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

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

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

PAPER

OPEN ACCESS

RECEIVED
23 July 2015

REVISED
12 November 2015

ACCEPTED FOR PUBLICATION
4 December 2015

PUBLISHED
8 January 2016

Intensity modulation and direct detection quantum key distribution based on quantum noise

Takuya Ikuta and Kyo Inoue
Division of Electrical, Electronic and Information Engineering, Osaka University, Suita, Osaka 565-0871, Japan
E-mail: ikuta@procyon.comm.eng.osaka-u.ac.jp

Keywords: quantum key distribution, quantum shot noise, intensity modulation, direct detection

Abstract

Quantum key distribution (QKD) has been studied for achieving perfectly secure cryptography based on quantum mechanics. This paper presents a novel QKD scheme that is based on an intensity-modulation and direct-detection system. Two slightly intensity-modulated pulses are sent from a transmitter, and a receiver determines key bits from the directly detected intensity. We analyzed the system performance for two typical eavesdropping methods, a beam splitting attack and an intercept-resend attack, with an assumption that the transmitting and receiving devices are fully trusted. Our brief analysis showed that short- or middle-range QKD systems are achievable with a simple setup.

1. Introduction

Quantum key distribution (QKD) has been studied for achieving perfectly secure cryptography. There are two main kinds of QKD scheme: single-photon-based QKD [1, 2] and continuous-variable QKD (CVQKD) [3, 4]. Single-photon-based QKD has the advantage of enabling long-range key distribution, whereas one disadvantage is that bulky and expensive single-photon detectors are required. CVQKD avoids this disadvantage by employing homodyne detection with conventional photodiodes. However, homodyne detection requires phase-stabilized local light, which is not easy to implement. Based on the above background, we previously proposed differential-phase-shift-keying (DPSK)-based CVQKD [5, 6]. A phase-modulated coherent pulse train with moderate power is transmitted, and it is detected using a delay Mach–Zehnder interferometer. Each pulse simultaneously acts as signal and local lights in this scheme, therefore, this method requires no external local light.

This paper presents a novel CVQKD scheme, which utilizes direct detection. Intensity-modulated (IM) coherent light with moderate power is transmitted and directly detected (DD). IM/DD systems are simpler than DPSK systems, as they do not use a delay interferometer, and have been well-developed in conventional optical communications. The present scheme achieves the QKD function with a simple setup.

2. Protocol and security

Figure 1 shows a schematic of the proposed IM/DD QKD system, in which the transmitter and receiver are called Alice and Bob, respectively. The protocol of this system is as follows.

(i) Alice transmits signal light, which is slightly intensity-modulated according to binary random numbers 0 or 1 as I or $(1+\delta)I$, at a moderate power level.

(ii) Bob directly detects the transmitted light. The measured signal levels are distributed because of noise, as shown in figure 2. The distribution has two peaks, corresponding to Alice's binary intensity modulation I and $(1+\delta)I$, that overlap with each other because δ is small compared to the noise variances.

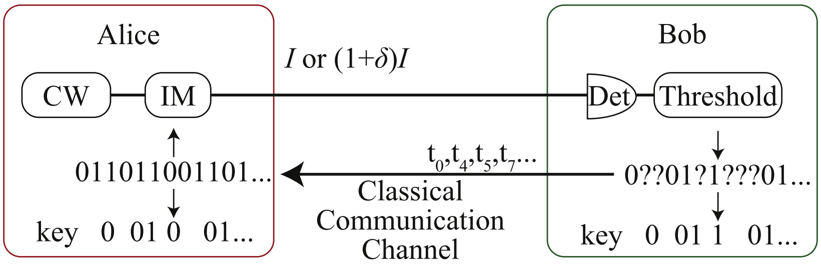

Figure 1. IM/DD QKD system. CW is a continuous-wave laser, IM is an intensity modulator, Det is a photo detector, and Threshold is a comparator. Alice transmits signal light with a power level of I or $(1 + \delta)I$ based on binary random numbers. Bob receives the light and estimates the original binary data. When Bob creates bits, he tells Alice of the bit creation time using a classical communication channel. Hereby, Alice and Bob can share a secret key.

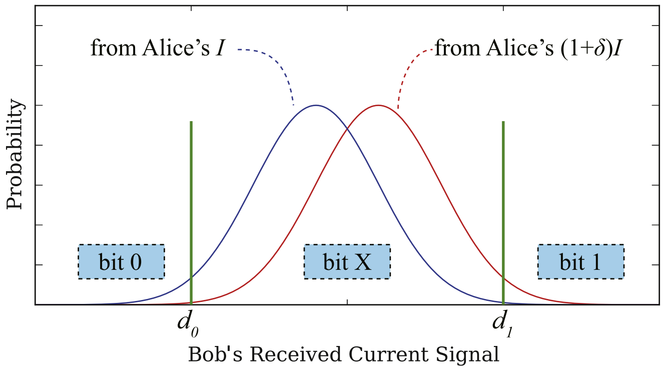

Figure 2. The distribution of Bob's received current signal.

(iii) Bob sets two thresholds at high and low levels d_0 and d_1, respectively, for the signal distribution, as shown in figure 2. When the measured signal is smaller than the lower threshold d_0, he creates bit 0. When the signal is larger than the higher threshold d_1, he creates bit 1. Otherwise, he creates no bit (called bit X).

(iv) Using a classical communication channel, Bob tells Alice the time of the signals from which he created bits. Alice creates bit 0 or 1 when the corresponding signal intensity is I or $(1 + \delta)I$, respectively. Then, Alice and Bob share an identical bit string, which can be a secret key.

