th} virtual qubit. The position of the j^{th} virtual qubit is randomly chosen from the $L-1$ virtual qubits according to Eq. (3). Then, the phase error rate is defined as a fraction that Alice obtains the measurement outcome $-$ in her X basis measurement on her j^{th} virtual qubit that is randomly chosen from the $L-1$ virtual qubits. In the phase error rate estimation, we consider the worst case scenario that if the total photon number contained in the L pulses exceeds ν_{th}, Bob surely detects such an event as a successful detection, and Alice obtains the measurement outcome $-$ on her j^{th} virtual qubit. By combining this worst case scenario and thanks to the randomness of j from Eq. (3), the phase error rate is given by

$$e_{\mathrm{ph}} = e_{\mathrm{src}}/Q + (1 - e_{\mathrm{src}}/Q)n^{-}/(L-1), \tag{6}$$

where n^{-} denotes the number of virtual qubits resulted in the measurement outcome of $-$ among the $L-1$ virtual qubits.

In the following, we explain how to estimate the upper bound on n^{-}. Here, we use the fact that the statistics of the X basis measurement on system virA is not affected by any operations conducted on system B. Therefore, in order to estimate the upper bound on n^{-}, we are allowed to perform the photon number measurement (PNM) on all the $L-1$ sending pulses in system B in Eq. (2). This PNM is an off-line measurement, and is not performed in either of the actual and virtual protocols. Let us denote by n_u and $\mathrm{M}_X^{(u)} \in \{+,-\}$ the outcome of the PNM of the u^{th} $(1 \leqslant u \leqslant L-1)$ sending pulse and the X basis measurement outcome performed on Alice's u^{th} virtual qubit, respectively. From these measurement results $n_1,\ldots,n_{L-1}$, we estimate the upper bound on n^{-}. For later convenience, we decompose n^{-} into

$$n^{-} = n_{\mathrm{nonvac}}^{-} + n_{\mathrm{vac}}^{-}, \tag{7}$$

where n_{nonvac}^{-} (n_{vac}^{-}) denotes the number of u that satisfies $n_u > 0$ $(n_u = 0)$ and $\mathrm{M}_X^{(u)} = -$.

Now, we calculate the upper bound on Eq. (7). First, we consider upper bounding n_{nonvac}^{-}. In so doing, we consider two worst case scenarios. The first worst case scenario is that if the u^{th} sending state includes more than zero photon (i.e., $n_u > 0$), we regard $\mathrm{M}_X^{(u)}$ as $-$. The second one is that ν_{th} photons are distributed over the $L-1$ pulses such that the number of pulses that contain no photon is minimized. With these two worst case scenarios, n_{nonvac}^{-} is upper bounded by

$$n_{\mathrm{nonvac}}^{-} \leqslant n_{\mathrm{nonvac}} \leqslant \nu_{\mathrm{th}}, \tag{8}$$

where n_{nonvac} denotes the number of u that satisfies $n_u > 0$ among the $L-1$ pulses. In Eq. (8), the first and the second inequalities are due to the first and the second worst case scenarios, respectively.

Next, we show the upper bound on n_{vac}^{-}, which is given by (see Sec. III in the Supplemental Material for details)

$$n_{\mathrm{vac}}^{-} = 0 \quad \big[\text{if } p_0^{(k)}(0) = p_1^{(k)}(0) \quad \text{holds for all } k(1 \leqslant k \leqslant L)\big], \tag{9}$$

$$\begin{aligned} n_{\mathrm{vac}}^{-} &\leqslant \frac{L-1-\nu_{\mathrm{th}}}{2}\max\left\{\frac{(\sqrt{p_{\mathrm{U},0}(0)} - \sqrt{p_{\mathrm{L},1}(0)})^2}{p_{\mathrm{U},0}(0)+p_{\mathrm{L},1}(0)}, \times \frac{(\sqrt{p_{\mathrm{L},0}(0)} - \sqrt{p_{\mathrm{U},1}(0)})^2}{p_{\mathrm{L},0}(0)+p_{\mathrm{U},1}(0)}\right\} + \max_{N_{\mathrm{vacd}}}\{N_{\mathrm{vacd}}t\} \\ &=: n_{\mathrm{vac,U}}^{-} \quad \big[\text{if } p_0^{(k)}(0) \neq p_1^{(k)}(0) \quad \text{for some or every } k\big], \end{aligned} \tag{10}$$

where $1 \leqslant N_{\mathrm{vacd}} \leqslant L-1-\nu_{\mathrm{th}}$ and $0 < t$. Note that N_{vacd} and t are related to a failure probability ϵ (see Eq. (17) in the Supplemental Material) of the Chernoff bound [38]. Below, we explain the above results in more detail.

