Optimal decoy intensity for decoy quantum key distribution

Masahito Hayashi

Graduate School of Mathematics, Nagoya University, Furocho, Chikusa-ku, Nagoya, 464-860, Japan
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore

E-mail: masahito@math.nagoya-u.ac.jp

Received 19 July 2015, revised 5 January 2016
Accepted for publication 3 February 2016
Published 8 March 2016

Abstract
In the decoy quantum key distribution, we show that a smaller decoy intensity gives a better key generation rate in the asymptotic setting when we employ only one decoy intensity and the vacuum pulse. In particular, the counting rate of single photon can be perfectly estimated in the limit that the decoy intensity is infinitesimally small. The same property holds even when the intensities cannot be perfectly identified. Further, we propose a protocol to improve the key generation rate over the existing protocol under the same decoy intensity.

Keywords: quantum key distribution, decoy method, BB84 protocol, optimal key generation rate

1. Introduction
Quantum key distribution (QKD) by BB84 protocol [1] is one of the most important applications of quantum information. The original QKD requires the single photon source. However, many economically realizable photon sources produce only weak coherent pulses. In weak coherent pulses, the photon number does not take the fixed value, and obeys the Poisson distribution. Usually, the average of the the photon number of the weak coherent pulse is called the intensity of the weak coherent pulse [3–8, 10, 11, 13, 23, 24]. In particular, when we make phase randomization properly, the state with the weak coherent pulse can be characterized by the Poisson mixture of the number states whose average number is the intensity. Hence, we assume the phase randomization in this paper. So, even if we identify the intensity, the photon number has fluctuation. Therefore, we cannot use the original QKD protocol with weak coherent pulse. To solve this problem, we need to estimate the detection rate of the single photon pulse.
Hwang [21] proposed the decoy method, in which, we estimate the detection rate of the single photon pulse from the detection rates of the weak coherent pulses with different intensities. As another solution, continuous variable QKD works with weak coherent pulses. (See [21] and references therein.) While continuous variable QKD can be implemented with an inexpensive Homodyne detection, the decoy method with BB84 protocol can achieve the longest distance with the current technology [14, 15]. So, it is natural to focus on the decoy method.

In the decoy method, we employ two kinds of weak coherent pulses; one is the signal pulse, which generates raw keys. The other is the decoy pulse, which is used only for the estimation of the detection rate of the single photon pulse. The key point is the difference between the signal and decoy intensities \( \mu_s \) and \( \mu_d \), which are the intensities of the signal and decoy pulses. Using the detection rates of these pulses, the decoy method determines a lower bound of the detection rate of single photon pulse. However, it cannot uniquely determine this detection rate although it has been improved by many researchers [3–11]. To improve this estimation, the papers [7, 8] proposed to increase the number of the decoy intensities, and showed that this detection rate can be uniquely determined when the number of the decoy intensities is infinitely large. However, it strains the network system of QKD to increase the number of decoy intensities. So, it is better to realize a precise estimation without increase of this number.

This paper focuses on the case when we employ only one decoy intensity \( \mu_d \) and the vacuum pulse for the estimation of the detection rate of single photon pulse. Firstly, we consider a formula for secure key generation rate that is different from the conventional one. Indeed, while the paper [18] discussed a similar key generation rate formula of finite-length setting, it did not discuss the asymptotic formulas. Although finite-length analysis is needed in the real setting, the asymptotic analysis is more useful for rough estimation because it brings us more analytic and non-trivial formulas. This paper derives the asymptotic version of the key generation rate given in [18]. Then, we show how better our formula is than the conventional one although the paper [18] could not clarify this improvement because it focuses on the finite-size effect. Secondly, we optimize the choice of the decoy intensity. This kind of optimization for the conventional formula for the asymptotic key generation rate has been done by Ma et al [5] when the source intensities are perfectly controlled. We derive the same optimization for our improved formula for the asymptotic key generation rate.

However, as was discussed by Wang et al [10, 11], there is a possibility that the true intensity is different from our setup value within a certain range while the intensity takes a fixed value. This situation is natural in practice because the error of the intensity takes a fixed value even though it cannot be identified perfectly when the beam splitter is well installed. Hence, it is needed to extend the decoy method to such a practical setting. Then, extending the obtained analysis to the practical case, we still have the same conclusion. On the other hand, Ma et al [5] also considered a similar optimization for the conventional formula for the asymptotic key generation rate when the source intensities have statistical fluctuation. Their situation corresponds to the case when the beam splitter is not well installed. Hence, as explained in the second paragraph of section 3, our analysis is different for their analysis.

The remaining part of this paper is organized as follows. Section 2 discusses the decoy method when the source intensities are controlled. Then, we explain our improved formula for the asymptotic key generation rate. We derive the optimal decoy intensity of this case. Section 3 extends the above result to the case when the source intensities cannot be perfectly identified. Section 4 discusses the relation of the obtained result with the finite-length case [18]. Several proofs are given in appendixes.
2. Controlled source intensities

First, we discuss the case when the source intensities are controlled. To discuss this case, we recall the improved GLLP formula \[12, 13\]. When we distill the secure key from given \[M\]-bits raw key in the bit basis from the signal pulse, we firstly apply error correction and then obtain the \[M\] s, \(e_{s,+}\) bits corrected key, where \(e_{s,+}\) is the error rate in the bit basis of the signal pulse. Here, \(h\) is the binary entropy with the logarithm to the base 2 and the parameter \(\eta\) is the efficiency of error correction, which is chosen to be 1.1 in a realistic case and to be 1 in the ideal case. The next step, the privacy amplification, requires the ratio \(p : q : r\) of the vacuum pulse, the single photon pulse, and the multi-photon pulse among the received pulses. When the error rate of the phase basis in the single photon pulse is \(e_s\), it is enough to apply universal2 hash functions sacrificing \(q h(e_s)\) bits \[22–24\]. Hence, we can obtain \((1 - \eta h(e_{s,+}) - q h(e_s) - r)M\) bits of secure key. That is, the secure key generation rate per received pulse with the matched basis is

\[
\frac{(p_0 + a \mu_s (1 - h(e_s))) e^{-\mu_s}}{p_{s,+}} = \eta h(e_{s,+}).
\]

However, the rate \(a\) and the phase error rate \(e_s\) cannot be directly measured although \(p_0\) can be directly measured by transmitting the vacuum pulse.

The decoy method enables us to estimate the quantities \(a\) and \(e_s\) by using the above measurable values and the detection rates \(p_{s,+}\) of the signal and decoy pulses with the phase basis, and the error rates \(e_{s,x}\) and \(e_{d,x}\) of the signal and decoy pulses with the phase basis. These rates can be measured by randomizing the basis and the intensity. Here, we need to explain the detail of our protocol. Since we consider the asymptotic case, we do not need to care about the ratio among the numbers of the signal pulses, the decoy pulses, and the vacuum pulses as long as these numbers are infinitely large. Hence, it is allowed to choose the numbers of the decoy pulses and the vacuum pulses are negligible under this condition. For example, such a condition is satisfies when the numbers of the decoy pulses and the vacuum pulses are the square root of the number of signal pulses when this number is sufficiently large.