The security of this protocol is based on the fact that two coherent states with a small amplitude difference are nonorthogonal to each other. Because of this nonorthogonality, an eavesdropper, Eve, cannot fully distinguish the transmitted state. She may set thresholds and obtain the key bits as Bob does. However, when she conducts this measurement while beam-splitting the transmitted signal, for example, the received signals fluctuate differently in Eve and Bob because the quantum noises of the beam-split lights have no correlation, and thus, the key bits created by Bob and Eve do not match. Eve may try this measurement of setting thresholds while intercepting and resending the transmitted signal. However, Eve sometimes (or most of the time) obtains no bit and is forced to resend randomly intensity-modulated signals, which cause Bob's bit errors and reveal eavesdropping. Note that Eve is not allowed to resend nothing when obtaining no bit, because a moderate signal power is transmitted from Alice to Bob, unlike in single-photon-based QKD, and thus, every signal is expected to be detected by Bob.

3. System performance evaluation

In this section, we describe a system performance evaluation of the above-described IM/DD QKD method, assuming specific eavesdropping, a beam splitting attack (BSA), and an intercept-resend attack (IRA). General attacks are not considered because this paper is proposing a novel QKD protocol featuring practicality, and a detailed theoretical analysis is beyond the scope of the present paper. We assume throughout this paper that all the devices Alice and Bob use are fully trusted and work with an arbitrary precision, in order to evaluate the basic performance of the present protocol.

3.1. Mutual information

From the information theoretical point of view, the final key creation rate after error correction and privacy amplification, i.e. the secure key creation rate, R_f, is given by

$$R_f = R_{\mathrm{AB}} - R_{\mathrm{AE}} \qquad \text{or} \qquad R_{\mathrm{AB}} - R_{\mathrm{BE}}, \tag{1}$$

where R_{AB}, R_{AE}, and R_{BE} are the mutual information between Alice and Bob, that between Alice and Eve, and that between Bob and Eve, respectively.

Which expression, R_{AE} or R_{BE}, in (1) is employed depends on the method of error correction, i.e., bidirectional or reverse reconciliation. In the former case, Eve obtains the error correcting information exchanged between Alice and Bob, and the final key rate should be $R_f = R_{\mathrm{AB}} - \max\,[R_{\mathrm{AE}},\ R_{\mathrm{BE}}]$ so as to exclude Eve's information from the key. In the later case, on the other hand, Eve only obtains the error correcting information sent from Bob to Alice, and the final key rate should be $R_f = R_{\mathrm{AB}} - R_{\mathrm{BE}}$ so as to exclude Eve's information obtained from Bob. Generally, the mutual information between Bob and Eve, R_{BE}, is smaller than that between Alice and Eve, R_{AE}. Thus, reverse reconciliation offers a higher final key creation rate.

In the following sections, we evaluate the above-described mutual information in our QKD system, utilizing the following formula [7]:

$$R_{XY} = \sum_x \sum_y P_{X,Y}(x,\ y) \log_2 \frac{P_{X,Y}(x,\ y)}{P_X(x) P_Y(y)} \qquad X,\ Y = \{A,\ B,\ E\}, \tag{2}$$

In the above expression, R_{XY} is mutual information between X and Y, $P_X(x)$ and $P_Y(y)$ are probabilities that X and Y create x and y, respectively, and $P_{X,Y}(x,\ y)$ is the joint probability that X's bit x coincides with Y's bit y. To be specific, we evaluate the joint probability between Alice and Bob, that between Alice and Eve, and that between Bob and Eve, and then, evaluate the mutual information by substituting them into (2). In practice, the error correction efficiency should be taken into account in estimating R_{AB}. In this paper, however, we assume 100% error correction efficiency in order to evaluate the upper bound of the performance of our protocol.

3.2. Joint probability between Alice and Bob

In this subsection, we derive the joint probabilities between Alice and Bob, and evaluate the mutual information between them. First, we evaluate the distribution of the photo-current signal at Bob's detector, which suffers from some kinds of noise. Here, we assume three kinds of additive white Gaussian noise (AWGN): optical classical noise, optical quantum noise, and electrical thermal noise. Classical noise is mainly caused by the non-ideal light source, whose noise power σ_C^2 is proportional to the square of the light intensity. Quantum noise is inherent in the nature of photons, whose power σ_Q^2 is proportional to the light intensity. Thermal noise is caused by the thermal motion of electrons in receiver circuits, whose power σ_T^2 is independent of the light intensity. Taking these noise characteristics into account, the mean value i_0 and the variance $\sigma_{i_0}^2$ of Bob's signal for Alice's signal of intensity of I_0 are expressed as

$$i_0 = \alpha T \eta I_0, \tag{3}$$

$$\begin{aligned} \sigma_{i_0}^2 &= \alpha^2 \left(\sigma_C^2 + \sigma_Q^2 \right) + \sigma_T^2 \\ &= B \left(a\alpha^2 T^2 \eta^2 I_0^2 + b\alpha^2 T \eta I_0 + c \right), \end{aligned} \tag{4}$$

where B is the base-band width of the receiver, T is the fiber transmittance, η is the quantum efficiency of the detector, a, b, and c are proportionality constants for the classical, quantum, and thermal noises, respectively, and $\alpha = e/h\nu$ (where e is the elementary charge, h is Plank's constant, and ν is the light frequency). Based on the above expressions, the probability density (p.d.) of Bob's signal when Alice sends bit 0, $p_{\mathrm{B|A}}(i|0)$, is given by

$$p_{\mathrm{B|A}}(i|0) = \frac{1}{\sqrt{2\pi}\,\sigma_{i_0}} \exp\left(-\frac{\left(i - i_0\right)^2}{2\sigma_{i_0}^2} \right). \tag{5}$$

For Alice's signal of intensity $(1 + \delta) I_0$, on the other hand, the mean current signal i_1 and the current variance $\sigma_{i_0}^2$ are given by

$$i_1 = \alpha T \eta (1 + \delta) I_0, \tag{6}$$

$$\sigma_{i_1}^2 = B \left(a\alpha^2\ T^2 \eta^2 (1 + \delta)^2 I_0^2 + b\alpha^2\ T\eta (1 + \delta) I_0 + c \right). \tag{7}$$

Table 1. Joint probabilities between Alice and Bob.