(i) The first case is that $p_0^{(k)}(0) = p_1^{(k)}(0)$ is satisfied for all k $(1 \leqslant k \leqslant L)$. From Eq. (5), we obtain $p_{-}^{(k)}(0) = 0$, and hence $n_{\mathrm{vac}}^{-} = 0$. This means that if $n_u = 0$, $\mathrm{M}_X^{(u)}$ is $+$ and never $-$. By combining the results in Eqs. (8) and (9), the phase error rate is upper bounded by

$$e_{\mathrm{ph}} \leqslant \min\left\{\frac{e_{\mathrm{src}}}{Q} + \left(1 - \frac{e_{\mathrm{src}}}{Q}\right)\frac{\nu_{\mathrm{th}}}{L-1}, 0.5\right\}. \tag{11}$$

Note that this upper bound is exactly the same as the one in the original security proof [21].

(ii) The second case is that $p_0^{(k)}(0) \neq p_1^{(k)}(0)$ occurs for some or every k. First, we give an example of how this situation arises. Suppose that Eve performs a THA where she injects a strong pulse into Alice's source to obtain some information on the source from the back-reflected light. To prevent this THA, Alice needs to suppress the intensity of the back-reflected light, which can be accomplished by installing some optical filters or optical isolators [31]. However, one cannot perfectly suppress the intensity, and moreover, optical components, such as phase modulators, may have polarization dependence [39], which leads to the situation of $p_0^{(k)}(0) \neq p_1^{(k)}(0)$. This means that even if $n_u = 0$, we cannot conclude $\mathrm{M}_X^{(u)} = +$.

Therefore, n^{-}_{vac} results in a nonzero value, and e_{ph} is increased compared with the one in case (i). In case (ii), by combining Eqs. (8) and (10), the phase error rate can be obtained as

$$e_{\mathrm{ph}} \leqslant \min\left\{\frac{p_{\mathrm{err}}}{Q} + \left(1 - \frac{p_{\mathrm{err}}}{Q}\right)\frac{\nu_{\mathrm{th}} + n^{-}_{\mathrm{vac,U}}}{L-1}, 0.5\right\}. \quad (12)$$

Here, we define $p_{\mathrm{err}} := e_{\mathrm{src}} + \epsilon - e_{\mathrm{src}}\epsilon$.

We emphasize that the phase error rates given in Eqs. (11) and (12) are derived only from the three assumptions: A1, A2, and A3. This property is one of the striking features of the RRDPS protocol because other protocols usually need more detailed specifications of imperfections [28,30] and Eve's side-channel attacks on the source [31]. In particular, the practical QKD systems are threatened by the THA [40], and the recent work quantitatively shows that the key generation rate of the BB84 protocol is compromised by this attack [31]. More specifically, [31] shows that when the mean photon number of the back-reflected light is $\mu_{\mathrm{out}} = 10^{-2}$, the achievable distance of the secure key generation is decreased down to only 10 km, while it is about 150 km without the THA. The reason for this drastic degradation is that the phase error rate is exponentially increasing with the distance [37]. In the RRDPS protocol, however, even if Eve performs the THA with $\mu_{\mathrm{out}} = 10^{-2}$, the increase of ν_{th} is only about $L\mu_{\mathrm{out}}$. Therefore, the increase of e_{ph} (e.g., $L = 100$) is about $L\mu_{\mathrm{out}}/(L-1) \sim 1\%$ regardless of the distance, implying that only a small amount of the additional privacy amplification is needed. This shows the robustness that the RRDPS has against the side-channel attacks on the source.

Based on the above security proof, we show the key generation rate simulation results for cases (i) and (ii). In the simulation, we assume that Alice uses a weak coherent light source with the mean photon number $\mu_{0(1)}$ when she chooses the bit 0(1) [41]. We set the channel transmittance as $\eta_{\mathrm{ch}} = 10^{-0.2l/10}$. In the detection side, we assume the detection efficiency and the dark count probability as $\eta_{\mathrm{d}} = 0.15$ and $p_{\mathrm{d}} = 5 \times 10^{-7}$, respectively. With these parameters, the successful detection probability that Bob detects the single photon and the bit error rate are assumed to be given by $Q = (L\mu_0\eta_{\mathrm{sy}})e^{-L\mu_0\eta_{\mathrm{sy}}}/2 + Lp_{\mathrm{d}}$ and $e_{\mathrm{bit}} = (L\mu_0\eta_{\mathrm{sy}}e^{-L\mu_0\eta_{\mathrm{sy}}}e_{\mathrm{sym}}/2 + Lp_{\mathrm{d}}/2)/Q$, respectively. Here, $\eta_{\mathrm{sy}} := \eta_{\mathrm{ch}}\eta_{\mathrm{d}}$, and e_{sym} is an overall misalignment error of the optical system, and we assume that e_{sym} is 5%. Also, we set f_{EC} as 1.16.

First, we show the simulation result for case (i). In this case, the mean photon numbers for both bits are the same $\mu_0 = \mu_1 =: \mu$. Under the above conditions, we plot the key rate R with $L = 128$ by the solid line in Fig. 1, where R is optimized over the choice of μ and ν_{th} through the relation $e_{\mathrm{src}} = 1 - \sum_{n=0}^{\nu_{\mathrm{th}}} e^{-L\mu}(L\mu)^n/n!$.