In the existing method \[4–8\], they derive the estimate \(\hat{a}\) of the detection rate \(a\) of single-photon pulse and the estimate \(\hat{b}\) of the rate \(b\) that the single-photon pulse is detected with the phase error as follows

\[
\hat{a}(p_{d,x}, p_{s,x}):= \left[\frac{\mu_d^2 e^{\mu_s}(p_{d,x} - p_0 e^{-\mu_s}) - \mu_d^2 e^{\mu_d}(p_{s,x} - p_0 e^{-\mu_d})}{\mu_d \mu_s (\mu_s - \mu_d)}\right],
\]

\[
\hat{b}(e_{d,x}, p_{d,x}):= \left[\frac{e_{d,x} p_{d,x} e^{\mu_d} - p_0/2}{\mu_d}\right].
\]
where we assume that $\mu_d < \mu_i$. The above estimates of the case $\mu_d > \mu_i$ can be derived by exchanging the roles of the decoy and signal pulses in the right-hand side. The key point of the derivation of (2) and (3) is the following expansions of the states of the decoy and signal pulses:

$$\sum_{n=0}^{\infty} e^{-\mu_d} \frac{\mu_d^n}{n!} |n\rangle = e^{-\mu_d} |0\rangle + e^{-\mu_s} \mu_d |1\rangle + (1 - (1 + \mu_d) e^{-\mu_d}) \rho_2,$$

and

$$\sum_{n=0}^{\infty} e^{-\mu_s} \frac{\mu_s^n}{n!} |n\rangle = e^{-\mu_s} |0\rangle + e^{-\mu_d} \mu_s |1\rangle + \beta_2 \rho_2 + \beta_3 \rho_3,$$

where the state $\rho_3$ is chosen properly. The estimate $\hat{a}$ in (2) is derived from the non-negativity of the detection rate $\alpha_3$ of the state $\rho_3$, and the estimate $\hat{b}$ in (3) is from the non-negativity of the rate that the pulse with the state $\rho_2$ is detected with the phase error. Substituting $\hat{a}$ and $\hat{b}$ into $a$ and $e_\infty$ of the formula (1), we obtain the key generation rate.

In this paper, instead of $\hat{a}$, we estimate the rate $c$ that the single-photon pulse is detected without the phase error. Since a smaller $c$ gives a better case, we can estimate $c$ in the same way as the detection rate $a$. Then, we obtain the estimate $\hat{c}$ as

$$\hat{c}(p_{a,s}, p_{e,s}, e_{a,s}) := \left[ \frac{\mu_s^2 e^{\mu_s}((1 - \mu_s - p_0 e^{-\mu_s})/2)}{\mu_d \mu_s (\mu_s - \mu_d)} - \frac{\mu_d^2 e^{\mu_d}((1 - e_{a,s} - p_0 e^{-\mu_d})/2)}{\mu_d \mu_s (\mu_s - \mu_d)} \right],$$

which is derived from the non-negativity of the rate $c_3$ that the pulse with the state $\rho_3$ is detected without the phase error. Since the rate $c_3$ is smaller than the rate $\alpha_3$, the non-negativity of $c_3$ is a stronger constraint than that of $\alpha_3$. So, the estimate $\hat{c}$ in (4) is better than the estimate given in (2). Therefore, substituting $\hat{c} + \hat{b}$ and $\frac{\hat{b}}{\hat{a} + \hat{c}}$ into $a$ and $e_\infty$ of the formula (1), we obtain a better key generation rate. Indeed, since the difference between our method and the conventional one is the calculation formula for the leaked information, our method requires the same device as the conventional one. So, there is no disadvantage of our method.

Now, we consider the case with no eavesdropper, i.e., the case when the true intensities coincide with our intent intensities. In the QKD theory, although we consider the protocol that works with the presence of eavesdropper, we usually evaluate the key generation rate of the protocol when there is no eavesdropper [3–8, 10, 11, 13, 23, 24]. In the following, the subscript $s$ expresses the signal pulse, and the subscript $d$ expresses the decoy pulse. Then, we adopt the following model for the detection rates $p_{e,s,d}$ and the error rates $e_{i,s,d}$ with the parameters $\alpha$ and $\gamma$ [16, 17]:

$$p_{i,s} = p_{i,d} = 1 - e^{-\alpha \mu_i} + p_0 e^{-\alpha \mu_i},$$

$$e_{i,s,d} = e_{i,s,d} = \gamma (1 - e^{-\alpha \mu_i}) + \frac{p_0}{2} e^{-\alpha \mu_i}, \quad i = s, d,$$

where $\alpha$ is the total transmission including quantum efficiency of the detector, and $\gamma$ is the error due to the imperfection of the optical system.

Under this assumption, we estimate the detection rate $a$ of the single photon pulse, the rate $b$ that the single-photon pulse is detected with the phase error, and the rate $c$ that the single-photon pulse is detected without the phase error. By letting $\mu_2$ be the larger intensity of $\mu_s$ and $\mu_d$ is and $\mu_1$ be the smaller one, their estimates $\hat{a}$, $\hat{b}$, and $\hat{c}$ are given as
\[ \hat{\alpha}(\mu_1, \mu_2) = \frac{\mu_2^2 e^{\mu_2}((1 - e^{-\mu_1}) + p_0 (e^{-\mu_1} - e^{-\mu_2}) - \mu_1^2 e^{\mu_1}((1 - e^{-\mu_1}) + p_0 (e^{-\mu_1} - e^{-\mu_2}))}{\mu_1 \mu_2 (\mu_2 - \mu_1)} \]
\[ = (\mu_2 \mu_1) \frac{e^{\mu_1} - (1 - p_0) e^{(1 - \gamma) \mu_1} - p_0}{\mu_1^2} \]
\[ \hat{b}(\mu_1) = \frac{\gamma (1 - e^{-\mu_1}) e^{\mu_1} + \frac{p_0}{2} (e^{(1 - \gamma) \mu_1} - 1)}{\mu_1} \]
\[ = (\mu_2 \mu_1) \frac{e^{\mu_1} - (1 - \gamma - p_0/2) e^{(1 - \gamma) \mu_1} - \frac{p_0}{2}}{\mu_1^2} \]
\[ \hat{c}(\mu_1, \mu_2) = \frac{\mu_2^2 e^{\mu_2}((1 - \gamma)(1 - e^{-\mu_1}) + \frac{p_0}{2} (e^{-\mu_1} - e^{-\mu_2}))}{\mu_1 \mu_2 (\mu_2 - \mu_1)} \]
\[ - \frac{\mu_1^2 e^{\mu_1}((1 - \gamma)(1 - e^{-\mu_1}) + \frac{p_0}{2} (e^{-\mu_1} - e^{-\mu_2}))}{\mu_1 \mu_2 (\mu_2 - \mu_1)} \]
\[ = (\mu_2 \mu_1) \frac{(1 - \gamma) e^{\mu_1} - (1 - \gamma - p_0/2) e^{(1 - \gamma) \mu_1} - \frac{p_0}{2}}{\mu_1^2} \]
\[ \times \frac{e^{\mu_1} - (1 - p_0) e^{(1 - \gamma) \mu_1} - p_0}{\mu_1^2} \]

By using these estimates, the key generation rates \( R(\mu_s, \mu_d) \) and \( \hat{R}(\mu_s, \mu_d) \) per transmitted pulse with the matched basis are written as

\[ R(\mu_s, \mu_d) = \begin{cases} 
\mu_s e^{-\mu_s} (\hat{c}(\mu_d, \mu_s) + \hat{b}(\mu_d)) \left( 1 - \frac{\hat{b}(\mu_s)}{\hat{c}(\mu_s, \mu_s) + \hat{b}(\mu_s)} \right) & \text{if } \mu_s < \mu_d, \\
\mu_s e^{-\mu_s} (\hat{c}(\mu_d, \mu_s) + \hat{b}(\mu_s)) \left( 1 - \frac{\hat{b}(\mu_s)}{\hat{c}(\mu_s, \mu_s) + \hat{b}(\mu_s)} \right) + e^{-\mu_s} p_0 - p_s + \eta \phi \left( \frac{\epsilon_s}{\rho_s} \right) & \text{if } \mu_s > \mu_d.
\end{cases} \]

\[ \hat{R}(\mu_s, \mu_d) = \begin{cases} 
\mu_s e^{-\mu_s} \hat{\alpha}(\mu_d, \mu_s) \left( 1 - \frac{\hat{b}(\mu_s)}{\hat{c}(\mu_s, \mu_s) + \hat{b}(\mu_s)} \right) + e^{-\mu_s} p_0 - p_s + \eta \phi \left( \frac{\epsilon_s}{\rho_s} \right) & \text{if } \mu_s < \mu_d, \\
\mu_s e^{-\mu_s} \hat{\alpha}(\mu_s, \mu_d) \left( 1 - \frac{\hat{b}(\mu_s)}{\hat{c}(\mu_s, \mu_s) + \hat{b}(\mu_s)} \right) + e^{-\mu_s} p_0 - p_s + \eta \phi \left( \frac{\epsilon_s}{\rho_s} \right) & \text{if } \mu_s > \mu_d.
\end{cases} \]

Then, we obtain the following lemma, which will be shown in appendix A.
Lemma 1. \((\hat{c}(\mu_1, \mu_2) + \hat{b}(\mu_1)) \left(1 - h\left(\frac{\hat{b}(\mu_1)}{\hat{c}(\mu_1, \mu_2) + \hat{b}(\mu_1)}\right)\right)\) is monotonically decreasing for \(\mu_1\) and \(\mu_2\) when \(\frac{\hat{b}(\mu_1)}{\hat{c}(\mu_1, \mu_2) + \hat{b}(\mu_1)} < \frac{1}{2}\). Similarly, \((\hat{a}(\mu_1, \mu_2) \left(1 - h\left(\frac{\hat{b}(\mu_1)}{\hat{a}(\mu_1, \mu_2)}\right)\right)\) is monotonically decreasing for \(\mu_1\) and \(\mu_2\) when \(\frac{\hat{b}(\mu_1)}{\hat{a}(\mu_1, \mu_2)} < \frac{1}{2}\).