Alice's bit a	Bob's bit b	Joint probability $P_{\mathrm{A,B}}(a,\ b)$
0	0	$\frac{1}{4}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right)$
0	X	$\frac{1}{2} - \frac{1}{4}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right) - \frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_0}{\sqrt{2}\,\sigma_0}\right)$
0	1	$\frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_0}{\sqrt{2}\,\sigma_0}\right)$
1	0	$\frac{1}{4}\ \mathrm{erfc}\left(\frac{i_1 - d_0}{\sqrt{2}\,\sigma_1}\right)$
1	X	$\frac{1}{2} - \frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right) - \frac{1}{4}\ \mathrm{erfc}\left(\frac{i_1 - d_0}{\sqrt{2}\,\sigma_1}\right)$
1	1	$\frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right)$

Based on these expressions, the p.d. of Bob's signal when Alice sends bit 1, $p_{\mathrm{B|A}}(i|1)$, is expressed as

$$p_{\mathrm{B|A}}(i|1) = \frac{1}{\sqrt{2\pi}\,\sigma_{i_1}} \exp\left(-\frac{\left(i - i_1\right)^2}{2\sigma_{i_1}^2}\right). \tag{8}$$

For the above two distributions expressed in (5) and (8), Bob determines two thresholds, a lower threshold d_0 and a higher threshold d_1. He creates bits 0 or 1 when the detected signal is lower than d_0 or higher than d_1, respectively.

The conditional probability that Bob creates bit 0 when Alice sends bit 0, $P_{\mathrm{B|A}}(0|0)$, is given by

$$\begin{aligned} P_{\mathrm{B|A}}(0|0) &= \int_{-\infty}^{d_0} p_{\mathrm{B|A}}(i|0)\mathrm{d}i \\ &= \int_{-\infty}^{d_0} \frac{1}{\sqrt{2\pi}\,\sigma_{i_0}} \exp\left(-\frac{\left(i - i_0\right)^2}{2\sigma_{i_0}^2}\right)\mathrm{d}i \\ &= \frac{1}{2}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right), \end{aligned} \tag{9}$$

where $\mathrm{erfc}(x)$ is the complementary error function expressed as $\frac{1}{\sqrt{\pi}}\int_x^{\infty} \mathrm{e}^{-t^2}\mathrm{d}t$. On the other hand, the probability that Alice sends bit 0 is $P_{\mathrm{A}}(0) = 1/2$. Thus, the joint probability that Alice's bit 0 coincides with Bob's bit 0, $P_{\mathrm{A,B}}(0,\ 0)$, is given by

$$P_{\mathrm{A,B}}(0,\ 0) = P_{\mathrm{A}}(0)P_{\mathrm{B|A}}(0|0) = \frac{1}{4}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right). \tag{10}$$

The other joint probabilities are similarly derived, which are listed in table 1. By substituting these probabilities into (2), we obtain the mutual information between Alice and Bob.

For a highly secure key, the numbers of bits 0 and 1 should be equal. Thus, Bob's probabilities of creating bit 0 and bit 1 must be equal, that is

$$\begin{gathered} P_{\mathrm{B}}(0) = P_{\mathrm{B}}(1), \\ P_{\mathrm{B,A}}(0,\ 0) + P_{\mathrm{B,A}}(0,\ 1) = P_{\mathrm{B,A}}(1,\ 1) + P_{\mathrm{B,A}}(1,\ 0), \\ \frac{1}{4}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right) + \frac{1}{4}\ \mathrm{erfc}\left(\frac{i_1 - d_0}{\sqrt{2}\,\sigma_1}\right) = \frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right) + \frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_0}{\sqrt{2}\,\sigma_0}\right). \end{gathered} \tag{11}$$

The second terms on both sides, which represent Bob's error probabilities, are usually much smaller than the first terms. Therefore, the above equation can be approximated as

$$\frac{1}{4}\ \mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right) = \frac{1}{4}\ \mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right). \tag{12}$$

From this equation, we have

$$d_1 = \frac{\sigma_{i_1}}{\sigma_{i_0}}\left(i_0 - d_0\right) + i_1. \tag{13}$$

Alice and Bob choose the system parameters of I_0, δ, and d_0 so as to achieve the largest final key rate under the above condition.

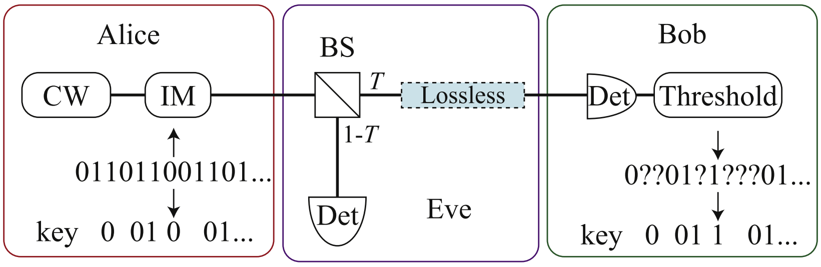

Figure 3. Beam-splitting attack. BS is a beam splitter with a transmittance T and a reflectance $1 - T$. Lossless is a lossless channel. Eve detects signal with an ideal direct detector.