Next, we show the simulation result for case (ii). We assume that μ_1 lies in the range $R_1 := [0.99\mu_0, 1.01\mu_0]$. In this case, the upper and the lower bounds on $p^{(k)}_{0(1)}(0)$ are given by $p_{\mathrm{U},0}(0) = e^{-\mu_0}$ $[p_{\mathrm{U},1}(0) = e^{-0.99\mu_0}]$ and $p_{\mathrm{L},0}(0) = e^{-\mu_0}$ $[p_{\mathrm{L},1}(0) = e^{-1.01\mu_0}]$, respectively. Under these conditions, we plot the key rate R with $L = 128$ by the dashed line in Fig. 1, where R is optimized over the choice of μ_0, ν_{th}, and ϵ through the relation $e_{\mathrm{src}} = 1 - \min_{\gamma\in R_1}\{\sum_{n=0}^{\nu_{\mathrm{th}}} e^{-L\gamma}(L\gamma)^n/n!\}$. This dashed line shows that even if $p^{(k)}_0(0) \neq p^{(k)}_1(0)$ occurs for some or every k, the degradation of the key generation rate is not so compromised. This result also shows the robustness of the RRDPS protocol against source flaws.

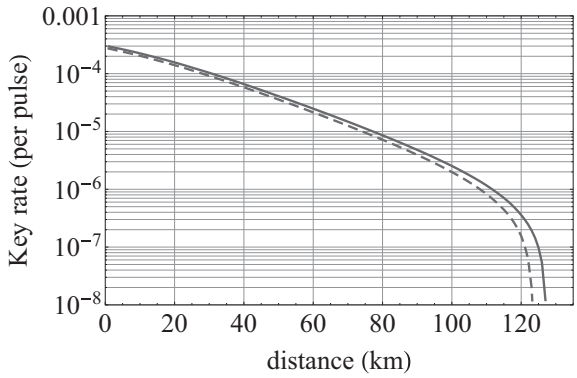

FIG. 1. Secret key rate R per pulse versus distances l. The solid line is for case (i): $p^{(k)}_0(0) = p^{(k)}_1(0)$ is satisfied for all k, and the dashed line is for case (ii): $p^{(k)}_0(0) \neq p^{(k)}_1(0)$ occurs for some or every k.

To conclude, we have shown the security of the RRDPS protocol with imperfect light sources and side-channel attacks on Alice's source. In our security analysis, the characterization of Alice's source is simple in the sense that if Alice monitors only ν_{th}, the vacuum emission probability and the independence among the sending states, the amount of privacy amplification needed can be obtained. This means that the security of the RRDPS protocol can be guaranteed without detailed specifications of the source imperfections and side-channel attacks on the source. Moreover, we found that if the probabilities of emitting the vacuum state are the same for both bits, the phase error rate is exactly the same as the one in the original paper [21]. Even if these probabilities differ, the performance of the key generation rate is not significantly compromised. These results show that the RRDPS protocol is highly robust against imperfections and side-channel attacks on the source, which is another practical advantage that this protocol has over other protocols.

The authors thank H.-K. Lo, M. Koashi, H. Takesue, T. Sasaki, T. Yamamoto, K. Azuma, L. Qian, R. Ikuta, S. Kawakami, and G. Kato for fruitful discussions. A.M. and N.I. acknowledge support from the JSPS Grant-in-Aid for Scientific Research(A) 25247068. This work was in part funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan).

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

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[5] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[6] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[7] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022.
[8] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[11] H.-K. Lo, arXiv:quant-ph/0102138.
[12] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[13] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[14] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
[15] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, arXiv:0804.0891.
[16] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).
[17] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[18] K. Tamaki, M. Koashi, and G. Kato, arXiv:1208.1995v1.
[19] T. Moroder, M. Curty, Charles Ci Wen Lim, L. P. Thinh, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **109**, 260501 (2012).
[20] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[21] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).
[22] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, arXiv:1505.02481v1.
[23] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[24] J.-Y. Guan, Z. Cao, Y. Liu, G. L. Shen-Tu, J. S. Pelc, M. N. Fejer, C. Z. Peng, X. Ma, Q. Zhang, and J. W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).
[25] Y.-H. Li *et al.*, arXiv:1505.08142.
[26] S. Wang *et al.*, Nat. Photonics **9**, 832 (2015).
[27] M. Tomamichel and A. Leverrier, arXiv:1506.08458.
[28] X.-B. Wang, C. Z. Peng, J. Zhang, L. Yang, and J. W. Pan, Phys. Rev. A **77**, 042311 (2008).
[29] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012); M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[30] K. Tamaki, M. Curty, G. Kato, H. K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014); A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).
[31] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).
[32] Z.-Q. Yin, Chi-Hang Fred Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **88**, 062322 (2013).
[33] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.92.060303 for detailed calculations and other details.
[34] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[35] M. Koashi, arXiv:quant-ph/0505108.
[36] R. Renner, Ph.D. thesis, ETH Zurich, 2005, arXiv:quant-ph/0512258.
[37] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[38] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952).
[39] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H. K. Lo, Phys. Rev. A **92**, 032305 (2015).
[40] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).
[41] Note that the phase of the coherent light needs not to be randomized.