Now, we fixed a signal intensity to be \(\mu_s\). Then, lemma 1 implies
\[
R(\mu_s, \mu_1) \geq R(\mu_s, \mu_2) \geq R(\mu_s, \mu_3) \geq R(\mu_s, \mu_4)
\]
for \(\mu_1 < \mu_2 < \mu_s < \mu_3 < \mu_4\). These inequalities imply that a smaller decoy intensity has a better key generation rate when the signal intensity is fixed. The same relation holds for \(\tilde{R}(\mu_s, \mu_4)\). Therefore, we obtain the following theorem.

Theorem 2. \(\tilde{R}(\mu_s, \mu_4)\) and \(R(\mu_s, \mu_4)\) are monotonically decreasing with respect to \(\mu_3\) for a given \(\mu_s\).

Note that although the argument for \(\tilde{R}(\mu_s, \mu_4)\) in theorem 2 was shown in [5], that for \(R(\mu_s, \mu_4)\) was not shown in [5]. This theorem implies that a smaller decoy intensity yields a larger key generation rate. Here, we should remark that we cannot choose the decoy pulse to be the vacuum pulse because we need the infinitesimal small difference between the decoy pulse and the vacuum pulse. Dependent on this difference, we observe the infinitesimal small differences for their detection rates and their error rates. Using the ratios between these differences, we can estimate the amount of leaked information. That is, this infinitesimal small difference is essential for this estimation.

In particular, the limit of the key generation rate is given in the limit that the decoy intensity is infinitesimally small. Then, the following lemma holds, which will be shown in appendix A.

Lemma 3. We also obtain
\[
\lim_{\mu_1 \to 0} \hat{c}(\mu_1, \mu_2) = (1 - \gamma)\alpha + \frac{p_0}{2},
\]
\[
\lim_{\mu_1 \to 0} \hat{b}(\mu_1) = \gamma\alpha + \frac{p_0}{2},
\]
\[
\lim_{\mu_1 \to 0} \hat{a}(\mu_1, \mu_2) = \alpha + p_0.
\]

Substituting the above in (9) and (10), we have
\[
\lim_{\mu_3 \to 0} R(\mu_s, \mu_4) = \lim_{\mu_3 \to 0} \tilde{R}(\mu_s, \mu_4)
\]
\[
\mu_4 e^{-\mu_4} (\alpha + p_0) \left(1 - h\left(\frac{\alpha\gamma + \frac{p_0}{2}}{\alpha + p_0}\right)\right) + e^{-\mu_4} p_0
\]
\[
- (1 - e^{-\alpha\mu_4} + p_0) h\left(1 - e^{-\alpha\mu_4} + \frac{p_0}{2}\right).
\]
That is, in the limit $\mu_d \to 0$, we can perfectly estimate the parameters $a$, $b$, and $c$. Since the signal intensity is related to the detection rate of the signal pulse and other factors, it is not so simple to find the optimal signal intensity.

### 3. Uncontrolled source intensities

Next, we consider the case when we cannot perfectly identify the true intensities $s_m$ and $d_m$. Similar to Wang et al [10, 11], we assume that the true intensities $\mu_i$ and $\tilde{\mu}_d$ belong to certain intervals $[(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]$ and $[(1 - \epsilon)\tilde{\mu}_d, (1 + \epsilon)\tilde{\mu}_d]$ with the error ratio $\epsilon > 0$, respectively. In this case, we have to consider the worst case with respect to the true intensities $\mu_i$ and $\tilde{\mu}_d$ in the intervals $[(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]$ and $[(1 - \epsilon)\tilde{\mu}_d, (1 + \epsilon)\tilde{\mu}_d]$, respectively. Indeed, the smaller intensity pulse is generated by the combination of the stronger pulse and beam splitter. If the beam splitter is well installed, the error only comes from the error of the stronger pulse source. In this assumption, the error ratio $\epsilon$ does not depend on the intensity.

Here, we should remark the relation with the setting in Ma et al [5]. They studied the case with the statistical fluctuation of the measurement outcomes [5, section IV]. However, we assume the source intensity is fixed but is different from our intent, and infinitely large data is available. That is, in our setting, there is no statistical fluctuation in our data. Hence, our model is simpler than their model. Although they could not obtain an analytical result in their model [5, section IV], we derive an analytical result in our model as follows.

Now, we treat the typical case when true intensities are $\tilde{\mu}_1$ and $\tilde{\mu}_2$ and there is no eavesdropper. Instead of (5), we assume that

$$p_{h,+} = p_{h,\times} = 1 - e^{-\alpha \tilde{\mu}_i} + p_0 e^{-\alpha \tilde{\mu}_i},$$  \hspace{1cm} (14)

$$e_{i,+} p_{h,+} = e_{i,-} p_{h,\times} = \gamma (1 - e^{-\alpha \tilde{\mu}_i}) + \frac{p_0}{2} e^{-\alpha \tilde{\mu}_i},$$  \hspace{1cm} (15)

for $i = s$, $d$. When we consider that the true signal and decoy intensities are $\mu_i$ and $\tilde{\mu}_d$, the detection rate of the single photon pulse is $a$, the rate that the single-photon pulse is detected with the phase error is $b$, and the rate that the single-photon pulse is detected without the
phase error is $c$, the two key generation rates are given as
\begin{align}
\hat{R} &= \left(p_0 + a_\mu \left(1 - h \left(\frac{b}{a}\right)\right)\right)e^{-\mu_1} - p_{\mu_1} + \eta h(\epsilon_{\mu_1}),
\end{align}
\begin{align}
R &= \left(p_0 + (b + c)\mu \left(1 - h \left(\frac{b}{b + c}\right)\right)\right)e^{-\mu_1} - p_{\mu_1} + \eta h(\epsilon_{\mu_1}).
\end{align}

Then, using the functions
\begin{align}
f_a(p_1, p_2, \mu_1, \mu_2) &= \begin{pmatrix} \mu_1^2 e^{\mu_1}(p_1 - p_0 e^{-\mu_1}) - \mu_2^2 e^{\mu_2}(p_2 - p_0 e^{-\mu_2}) \end{pmatrix},
\end{align}
\begin{align}
f_b(\gamma_1, \mu_1) &= \begin{pmatrix} \gamma_1 e^{\mu_1} - p_0 \end{pmatrix},
\end{align}
\begin{align}
f_c(p_1, p_2, \mu_1, \mu_2) &= \begin{pmatrix} \mu_1^2 e^{\mu_1}(p_1 - p_0 e^{-\mu_1}2) - \mu_2^2 e^{\mu_2}(p_2 - p_0 e^{-\mu_2}2) \end{pmatrix},
\end{align}
we can estimate the parameters $a, b,$ and $c$ as
\begin{align}
\hat{a} &= \begin{cases} f_a(p_{\mu_2}, p_{\mu_2}, \mu_2, \mu_2) & \text{if } \mu_2 < \mu_3, \\
 f_a(p_{\mu_2}, p_{\mu_2}, \mu_2, \mu_2) & \text{if } \mu_2 > \mu_3, \end{cases}
\end{align}
\begin{align}
\hat{b} &= \begin{cases} f_b(\epsilon_{\mu_2}, \mu_2) & \text{if } \mu_2 < \mu_3, \\
 f_b(\epsilon_{\mu_2}, \mu_2) & \text{if } \mu_2 > \mu_3, \end{cases}
\end{align}
\begin{align}
\hat{c} &= \begin{cases} f_c((1 - \epsilon_{\mu_2})p_{\mu_2}, (1 - \epsilon_{\mu_2})p_{\mu_2}, \mu_2) & \text{if } \mu_2 < \mu_3, \\
 f_c((1 - \epsilon_{\mu_2})p_{\mu_2}, (1 - \epsilon_{\mu_2})p_{\mu_2}, \mu_2) & \text{if } \mu_2 > \mu_3. \end{cases}
\end{align}