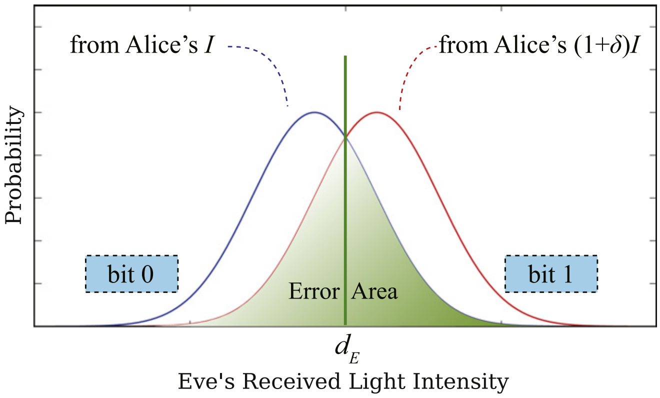

Figure 4. The distribution of Eve's received light intensity.

3.3. Mutual information in BSA

In fiber transmission systems, the signal power is attenuated in the fiber. Eve can eavesdrop using the lost signal power by inserting a beam splitter and replacing the fiber with a lossless line, as illustrated in figure 3. This eavesdropping method is called a BSA. In this subsection, we estimate the joint probability between Alice and Eve and that between Bob and Eve, and then, obtain the mutual information between them in the case of a BSA. In the following discussion, Eve is assumed to measure the signal light with an ideal direct detector, which has 100% quantum efficiency and causes no thermal noise. This assumption is made because the bit information is encoded into the light intensity (or the photon number) with an arbitrary phase, and thus, the use of an ideal direct detector (or a photon number detector) is the optimal strategy for Eve to measure the signal state.

3.3.1. Joint probability between Alice and Eve

Figure 4 shows the distribution of Eve's measured light intensity. It has two peaks, corresponding to Alice's bits 0 and 1, respectively, that partially overlap because of quantum noise and optical classical noise. For this signal distribution, Eve sets a threshold d_{E} between the two peaks, and creates bit 0 or 1 when the received signal is lower or higher than d_{E}, respectively. When Alice launches the light intensity I_0 into a fiber line with transmittance T, Eve's mean light intensity I_{E_0} and it's variance $\sigma^2_{\mathrm{E}_0}$ are given by

$$I_{\mathrm{E}_0} = (1 - T)I_0, \tag{14}$$

$$\sigma^2_{\mathrm{E}_0} = B\left\{a(1 - T)^2{I_0}^2 + b(1 - T)I_0\right\}. \tag{15}$$

When Alice transmits the light intensity $(1 + \delta)I_0$, on the other hand, Eve's mean light intensity I_{E_1} and it's variance $\sigma^2_{\mathrm{E}_1}$ are expressed as

$$I_{\mathrm{E}_1} = (1 - T)(1 + \delta)I_0, \tag{16}$$

$$\sigma^2_{\mathrm{E}_1} = B\left\{a(1 - T)^2(1 + \delta)^2 I_0^2 + b(1 - T)(1 + \delta)I_0\right\}. \tag{17}$$

With these parameters and the threshold d_{E}, the joint probabilities between Alice and Eve are obtained using a procedure similar to that used in section 3.2. These probabilities are summarized in the table 2.

To actually calculate the joint probability summarized in table 2, we need to know Eve's threshold d_{E}, which is determined as follows. In judging Alice's bit, Eve sets a threshold at a value at which the tails of the two peaks

Table 2. Joint probabilities between Alice and Eve for BSA.

Alice's bit a	Eve's bit e	Joint probability $P_{\mathrm{A,E}}(a,\ e)$
0	0	$\frac{1}{2}-\frac{1}{4}\,\mathrm{erfc}\left[\frac{d_{\mathrm{E}}-(1-T)I_0}{\sqrt{2}\,\sigma_{\mathrm{E}_0}}\right]$
0	1	$\frac{1}{4}\,\mathrm{erfc}\left[\frac{d_{\mathrm{E}}-(1-T)I_0}{\sqrt{2}\,\sigma_{\mathrm{E}_0}}\right]$
1	0	$\frac{1}{4}\,\mathrm{erfc}\left[\frac{(1-T)I_1-d_{\mathrm{E}}}{\sqrt{2}\,\sigma_{\mathrm{E}_1}}\right]$
1	1	$\frac{1}{2}-\frac{1}{4}\,\mathrm{erfc}\left[\frac{(1-T)I_1-d_{\mathrm{E}}}{\sqrt{2}\,\sigma_{\mathrm{E}_1}}\right]$

corresponding to Alice's bits 0 and 1 intersect, as shown in figure 4. This condition is expressed as

$$\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{E}_0}}\exp\left[-\frac{\left\{d_{\mathrm{E}}-(1-T)I_0\right\}^2}{2\sigma_{\mathrm{E}_0}^2}\right]=\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{E}_1}}\exp\left[-\frac{\left\{d_{\mathrm{E}}-(1-T)I_1\right\}^2}{2\sigma_{\mathrm{E}_1}^2}\right]. \tag{18}$$

From this equation, we obtain Eve's threshold as:

$$d_{\mathrm{E}}=\frac{1-T}{\sigma_{\mathrm{E}_1}^2-\sigma_{\mathrm{E}_0}^2}\left(\sigma_{\mathrm{E}_1}^2I_0-\sigma_{\mathrm{E}_0}^2I_1+\sigma_{\mathrm{E}_0}\sigma_{\mathrm{E}_1}\sqrt{\left(I_1-I_0\right)^2-\left(\sigma_{\mathrm{E}_1}^2-\sigma_{\mathrm{E}_0}^2\right)\ln\frac{\sigma_{\mathrm{E}_0}^2}{\sigma_{\mathrm{E}_1}^2}}\right). \tag{19}$$

When $\sigma_{\mathrm{E}_0}^2\approx\sigma_{\mathrm{E}_1}^2$, (19) can be approximated as

$$d_{\mathrm{E}}=(1-T)\frac{\sigma_{\mathrm{E}_1}I_0+\sigma_{\mathrm{E}_0}I_1}{\sigma_{\mathrm{E}_0}+\sigma_{\mathrm{E}_1}}. \tag{20}$$

3.3.2. Joint probability between Bob and Eve

In this subsection, we derive the joint probabilities between Bob and Eve. The deriving proceedure is somewhat different from that in the previous subsections, because the optical classical noise has a correlation between Bob and Eve. To take this correlation into account, we separately consider the probability densities caused by the classical noise and by the quantum noise.