Thus, when we consider that the true signal and decoy intensities are $\mu_s$ and $\mu_d$, by using the above estimates $\hat{a}, \hat{b},$ and $\hat{c}$, the two key generation rates are given as
\begin{align}
R_s(\mu_s, \mu_d, \hat{\mu}_s, \hat{\mu}_d) &= \mu_s e^{-\mu_s}(\hat{c} + \hat{b}) \left(1 - h \left(\frac{\hat{b}}{\hat{c} + \hat{b}}\right)\right) + e^{-\mu_s}p_0 - p_{\mu_s} + \eta h(\epsilon_{\mu_s}),
\end{align}
\begin{align}
\hat{R}_s(\mu_s, \mu_d, \hat{\mu}_s, \hat{\mu}_d) &= \mu_s e^{-\mu_s} \hat{a} \left(1 - h \left(\frac{\hat{b}}{\hat{a}}\right)\right) + e^{-\mu_s}p_0 - p_{\mu_s} + \eta h(\epsilon_{\mu_s}).
\end{align}

Therefore, by taking the worst case, the key generation rates are given by
\begin{align}
\hat{R}_s(\hat{\mu}_s, \hat{\mu}_d, \epsilon) &= \min_{\mu_s \in [(1 - \epsilon)\hat{\mu}_s, (1 + \epsilon)\hat{\mu}_s], \mu_d \in [[1 - \epsilon)\hat{\mu}_d, (1 + \epsilon)\hat{\mu}_d]} \hat{R}_s(\hat{\mu}_s, \hat{\mu}_d, \mu_s, \mu_d),
\end{align}
\begin{align}
\hat{R}_s(\hat{\mu}_s, \hat{\mu}_d, \epsilon) &= \min_{\mu_s \in [(1 - \epsilon)\hat{\mu}_s, (1 + \epsilon)\hat{\mu}_s], \mu_d \in [[1 - \epsilon)\hat{\mu}_d, (1 + \epsilon)\hat{\mu}_d]} \hat{R}_s(\hat{\mu}_s, \hat{\mu}_d, \mu_s, \mu_d).
\end{align}

Indeed, it is quite difficult to find the values $\mu_s \in [(1 - \epsilon)\hat{\mu}_s, (1 + \epsilon)\hat{\mu}_s]$, $\mu_d \in [[1 - \epsilon)\hat{\mu}_d, (1 + \epsilon)\hat{\mu}_d]$ realizing the above minimums. However, our numerical demonstration (figure 2) suggests the following when $\epsilon > 0$ is sufficiently small. When $(1 + \epsilon)\hat{\mu}_d < (1 - \epsilon)\hat{\mu}_s$, $\mu_s = (1 + \epsilon)\hat{\mu}_d$ and $\mu_s = (1 - \epsilon)\hat{\mu}_d$ give the minimums. When $(1 + \epsilon)\hat{\mu}_s < (1 - \epsilon)\hat{\mu}_d$, $\mu_s = (1 + \epsilon)\hat{\mu}_s$ and $\mu_s = (1 - \epsilon)\hat{\mu}_d$ give the minimums. In the remaining case, we cannot distinguish two intensities. So, the decoy method does not work.
Indeed, as will be shown in theorem 4, \( \mu_d \) and \( \mu_s \) give the minimum \( R_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon) \) under the limit \( \tilde{\mu}_d \to 0 \).

As is numerically demonstrated in figure 3, \( R_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon) \) are not necessarily monotonically decreasing with respect to \( \tilde{\mu}_d \) when \( \tilde{\mu}_s < \tilde{\mu}_d \). However, our numerical analysis in figure 3, suggests that the maximums of \( R_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon) \) are realized by \( \tilde{\mu}_d \to 0 \) with fixed \( \tilde{\mu}_s \) and \( \epsilon > 0 \). This implication can be shown as the following theorem, which will be shown in appendix B.
Theorem 4. When a fixed intensity $\tilde{\mu}_s$ satisfies that
\[
\tilde{\mu}_s(1 + \epsilon) \leq 1 - \frac{p_0}{\left(\frac{1}{1 + \epsilon} + p_0\right)}(1 - h\left(\frac{\gamma + \frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}{\frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}\right)),
\]
equation number (21)
we obtain
\[
R_e(\tilde{\mu}_s, \epsilon) \equiv \sup_{\tilde{\mu}_d} \tilde{\mu}_s, \tilde{\mu}_d, \epsilon = \lim_{\tilde{\mu}_d \rightarrow 0} R_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon)
\]
\[
= \lim_{\tilde{\mu}_d \rightarrow 0} R_e(\tilde{\mu}_s, \tilde{\mu}_d, (1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_d)
\]
\[
= (1 - \epsilon)\tilde{\mu}_s e^{-(1-\epsilon)\tilde{\mu}_d} \left(\frac{\alpha}{1 + \epsilon} + p_0\right) \left(1 - h\left(\frac{\gamma + \frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}{\frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}\right)\right)
\]
\[
+ e^{-(1-\epsilon)\tilde{\mu}_d} p_0 - p_{k_e} \eta(e_{k_e}),
\]
equation number (22)
\[
\hat{R}_e(\tilde{\mu}_s, \epsilon) \equiv \sup_{\tilde{\mu}_d} \hat{R}_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon) = \lim_{\tilde{\mu}_d \rightarrow 0} \hat{R}_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon)
\]
\[
= \lim_{\tilde{\mu}_d \rightarrow 0} \hat{R}_e(\tilde{\mu}_s, \tilde{\mu}_d, (1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_d)
\]
\[
= (1 - \epsilon)\tilde{\mu}_s e^{-(1-\epsilon)\tilde{\mu}_d} \left(\frac{\alpha}{1 + \epsilon} + p_0\right) \left(1 - h\left(\frac{\gamma + \frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}{\frac{\alpha}{1 + \epsilon} + \frac{p_0}{2}}\right)\right)
\]
\[
+ e^{-(1-\epsilon)\tilde{\mu}_d} p_0 - p_{k_e} \eta(e_{k_e}).
\]
equation number (23)

This theorem implies that the infinitesimal small limit for the decoy intensity gives the limit of the key generation rate. Using this theorem, we numerically demonstrate $R_e(\tilde{\mu}_s, \epsilon)$ in figure 4. Then, we find the optimal signal intensity for our method as in table 1.
4. Relation with the finite-length case

However, in the realistic setting, we have to care about the length of our code. That is, we have to estimate the parameters $a$, $b$, and $c$ from the finite number of pulses. Such a case has been discussed in the recent paper [18]. Due to the analysis in [18], the errors of the estimates $a$, $b$, and $c$ become large when the decoy intensity is close to zero. So, we cannot say that a smaller decoy intensity is better in the real implementation. However, when the size of code is sufficiently large, we can expect that the contribution of such errors is not so large. To verify this implication, we numerically compare our asymptotic key generation rate $R_{0.5}(\bar{\mu}_d, s)$ with the rates given in [18] as figure 5. The numerical comparison suggests that the finite-length case has a trend similar to the asymptotic case. The paper [19] reports that privacy amplification has been implemented with the bit-length of raw keys up to $10^6$. However, there is a possibility to improve the method [19]. The forthcoming paper [20] will propose a new

| $\epsilon$ | $\bar{\mu}_d$ | $R_e$ |
|---------|-------------|-----|
| 0%      | 0.539 023   | 0.000 136 994 |
| 1%      | 0.539 212   | 0.000 133 318 |
| 3%      | 0.539 293   | 0.000 125 944 |
| 5%      | 0.535 419   | 0.000 119 117 |
| 10%     | 0.528 461   | 0.000 102 458 |

Table 1. The limit of the key generation rate $R_e(\bar{\mu}_d, +0, \epsilon)$, and the limit of the optimal signal intensities $\bar{\mu}_d$ when the decoy intensity $\bar{\mu}_d$ approaches to infinitesimal. Here, the parameter $\epsilon$ describes the error rate between the true intensities and our intents.

Figure 5. The horizontal axis expresses the decoy intensity $\mu_d$. The top blue graph describes the asymptotic key generation rate $R_{0.5}(\bar{\mu}_d)$ with the signal intensity 0.5. Other graphs describe the key generation rate with finite-length codes, in which, the number of each transmitted decoy pulses is one tenth of the number of the transmitted signal pulses. The bit-length of raw keys is chosen to be $10^6$ (red), $10^9$ (green), and $10^8$ (orange), from the second top to the bottom.
algorithm to realize secure hash functions. Combining the method [19] and the algorithm [20], the bit-length of raw keys was increased up to $10^9$ [25]. So, we can conclude that our asymptotic analysis has reflects the trends of realizable finite-length codes.

5. Conclusion

First, we have improved the decoy protocol when we employ only one decoy intensity and the vacuum pulse by introducing the new parameterization of the channel. Then, in both the existing method and our improved method, we have shown that a smaller decoy intensity gives a larger key generation rate in the asymptotic setting. Hence, the infinitesimal limit of the decoy intensity realizes the limit of the asymptotic key generation rate, and yields the perfect estimation of the counting rate and the phase error rate of the single photon pulse. We also verify the latter conclusion even when we cannot control or identify the intensities $\mu$ and $\mu$ by assuming an assumption similar to Wang et al [10, 11]. Then, we have numerically optimized the signal intensity under the optimal decoy intensity. Finally, we have numerically checked that our conclusion is almost valid even for finite-length code [18].

Acknowledgments

The author thanks Professor Akihisa Tomita, Dr Toyohiro Tsurumaru, and Mr Ryota Nakayama for valuable comments. He would like to express his appreciation to the referee of this paper for improving the presentation. He is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071. He is also partially supported by the National Institute of Information and Communication Technology (NICT), Japan. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

Appendix A. Proof of lemmas 1 and 3

Define the function $f(c, b) := (c + b)\left(1 + h\left(\frac{b}{c + b}\right)\right)$. Since the assumption implies

$$\frac{df}{dc} = 1 + \log \frac{c}{c + b} > 0, \quad \frac{df}{db} = 1 + \log \frac{b}{c + b} < 0,$$

in order to show the first argument of lemma 1, it is sufficient to show that $\hat{c}(\mu_1, \mu_2)$ is monotonically decreasing for $\mu_1$ and $\mu_2$ and $\hat{b}(\mu_1)$ is monotonically increasing for $\mu_1$. Similarly, define the function $g(a, b) := a\left(1 + h\left(\frac{b}{a}\right)\right)$. Since the assumption implies

$$\frac{dg}{da} = 1 + \log \frac{a - b}{a} > 0, \quad \frac{dg}{db} = \log \frac{b}{a - b} < 0,$$

in order to show the second argument of lemma 1, it is sufficient to show that $\hat{a}(\mu_1, \mu_2)$ is monotonically decreasing for $\mu_1$ and $\mu_2$ and $\hat{b}(\mu_1)$ is monotonically increasing for $\mu_1$. 

Since
\[ \hat{b}(\mu_1) = \frac{\gamma(e^{\mu_1} - e^{(1-\alpha)\mu_1}) + p_0(e^{(1-\alpha)\mu_1} - 1)/2}{\mu_1} \]
\[ = \gamma \alpha + \frac{p_0}{2} + \sum_{n=2}^{\infty} \left( (1 - (1 - \alpha)^n) + \frac{p_0(1 - (1 - \alpha)^2)}{2} \right) \frac{\mu_1^{n-1}}{n!} \]  
(A.1)
and \( \gamma(1 - (1 - \alpha)^n) + \frac{p_0}{2}(1 - \alpha)^n \geq 0, \) \( \hat{b}(\mu_1) \) is monotonically increasing for \( \mu_1 \).

Further
\[ \hat{c}(\mu_1, \mu_2) = \frac{(1-\gamma)e^{\mu_1} - (1-\gamma - p_0/2)e^{(1-\alpha)\mu_1} - p_0/2}{\mu_1^2} \]
\[ = \frac{(1-\gamma)(1-\gamma - p_0/2)(1-\alpha)^{\mu_1^{n-2}}}{n!} - \sum_{n=2}^{\infty} \frac{(1 - (1 - \alpha)^n) - (1 - p_0/2)(1 - (1 - \alpha)^n)}{n!} \]
\[ = (\mu_2 \mu_1) \sum_{n=1}^{\infty} (1 - \gamma - (1 - \gamma - p_0/2)(1 - (1 - \alpha)^n)(\mu_1^{n-2} - \mu_2^{n-2}) \]
\[ = (1 - \gamma)p_0/2 + (1 - \gamma)\alpha + (\mu_2 \mu_1) \times \sum_{n=3}^{\infty} (1 - \gamma - (1 - \gamma - p_0/2)(1 - (1 - \alpha)^n)(\mu_1^{n-2} - \mu_2^{n-2}) \]
\[ = (1 - \gamma)p_0/2 + (1 - \gamma)\alpha - (\mu_2 \mu_1) \times \sum_{n=3}^{\infty} (1 - \gamma - (1 - \gamma - p_0/2)(1 - (1 - \alpha)^n)(\mu_1^{n-2} - \mu_2^{n-2}) \]
\[ = (1 - \gamma)p_0/2 + (1 - \gamma)\alpha - \sum_{n=3}^{\infty} (1 - \gamma)(1 - (1 - \alpha)^n)(1 - (1 - \alpha)p_0/2)(\sum_{m=0}^{n-3} \mu_1^{m+1} \mu_2^{n-2-m}) \]  
(A.2)
Here, \( \frac{1 - (1 - (1 - \alpha)^n) + (1 - \alpha)p_0/2}{n!} \) is always positive. Hence, \( \hat{c}(\mu_1, \mu_2) \) is monotonically decreasing for \( \mu_1 \) and \( \mu_2 \).

Since similar to (A.3), we have
\[ \hat{a}(\mu_1, \mu_2) = (1 - \alpha)p_0 + \alpha - \sum_{n=3}^{\infty} (1 - (1 - \alpha)^n)(1 - (1 - \alpha)p_0/2)(\sum_{m=0}^{n-3} \mu_1^{m+1} \mu_2^{n-2-m}) \]  
(A.4)
\( \hat{a}(\mu_1, \mu_2) \) is monotonically decreasing for \( \mu_1 \) and \( \mu_2 \). Hence, we obtain lemma 1.