When Alice sends bit 0, the p.d. of her classical light intensity I_{BS}, $p_{\mathrm{A}}(I_{\mathrm{BS}})$, is given by

$$p_{\mathrm{A}}\left(I_{\mathrm{BS}}\right)=\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{CA}}}\exp\left\{-\frac{\left(I_{\mathrm{BS}}-I_0\right)^2}{2\sigma_{\mathrm{CA}}^2}\right\}, \tag{21}$$

which originates from the optical classical noise with a variance of $\sigma_{\mathrm{CA}}^2=BaI_0^2$. In the above equation, I_{BS} fluctuates because of the quantum noise, which has no correlation between the two beam-splitter outputs. Taking this into account, the conditional probability that Eve creates bit 0 from this signal intensity I_{BS} is given by

$$P_{\mathrm{E|A}}\left(0\middle|I_{\mathrm{BS}}\right)=\int_{-\infty}^{d_{\mathrm{E}}}\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{Eq}}}\exp\left\{-\frac{\left(I_{\mathrm{E}}-(1-T)I_{\mathrm{BS}}\right)^2}{2\sigma_{\mathrm{Eq}}^2}\right\}\mathrm{d}I_{\mathrm{E}}, \tag{22}$$

where I_{E} is Eve's received light intensity, and $\sigma_{\mathrm{Eq}}^2=Bb(1-T)I_{\mathrm{BS}}\approx Bb(1-T)I_0$ is her quantum noise. On the other hand, the conditional probability that Bob creates bit 0 when Alice transmits I_{BS} is given by

$$P_{\mathrm{B|A}}\left(0\middle|I_{\mathrm{BS}}\right)=\int_{-\infty}^{d_0}\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{B}_0}}\exp\left\{-\frac{\left(i_{\mathrm{B}}-\alpha T\eta I_{\mathrm{BS}}\right)^2}{2\sigma_{\mathrm{B}_0}^2}\right\}\mathrm{d}i_{\mathrm{B}}, \tag{23}$$

where i_{B} is Bob's received current signal, and $\sigma_{\mathrm{B}_0}^2=\alpha^2\sigma_{\mathrm{Q}}^2+\sigma_{\mathrm{T}}^2$ is his current variance.

From (21)–(23), the joint probability $P_{\mathrm{B,E|A}}(0,\ 0|0)$, that Bob's bit 0 coincides with Eve's bit 0 when Alice sends bit 0, is given by

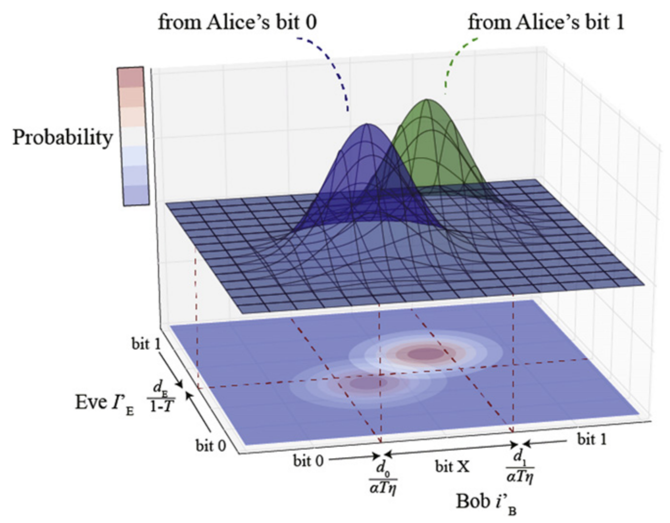

Figure 5. Bivariate normal distribution between Bob and Eve in BSA. The horizontal axis and the vertical axis represent Bob's transformed signal, i'_{B}, and Eve's transformed signal, I'_{E}, respectively. The blue surface and green surface correspond to Alice's bit 0 and bit 1, respectively.

$$\begin{aligned}P_{\mathrm{B,E|A}}(0,\,0|0) &= \int_{-\infty}^{\infty} \mathrm{d}I_{\mathrm{BS}} P_{\mathrm{B|A}}\left(0\middle|I_{\mathrm{BS}}\right)P_{\mathrm{E|A}}\left(0\middle|I_{\mathrm{BS}}\right)p_{\mathrm{A}}\left(I_{\mathrm{BS}}\right),\\ &= \int_{-\infty}^{\infty} \mathrm{d}I_{\mathrm{BS}}\left[\int_{-\infty}^{d_0}\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{B}_0}}\exp\left\{-\frac{\left(i_{\mathrm{B}}-\alpha T\eta I_{\mathrm{BS}}\right)^2}{2\sigma_{\mathrm{B}_0}^2}\right\}\mathrm{d}i_{\mathrm{B}}\right]\\ &\quad\times\left[\int_{-\infty}^{d_{\mathrm{E}}}\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{Eq}}}\exp\left\{-\frac{\left(I_{\mathrm{E}}-(1-T)I_{\mathrm{BS}}\right)^2}{2\sigma_{\mathrm{Eq}}^2}\right\}\mathrm{d}I_{\mathrm{E}}\right]\\ &\quad\times\frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{CA}}}\exp\left\{-\frac{\left(I_{\mathrm{BS}}-I_0\right)^2}{2\sigma_{\mathrm{CA}}^2}\right\}.\end{aligned}\tag{24}$$