Lemma 3 can be proven by substituting 0 into \( \mu_1 \) in (A.1), (A.3), and (A.4). \( \square \)

**Appendix B. Proof of theorem 4**

For a proof of theorem 4, we prepare the following two lemmas under the assumption that \( \mu_d < \mu_v \).
Lemma 5. Assume that
\[
\tilde{a} = f_a \left( 1 - e^{-\alpha \tilde{b}} \right) + p_0, \quad 1 - e^{-\alpha \tilde{b}} + p_0, \mu_a, \mu_s \nonumber \\
= \mu_s^2 e^{\mu_a(1 - e^{-\alpha \tilde{b}} + p_0) - \mu_s^2 e^{\mu_a(1 - e^{-\alpha \tilde{b}} + p_0)}} 
\mu_a \mu_s (\mu_s - \mu_d) 
\] (B.1)
\[
\tilde{b} = f_b \left( \frac{\gamma (1 - e^{-\alpha \tilde{b}}) + p_0 / 2}{\mu_d} \right) 
\] (B.2)
\[
\tilde{c} = f_c \left( (1 - \gamma)(1 - e^{-\alpha \tilde{b}}) + p_0 / 2 - \mu_s^2 e^{\mu_c ((1 - \gamma)(1 - e^{-\alpha \tilde{b}}) + p_0 / 2)} \right) 
\mu_d \mu_s (\mu_s - \mu_d) 
\] (B.3)

Then,

(i) \( \tilde{a} \) is monotonically increasing with respect to \( \tilde{b} \) and monotonically decreasing with respect to \( \tilde{c} \).

(ii) \( \tilde{b} \) is monotonically increasing with respect to \( \tilde{b} \).

(iii) \( \tilde{c} \) is monotonically increasing with respect to \( \tilde{b} \) and monotonically decreasing with respect to \( \tilde{c} \).

(iv) \( \tilde{a} \) is monotonically decreasing with respect to \( \tilde{a} \).

(v) \( \tilde{b} \) is monotonically decreasing with respect to \( \tilde{b} \).

(vi) \( \frac{\tilde{b}}{\tilde{a}} \left( 1 - h \left( \frac{\tilde{b}}{\tilde{a}} \right) \right) \) is monotonically increasing with respect to \( \tilde{a} \) and monotonically decreasing with respect to \( \tilde{b} \).

(vii) \( \tilde{c} \left( 1 - h \left( \frac{\tilde{b}}{\tilde{a}} \right) \right) \) is monotonically increasing with respect to \( \tilde{a} \) and monotonically decreasing with respect to \( \tilde{b} \).

Proof. First, we notice that \( 1 - e^{-\alpha \tilde{b}} \) is monotonically increasing with respect to \( \tilde{b} \) for \( i = s, d \). Using this fact, we can show the items (i), (ii), and (iii).

Next, we will show (iv). Since
\[
\tilde{b} = \frac{\mu_s (\mu_s - \mu_d) e^{\mu_c \gamma (1 - e^{-\alpha \tilde{b}}) + \mu_s (\mu_s - \mu_d) e^{\mu_c (1 - e^{-\mu_s}) p_0 / 2}}}{\mu_d \mu_s (\mu_s - \mu_d)} 
\]
we have
\[
\frac{\tilde{b}}{\tilde{a}} = \frac{\mu_s (\mu_s - \mu_d) e^{\mu_c \gamma (1 - e^{-\alpha \tilde{b}}) + \mu_s (\mu_s - \mu_d) e^{\mu_c (1 - e^{-\mu_s}) p_0 / 2}}}{\mu_d \mu_s (\mu_s - \mu_d) e^{\mu_c (1 - e^{-\alpha \tilde{b}}) + p_0} - \mu_s^2 e^{\mu_c (1 - e^{-\alpha \tilde{b}}) + p_0}} 
= \frac{\mu_s (\mu_s - \mu_d) e^{\mu_c \gamma (1 - e^{-\alpha \tilde{b}}) + \mu_s (\mu_s - \mu_d) e^{\mu_c (1 - e^{-\mu_s}) p_0 / 2}}}{\mu_d \mu_s (\mu_s - \mu_d) e^{\mu_c (1 - e^{-\alpha \tilde{b}}) + p_0} - \mu_s^2 e^{\mu_c (1 - e^{-\alpha \tilde{b}}) + p_0}} 
A_3 (1 - e^{-\alpha \tilde{b}}) + A_2 
= \frac{A_3 (1 - e^{-\alpha \tilde{b}}) + A_2}{A_3 (1 - e^{-\alpha \tilde{b}}) - A_4 (1 - e^{-\alpha \tilde{b}}) + A_5}, 
\]
where
\[ A_1 = \mu_s(\mu_s - \mu_d)e^{\mu_s}\gamma, \quad A_2 := \mu_s(\mu_s - \mu_d)e^{\mu_s}(1 - e^{-\mu_s})p_0/2, \]
\[ A_3 = \mu_d^2e^{\mu_s}, \quad A_4 := \mu_d^2e^{\mu_s}, \quad A_5 := p_0(\mu_d^2e^{\mu_s} - \mu_s^2e^{\mu_s}). \]

As is shown below, we have \( \frac{A_2}{A_5} \leq \frac{A_2}{A_4(1 - e^{-\mu_s})} \). Thus, since \( 1 - e^{-\alpha\tilde{\mu}_d} \) is monotonically increasing with respect to \( \tilde{\mu}_d \), \( \frac{A_5}{A_2(1 - e^{-\alpha\gamma})} \) is monotonically decreasing with respect to \( \tilde{\mu}_d \). Then, we obtain the item (iv). Now, we will show \( \frac{A_2}{A_5} \leq \frac{A_2}{A_4(1 - e^{-\mu_s})} \). Since \( \gamma \leq 1/2 \) and \( \mu_s^2e^{\mu_s} \geq \mu_d^2 \),
\[
\frac{\gamma}{\mu_d^2e^{\mu_s}} \leq \frac{(1 - e^{-\mu_s})p_0/2}{p_0(\mu_d^2e^{\mu_s} - \mu_s^2e^{\mu_s}) - \mu_s^2e^{\mu_s}(1 - e^{-\mu_s})}.
\]

Multiplying \( \mu_s(\mu_s - \mu_d)e^{\mu_s} \), we have
\[
\frac{A_2}{A_5} = \frac{\mu_s(\mu_s - \mu_d)e^{\mu_s}}{\mu_d^2e^{\mu_s}} \leq \frac{\mu_s(\mu_s - \mu_d)e^{\mu_s}(1 - e^{-\mu_s})p_0/2}{p_0(\mu_d^2e^{\mu_s} - \mu_s^2e^{\mu_s}) - \mu_s^2e^{\mu_s}(1 - e^{-\mu_s})} = \frac{B_2}{B_4(1 - e^{-\mu_s})}.
\]

Next, we will show (iv). We have
\[
\frac{\hat{b}}{\hat{c} + \hat{b}} = \frac{\mu_s^2e^{\mu_s}(\mu_s - \mu_d)\gamma(1 - e^{-\alpha\gamma}) + \mu_s(\mu_s - \mu_d)e^{\mu_s}(1 - e^{-\mu_s})p_0/2}{\mu_s^2e^{\mu_s}(\mu_s - \mu_d)\gamma + \mu_s^2e^{\mu_s}(1 - e^{-\mu_s})(\mu_s - \mu_d/2)p_0 - B_1} = \frac{B_2}{B_4(1 - e^{-\mu_s})} + \frac{B_3}{B_4(1 - e^{-\mu_s})} + B_3.
\]

where
\[
B_1 := \mu_d^2e^{\mu_s}(1 - \gamma)(1 - e^{-\gamma\mu_s}) + (1 - e^{-\mu_s})p_0/2, \quad B_2 := \mu_s^2e^{\mu_s}(\mu_s - \mu_d)\gamma, \quad B_3 := \mu_s(\mu_s - \mu_d)e^{\mu_s}(1 - e^{-\mu_s})p_0/2, \quad B_4 := \mu_s^2e^{\mu_s}(\mu_s - \mu_d)\gamma, \quad B_5 := \mu_s^2e^{\mu_s}(1 - e^{-\mu_s})(\mu_s - \mu_d/2)p_0 - B_1.
\]

As is shown below, we have \( \frac{B_2}{B_4} \leq \frac{B_2}{B_4} \). Thus, since \( 1 - e^{-\alpha\tilde{\mu}_d} \) is monotonically increasing with respect to \( \tilde{\mu}_d \), \( \frac{B_2(1 - e^{-\alpha\gamma}) + B_1}{B_4(1 - e^{-\alpha\gamma})} \) is monotonically decreasing with respect to \( \tilde{\mu}_d \). Then, we obtain the desired argument for \( \frac{\hat{b}}{\hat{c} + \hat{b}} \).
Now, we will show \( B_2 \leq \frac{\bar{B}_5}{B_5} \). Since \( g \leq \frac{1}{2} \), we have \( \frac{\gamma}{(\mu_s - \mu_d)} \leq \frac{1}{2(\mu_s - \mu_d/2)} \), which implies

\[
\begin{align*}
B_2 &= \frac{\mu_s e^{\mu_s}(\mu_s - \mu_d) \gamma}{\mu_s e^{\mu_s}(\mu_s - \mu_d/2) \gamma} \\
&= \frac{\mu_s e^{\mu_s}(\mu_s - \mu_d) e^{\mu_d}(1 - e^{-\mu_d}) \gamma}{\mu_s e^{\mu_s}(\mu_s - \mu_d/2) \gamma} \\
&= \frac{\mu_s e^{\mu_s}(1 - e^{-\mu_d}) \gamma}{\mu_s e^{\mu_s}(1 - e^{-\mu_d}/2) \gamma} \\
&\leq \frac{\mu_s e^{\mu_s}(1 - e^{-\mu_d}) \gamma}{\mu_s e^{\mu_s}(1 - e^{-\mu_d}/2) \gamma} = B_2.
\end{align*}
\]

For a proof of (vi), we use the function \( g(a, b) \) defined in the proof of theorem 1. Since \( g(a, b) \) is monotonically increasing with respect to \( a \) and monotonically decreasing with respect to \( b \), we obtain the item (vi). The item (vii) can be shown in the same way by replacing the function \( g(a, b) \) by the function \( f(c, b) \) defined in the proof of theorem 1.

\[\Box\]

Lemma 6. When \( \mu_s \leq (1 + \epsilon) \tilde{\mu}_u \),

\[
\begin{align*}
\sup_{\mu_d > 0 < \mu_s < \tilde{\mu}_u} f_\alpha \left( (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + p_0, (1 - e^{-\tilde{\gamma} \mu_d}) + p_0, \mu_d, \mu_s \right) &= \alpha(1 + \epsilon)^{-1} + p_0, \tag{B.4}
\end{align*}
\]

\[
\begin{align*}
\sup_{\mu_d > 0 < \mu_s < \tilde{\mu}_u} f_\alpha \left( (1 - \gamma) (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + \frac{p_0}{2}, (1 - \gamma) (1 - e^{-a \mu_d}) + \frac{p_0}{2}, \mu_d, \mu_s \right) &= \alpha(1 + \epsilon)^{-1} + \frac{p_0}{2}. \tag{B.5}
\end{align*}
\]

\[
\begin{align*}
\sup_{\mu_d > 0 < \mu_s < \tilde{\mu}_u} f_\alpha \left( (1 - \gamma) (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + \frac{p_0}{2}, (1 - \gamma) (1 - e^{-a \mu_d}) + \frac{p_0}{2}, \mu_d, \mu_s \right) &= (1 - \gamma) \alpha(1 + \epsilon)^{-1} + \frac{p_0}{2}. \tag{B.6}
\end{align*}
\]

Proof. Since \( f_\alpha \left( (1 - \gamma) (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + \frac{p_0}{2}, (1 - \gamma) (1 - e^{-a \mu_d}) + \frac{p_0}{2}, \mu_d, \mu_s \right) = \frac{(1 - \gamma) (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + \frac{p_0}{2}, (1 - \gamma) (1 - e^{-a \mu_d}) + \frac{p_0}{2}, \mu_d, \mu_s \right) \) is monotonically decreasing with respect to \( \mu_d \), we obtain (B.5). Similarly, it is sufficient for (B.6) to show that \( f_\alpha \left( (1 - \gamma) (1 - e^{-a(1+\epsilon)\gamma}) \mu_s + \frac{p_0}{2}, (1 - \gamma) (1 - e^{-a \mu_d}) + \frac{p_0}{2}, \mu_d, \mu_s \right) \) is monotonically decreasing with respect to \( \mu_d \). Choosing \( \tilde{\alpha} \) as \( \alpha(1 + \epsilon)^{-1} \), we obtain
\[ f_p \left( (1 - \gamma)(1 - e^{-\alpha(1 + \epsilon)} \rho) + \frac{p_0}{2} (1 - \gamma)(1 - e^{-\alpha\tilde{\rho}}) + \frac{p_0}{2} \mu_d, \mu_s \right) = \left( \mu_s e^{\alpha\rho} ((1 - \gamma)(1 - e^{-\alpha\rho}) + p_0 (1 - e^{-\alpha\rho})/2) - \mu_d e^{\alpha\rho} ((1 - \gamma)(1 - e^{-\alpha\rho}) + p_0 (1 - e^{-\alpha\rho})/2) - \mu_s e^{\alpha\tilde{\rho}} (1 - \gamma)(1 - e^{-\alpha\tilde{\rho}}) + p_0 (1 - e^{-\alpha\tilde{\rho}})/2) \right) \mu_s (\mu_s - \mu_d) \]
\[ = \frac{p_0}{2} (1 - \gamma) \tilde{\alpha} - \sum_{n=3}^{\infty} \frac{(1 - \gamma)(1 - (1 - \alpha)^n) + p_0/2}{n!} \left( \sum_{m=0}^{n-3} \mu_d^{n-1} \mu_s^{n-2-m} \right) \]
\[ = - \frac{\mu_s e^{\alpha\rho} (1 - \gamma)(e^{-\alpha\rho} - e^{-\alpha\tilde{\rho}})}{\mu_s (\mu_s - \mu_d)}. \]

Since \( e^{-\alpha\rho} - e^{-\alpha\tilde{\rho}} \geq 0 \), the final term is monotonically decreasing with respect to \( \mu_d \). Other terms are also monotonically decreasing with respect to \( \mu_d \).

Similarly, we have
\[ f_d \left( (1 - e^{-\alpha(1 + \epsilon)} \rho) + p_0, (1 - e^{-\alpha\tilde{\rho}}) + p_0, \mu_d, \mu_s \right) = p_0 + \tilde{\alpha} - \sum_{n=3}^{\infty} \frac{(1 - \gamma)(1 - (1 - \alpha)^n) + p_0/2}{n!} \left( \sum_{m=0}^{n-3} \mu_d^{n-1} \mu_s^{n-2-m} \right) - \frac{\mu_d e^{\alpha\rho} (e^{-\alpha\rho} - e^{-\alpha\tilde{\rho}})}{\mu_s (\mu_s - \mu_d)}. \]
So, \( f_d \left( (1 - e^{-\alpha(1 + \epsilon)} \rho) + p_0, (1 - e^{-\alpha\tilde{\rho}}) + p_0, \mu_d, \mu_s \right) \) is also monotonically decreasing with respect to \( \mu_d \). Therefore, we obtain (B.4).

**Proof of theorem 4.** First, we show the case of \( R_e(\tilde{\mu}_s, \tilde{\mu}_d, \epsilon) \). For a fixed \( \tilde{\mu}_s \) and \( \mu_s \) satisfying \( (1 - \epsilon)\tilde{\mu}_s < \mu_s < (1 + \epsilon)\tilde{\mu}_s \), lemmas 5 and 6 imply
\[ \sup_{\tilde{\mu}_d < \mu_d < \mu_s} \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \]
\[ = \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} \sup_{\tilde{\mu}_d < \mu_d < \mu_s} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \]
\[ = \sup_{\tilde{\mu}_d < \mu_d < \mu_s} R_e(\mu_s, \mu_d, \tilde{\mu}_s, (1 + \epsilon)^{-1} \mu_d) = \lim_{\mu_d \to +0} R_e(\mu_s, \mu_d, \tilde{\mu}_s, (1 + \epsilon)^{-1} \mu_d). \quad \text{(B.7)} \]

Hence, we obtain
\[ \sup_{\tilde{\mu}_d < \mu_d < \mu_s} \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \]
\[ = \lim_{\mu_d \to +0} \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \]
\[ = \lim_{\mu_d \to +0} R_e(\mu_s, (1 + \epsilon)^{-1} \mu_d, \tilde{\mu}_s, \tilde{\mu}_d). \quad \text{(B.8)} \]