By integrating over I_{BS} and then transforming variables as $I'_{\mathrm{E}}=I_{\mathrm{E}}/(1-T)$, $i'_{\mathrm{B}}=i_{\mathrm{B}}/(\alpha T\eta)$, $\sigma_X^2=\sigma_{\mathrm{Eq}}^2/(1-T)^2+\sigma_{\mathrm{CA}}^2$, $\sigma_Y^2=\sigma_{\mathrm{B}_0}^2/(\alpha T\eta)^2+\sigma_{\mathrm{CA}}^2$, and $\rho_{XY}=\dfrac{\sigma_{\mathrm{CA}}^2}{\sqrt{\sigma_{\mathrm{B}_0}^2\sigma_{\mathrm{CA}}^2/(\alpha T\eta)^2+\sigma_{\mathrm{Eq}}^2\sigma_{\mathrm{CA}}^2/(1-T)^2+\sigma_{\mathrm{Eq}}^2\sigma_{\mathrm{B}_0}^2/\{(1-T)\alpha T\eta\}^2+\sigma_{\mathrm{CA}}^4}}$, this joint probability is rewritten as

$$\begin{aligned}P_{\mathrm{B,E|A}}(0,\,0|0) &= \int_{-\infty}^{\frac{d_{\mathrm{E}}}{1-T}}\mathrm{d}I'_{\mathrm{E}}\int_{-\infty}^{\frac{d_0}{\alpha T\eta}}\mathrm{d}i'_{\mathrm{B}}\frac{1}{2\pi\sigma_X\sigma_Y\sqrt{1-\rho_{XY}^2}}\\ &\quad\times\exp\left[-\frac{1}{2\left(1-\rho_{XY}^2\right)}\left\{\frac{\left(I'_{\mathrm{E}}-I_0\right)^2}{\sigma_X^2}+\frac{\left(i'_{\mathrm{B}}-I_0\right)^2}{\sigma_Y^2}-\frac{2\rho_{XY}\left(I'_{\mathrm{E}}-I_0\right)\left(i'_{\mathrm{B}}-I_0\right)}{\sigma_X\sigma_Y}\right\}\right].\end{aligned}\tag{25}$$

The joint probabilities of other bit combinations between the three parties (Alice, Bob, and Eve) can be similarly derived, the results of which are schematically shown in figure 5. The horizontal axis and vertical axis represent Bob's transformed signal, i'_{B}, and Eve's transformed signal, I'_{E}, respectively. The six regions divided by the thresholds of Bob and Eve represent their bits. We obtain the other joint probabilities by integrating the distributions in corresponding regions, as in (25).

Applying these results to (2), we can evaluate the mutual information.

3.4. Mutual information in IRA

In this subsection, we discuss the system performance (or mutual information) under an IRA. In this eavesdropping strategy, Eve intercepts and measures the signal on the transmission line, and then resends a fake signal to Bob based on the measured result. When Eve conducts this eavesdropping, Bob's error rate increases, because she cannot correctly measure and resend the signal; this increase in error rate can reveal the

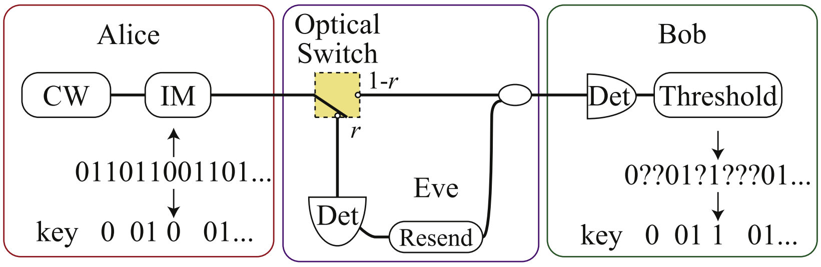

Figure 6. Intercept-resend attack. Eve randomly switches the transmission line, and detects signal with an ideal direct detector. She resends a signal corresponding to the result from the detector.

eavesdropping in principle. In practice, however, Bob's error rate fluctuates and Eve can partially perform the IRA with an optical switch, masking the eavesdropping-induced bit errors with the bit error rate fluctuation.

3.4.1. Key creation rate

Figure 6 shows the setup of the partial IRA, where Eve occasionally extracts the transmitted signal via an optical switch, and performs an IRA on the extracted signal. In this eavesdropping strategy, the switching rate r is an important parameter for Eve to efficiently steal the information. When she employs a high r value, she can measure a large fraction of the transmitted signal, but will induce a large error-rate at Bob, and therefore, has a high risk of being revealed. When employing a low r value, on the other hand, the risk of being revealed is low but the obtainable information amount is small. Thus, there is an optimum switching rate, which is discussed in the following.

First, we suppose that the information amount when Eve conducts full-IRA without an optical switch is given. Using this assumption, we discuss Eve's strategy for optimizing her switching ratio. The full-IRA information amount between Alice, Bob, and Eve is discussed in the next subsection. We assume that Bob creates a sifted key string of n bits, performs error-correction on it, and sets an error-rate threshold e_{th} for it. When the error rate of the key string e, calculated from the error-corrected bits, is larger than e_{th}, Bob discards the key, considering that Eve has eavesdropped on a large number of key bits. When the error-rate e is lower than e_{th}, on the other hand, he assumes that the amount of leaked information is small, and therefore, performs privacy amplification on the corrected key.