Since the convergence (B.7) is uniform with respect to \( \mu_s \) and \( \tilde{\mu}_s \), the convergence (B.8) is uniform with respect to \( \mu_s \) and \( \tilde{\mu}_s \). Hence, we obtain
\[ \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} \sup_{\mu_d \to +0} \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \]
\[ = \lim_{\mu_d \to +0} \min_{\mu_s \in [(1 - \epsilon)\tilde{\mu}_s, (1 + \epsilon)\tilde{\mu}_s]} R_e(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d). \quad \text{(B.9)} \]
On the other hand
\[
\min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \lim_{\mu_d \rightarrow +0} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} R_c(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \\
= \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \sup_{\mu_d \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} R_c(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \\
\geq \sup_{\tilde{\mu}_d \rightarrow +0} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} R_c(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d). \tag{B.10}
\]

Combining (B.9) and (B.10), we obtain
\[
\sup_{\tilde{\mu}_d \rightarrow +0} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} R_c(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \\
= \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \lim_{\mu_d \rightarrow +0} \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} R_c(\mu_s, \mu_d, \tilde{\mu}_s, \tilde{\mu}_d) \\
= \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \lim_{\mu_d \rightarrow +0} R_c(\mu_s, (1+\epsilon)\tilde{\mu}_d, \tilde{\mu}_s, \tilde{\mu}_d) \\
= \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \lim_{\mu_d \rightarrow +0} R_c(\mu_s, \mu_d, \tilde{\mu}_s, (1+\epsilon)^{-1}\mu_d) \\
= \min_{\mu_s \in [(1-\epsilon)\mu_a, (1+\epsilon)\mu_a]} \mu_s e^{-\mu_s} \left( \frac{\alpha}{1+\epsilon} + p_0 \right) \left( 1 - h \left( \frac{\gamma (1+\epsilon)}{\alpha (1+\epsilon)} + p_0 \right) \right) \\
+ e^{-\mu_s} p_0 - \eta h(e_{s,+}) \\
= (1-\epsilon)\tilde{\mu}_s e^{-(1-\epsilon)\tilde{\mu}_s} \left( \frac{\alpha}{1+\epsilon} + p_0 \right) \left( 1 - h \left( \frac{\gamma (1+\epsilon)}{\alpha (1+\epsilon)} + p_0 \right) \right) \\
+ e^{-(1-\epsilon)\tilde{\mu}_s} p_0 - \eta h(e_{s,+}), \tag{B.11}
\]

where the final equation follows from (21) and the following fact. Choosing the constant
\[
C = \left( \frac{\alpha}{1+\epsilon} + p_0 \right) \left( 1 - h \left( \frac{\gamma (1+\epsilon)}{\alpha (1+\epsilon)} + p_0 \right) \right) + e^{-\mu_s} p_0 \\
= \left( \frac{\alpha}{1+\epsilon} + p_0 \right) \left( 1 - h \left( \frac{\gamma (1+\epsilon)}{\alpha (1+\epsilon)} + p_0 \right) \right) (\mu_s e^{-\mu_s} + Ce^{-\mu_s}).
\]

Since the function $\mu_s \mapsto \mu_s e^{-\mu_s} + Ce^{-\mu_s}$ is monotonically increasing due to the assumption (21), we obtain the above equation (B.11). Thus, we obtain (22).

Next, we show the case of $R_c(\mu_s, \tilde{\mu}_d, \epsilon)$. Similar to (B.7), using lemmas 5 and 6, we have
Thus, we obtain
\[
\begin{align*}
\sup_{\hat{\mu}_d:0<\hat{\mu}_d<\frac{1-\epsilon}{1+\epsilon} \hat{\mu}_d} \min_{\hat{\mu}_s:0<\hat{\mu}_s<\frac{1-\epsilon}{1+\epsilon} \hat{\mu}_s} \hat{R}_e(\hat{\mu}_s, \hat{\mu}_d, \hat{\mu}_s, \hat{\mu}_d) \\
= \lim_{\hat{\mu}_s \to +0} \hat{R}_e(\hat{\mu}_s, \hat{\mu}_d, \hat{\mu}_s, \hat{\mu}_d) (1 + \epsilon)^{-1} \hat{\mu}_d).
\end{align*}
\] (B.12)

We also have the same relations for \( \hat{R}_e(\hat{\mu}_s, \hat{\mu}_d, \epsilon) \) as (B.9) and (B.10). Hence, we obtain
\[
\begin{align*}
\sup_{\hat{\mu}_s:0<\hat{\mu}_s<\frac{1-\epsilon}{1+\epsilon} \hat{\mu}_s} \min_{\hat{\mu}_d:0<\hat{\mu}_d<\frac{1-\epsilon}{1+\epsilon} \hat{\mu}_d} \hat{R}_e(\hat{\mu}_s, \hat{\mu}_d, \hat{\mu}_s, \hat{\mu}_d) \\
= \min_{\hat{\mu}_s:0<\hat{\mu}_s<\frac{1-\epsilon}{1+\epsilon} \hat{\mu}_s} \hat{\mu}_se^{-\hat{\mu}_s}\left(\frac{\alpha}{1+\epsilon} + p_0\right) \left(1 - h\left(\frac{\alpha}{1+\epsilon} + p_0\right)\right) \\
+ e^{-\hat{\mu}_s}p_0 - p_{s+}\eta h(e_{s+}) \\
= (1 - \epsilon)\hat{\mu}_se^{-\epsilon(1-\epsilon)}\hat{\mu}_s\left(\frac{\alpha}{1+\epsilon} + p_0\right) \left(1 - h\left(\frac{\alpha}{1+\epsilon} + p_0\right)\right) \\
+ e^{-\epsilon(1-\epsilon)}p_0 - p_{s+}\eta h(e_{s+}).
\end{align*}
\]

Thus, we obtain (23).

\[\Box\]

References

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers Systems and Signal Processing (Bangalore, India) (New York: IEEE) pp 175–9
[2] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[3] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[4] Wang X-B 2005 Phys. Rev. Lett. 94 230503
[5] Ma X-F, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326
[6] Wang X-B 2005 Phys. Rev. A 72 012322
[7] Hayashi M 2007 New J. Phys. 9 284
[8] Tsurumaru T, Soujaeff A and Takeuchi S 2008 Phys. Rev. A 77 022319
[9] Curty M, Moroder T, Ma X, Lo H-K and Lütkenhaus N 2009 Phys. Rev. A 79 032335
[10] Wang X-B, Yang L, Peng C-Z and Pan J-W 2009 New J. Phys. 11 070506
[11] Wang X-B, Peng C-Z, Zhang J, Yang L and Pan J-W 2008 Phys. Rev. A 77 042311
[12] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Quantum Inf. Comput. 5 325–60
[13] Lo H-K 2005 Quantum Inf. Comput. 5 413
[14] Sasaki M et al 2011 Opt. Express 19 10387
[15] Stucki D et al 2011 New J. Phys. 13 123001
[16] Levine B F and Belthac G C 1984 Appl. Phys. Lett. 44 553
[17] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[18] Hayashi M and Nakayama R 2014 New J. Phys. 16 063009
[19] Asai T and Tsurumaru T 2011 IEICE Technical Report ISEC2010-121 (in Japanese)
[20] Hayashi M and Nakayama R 2013 arXiv:1311.5322 (submitted to IEEE Trans. Inf. Theor.)
[21] Weedbrook C, Pirandola S, Garcia-Patron R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Rev. Mod. Phys. 84 621
[22] Renner R 2005 Security of quantum key distribution PhD Thesis Dipl. Phys. ETH, Switzerland arXiv:quantph/0512258a
[23] Hayashi M 2007 Phys. Rev. A 76 012329
[24] Hayashi M 2009 Phys. Rev. A 79 019901(E)
[25] Hayashi M and Tsurumaru T 2012 New J. Phys. 14 093014
[26] Tsurumaru T 2013 private communication