Here, we discuss the error-rate distribution when the partial IRA is conducted, assuming that γ out of n bits of Bob's sifted key are intercepted and resent by Eve, and Bob's and Eve's original mean error-rates are e_{Bob} and e_{Eve}, respectively. Note that γ is a stochastic variable because whether an intercepted-resent signal exceeds the Bobs thresholds is probabilistic. Unintercepted $(n - \gamma)$ bits have a mean error-rate $\bar{y}$ equal to e_{Bob}, while the mean error-rate of the intercepted-resent γ bits is $\bar{x} = e_{\mathrm{Bob}} + e_{\mathrm{Eve}} - 2e_{\mathrm{Bob}}e_{\mathrm{Eve}}$. Because these probabilities are independent of each other, the p.d. of the error-rate in intercepted-resent γ bits, $p_{\mathrm{IR}}(x)$, and that of the untouched $n - \gamma$ bits, $p_{u\mathrm{IR}}(y)$, respectively, follow binomial distributions. With Gaussian approximation, they are given by

$$p_{\mathrm{IR}}(x) = \frac{1}{\sqrt{2\pi}\,\sigma_{\mathrm{IR}}} \exp\left\{-\frac{\left(x - \bar{x}\right)^2}{2\sigma_{\mathrm{IR}}^2}\right\}, \tag{26}$$

$$p_{u\mathrm{IR}}(y) = \frac{1}{\sqrt{2\pi}\,\sigma_{u\mathrm{IR}}} \exp\left\{-\frac{\left(y - \bar{y}\right)^2}{2\sigma_{u\mathrm{IR}}^2}\right\}, \tag{27}$$

where $\sigma_{\mathrm{IR}}^2 = \bar{x}(1 - \bar{x})/\gamma$ and $\sigma_{u\mathrm{IR}}^2 = \bar{y}(1 - \bar{y})/(n - \gamma)$. The total error rate of n bits, $z = \frac{\gamma}{n}x + \frac{n - \gamma}{n}y$, is a linear combination of x and y. Thus, the p.d. of the total error rate, $p_{\mathrm{error}}(z)$, is given by

$$p_{\mathrm{error}}(z) = \frac{1}{\sqrt{2\pi}\,\sigma_z\left(r'\right)} \exp\left\{-\frac{\left(z - \bar{z}\left(r'\right)\right)^2}{2\sigma_z^2\left(r'\right)}\right\}, \tag{28}$$

where $r' = \gamma/n$, $\bar{z}(r') = r\bar{x} + (1 - r')\bar{y}$, and $\sigma_z^2(r') = \{r'\bar{x}(1 - \bar{x}) + (1 - r')\bar{y}(1 - \bar{y})\}/n$.

Next, we estimate Eve's net amount of eavesdropping information, R_{netE}, which is determined by two factors: the information amount that Eve obtains from the intercepted signal and the probability that Bob does not discard a sifted key. Denoting R_{E}' as the information amount that Eve obtains from an intercepted signal, the

Table 3. Joint probabilities between Alice and Eve for IRA.

Alice's bit a	Eve's bit e	Joint probability $P_{\mathrm{A,E}}(a,\ e)$
0	0	$\frac{1}{2} - \frac{1}{4}\operatorname{erfc}\left(\frac{d_{\mathrm{E}} - I_0}{\sqrt{2}\,\sigma_{\mathrm{E}0}}\right)$
0	1	$\frac{1}{4}\operatorname{erfc}\left(\frac{d_{\mathrm{E}} - I_0}{\sqrt{2}\,\sigma_{\mathrm{E}0}}\right)$
1	0	$\frac{1}{4}\operatorname{erfc}\left(\frac{I_1 - d_{\mathrm{E}}}{\sqrt{2}\,\sigma_{\mathrm{E}1}}\right)$
1	1	$\frac{1}{2} - \frac{1}{4}\operatorname{erfc}\left(\frac{I_1 - d_{\mathrm{E}}}{\sqrt{2}\,\sigma_{\mathrm{E}1}}\right)$

net eavesdropping information amount when γ bits out of n bits of the sifted key are intercept-resent bits is given by

$$R_{\mathrm{netE}}(\gamma) = \gamma/n \cdot R'_{\mathrm{E}} \cdot P\left(z \leqslant e_{\mathrm{th}}\right), \tag{29}$$

where $P(z \leqslant e_{\mathrm{th}}) = \int_{-\infty}^{e_{\mathrm{th}}} p_{\mathrm{error}}(z)\mathrm{d}z$ is the probability of Bob employing a sifted key. In the above expression, γ is a stochastic variable. Assuming that γ follows a binomial distribution with Gaussian approximation determined by the switching rate r, we obtain the net eavesdropping information amount, R_{netE}, as

$$R_{\mathrm{netE}} = \int_{-\infty}^{\infty} \left\{r' R'_{\mathrm{E}} P\left(z \leqslant e_{\mathrm{th}}\right)\right\} \cdot \frac{1}{\sqrt{2\pi}\,\sigma_{r'}} \exp\left\{-\frac{\left(r' - r\right)^2}{2\sigma_{r'}^2}\right\} \mathrm{d}r', \tag{30}$$

where $\sigma_{r'}^2 = r(1 - r)/n$ is the variance of $r' = \gamma/n$. It is efficient for Eve to maximize the net eavesdropping information amount, R_{netE}, and Alice and Bob conduct privacy amplification assuming the maximized R_{netE}.

The mutual information between Alice and Bob, on the other hand, is determined by Bob's error-rate and the probability that he discards a sifted key because of its large error-rate. Denoting the information amount shared between Alice and Bob without discarding as R'_{AB}, the net information amount between them, R_{netAB}, is given by

$$R_{\mathrm{netAB}} = \int_{-\infty}^{\infty} \left\{R'_{\mathrm{AB}} P\left(z \leqslant e_{\mathrm{th}}\right)\right\} \cdot \frac{1}{\sqrt{2\pi}\,\sigma_{r'}} \exp\left\{-\frac{\left(r' - r\right)^2}{2\sigma_{r'}^2}\right\} \mathrm{d}r'. \tag{31}$$

Therefore, the net final key creation rate on IRA, $R_{\mathrm{net}f}$, is given by

$$\begin{aligned} R_{\mathrm{net}f} &= \int_{-\infty}^{\infty} \left[\left\{R'_{\mathrm{AB}} - r' R'_{\mathrm{E}}\right\} P\left(z \leqslant e_{\mathrm{th}}\right)\right] \cdot \frac{1}{\sqrt{2\pi}\,\sigma_{r'}} \exp\left\{-\frac{\left(r' - r\right)^2}{2\sigma_{r'}^2}\right\} \mathrm{d}r' \\ &= R_{\mathrm{netAB}} - R_{\mathrm{netE}}. \end{aligned} \tag{32}$$

3.4.2. Joint probabilities in IRA

The previous subsection derives the final key creation rate, assuming that Eve's information amount R'_{E} and the mutual information amount between Alice and Bob R'_{AB} are given. In this subsection, we discuss these parameters. In IRA, Eve measures all of Alice's signal in the intercepting stage. Thus, the intensity variance of Eve's received signal when Alice sends bit 0, $\sigma_{\mathrm{E}0}^2$, is given by

$$\sigma_{\mathrm{E}0}^2 = B\left(aI_0^2 + bI_0\right). \tag{33}$$

The variance when Alice sends bit 1 is similarly determined. Then, the joint probabilities between Alice and Eve in IRA are obtained using the same procedure as in section 3.3.1, the results of which are summarized in table 3. Using these joint probabilities, we can estimate R'_{E}.

Regarding Eve as a transmitter, we can estimate the conditional probabilities of Bob's bits. To deceive Bob, Eve resends a fake signal with the same properties as Alice's signal. For such signals, the probabilities of Bob's bits when Eve resends bit 0 or 1 are the same as those when Alice sends bit 0 or 1, which are summarized in table 4.

Here, however, there is a difference between Alice and Eve in their bit creation probabilities. Eve's bit creation probabilities can be estimated from the joint probabilities between Alice and Eve that are summarized in table 3. Taking these into account, a joint probability between Eve and Bob in IRA, $P_{\mathrm{B,E}}$, is obtained as

Table 4. Conditional probabilities between Eve and Bob for IRA.

Eve's bit a	Bob's bit b	Conditional probability $P_{\mathrm{B}\vert\mathrm{E}}(b\vert e)$
0	0	$\frac{1}{2}\,\mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right)$
0	X	$1 - \frac{1}{2}\,\mathrm{erfc}\left(\frac{i_0 - d_0}{\sqrt{2}\,\sigma_0}\right) - \frac{1}{2}\,\mathrm{erfc}\left(\frac{d_1 - i_0}{\sqrt{2}\,\sigma_0}\right)$
0	1	$\frac{1}{2}\,\mathrm{erfc}\left(\frac{d_1 - i_0}{\sqrt{2}\,\sigma_0}\right)$
1	0	$\frac{1}{2}\,\mathrm{erfc}\left(\frac{i_1 - d_0}{\sqrt{2}\,\sigma_1}\right)$
1	X	$1 - \frac{1}{2}\,\mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right) - \frac{1}{2}\,\mathrm{erfc}\left(\frac{i_1 - d_0}{\sqrt{2}\,\sigma_1}\right)$
1	1	$\frac{1}{2}\,\mathrm{erfc}\left(\frac{d_1 - i_1}{\sqrt{2}\,\sigma_1}\right)$

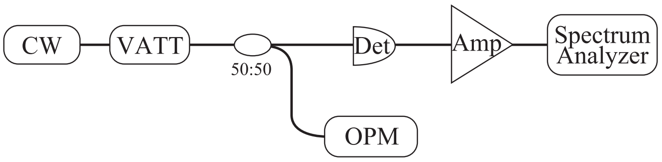

Figure 7. Experimental setup to obtain the noise proportionality constants. CW is a continuous wave laser. VATT is an optical variable attenuator. OPM is an optical power meter. Det is an optical receiver module. Amp is an electrical amplifier. Spectrum analyzer is an electrical spectrum analyzer.

$$P_{\mathrm{B,E}}(0,\,0) = P_{\mathrm{E}}(0)P_{\mathrm{B|E}}(0|0) = \Big(P_{\mathrm{A,E}}(0,\,0) + P_{\mathrm{A,E}}(1,\,0)\Big)\cdot P_{\mathrm{B|E}}(0|0), \tag{34}$$

The other joint probabilities are similarly obtained. From these joint probabilities between Eve and Bob, we obtain R'_{E}, which was given a temporary value in the previous subsection.

The mutual information between Alice and Bob in IRA, R'_{AB}, is separable into those with and without Eve's interception, R_{onAB} and R_{offAB}, as

$$R'_{\mathrm{AB}} = rR_{\mathrm{onAB}} + (1 - r)R_{\mathrm{offAB}}. \tag{35}$$

R_{offAB} is equal to the mutual information without Eve, which is discussed in section 3.1. On the other hand, R_{onAB} is evaluated based on the joint probabilities between Alice and Bob via Eve. These values are obtained from the joint probabilities between Alice and Eve summarized in table 3 and Bob's bit probabilities for Eve's bits are summarized in table 4, as

$$\begin{aligned}P_{\mathrm{A,B}}(0,\,0) &= P_{\mathrm{A|E}}(0|0)\cdot P_{\mathrm{B|E}}(0|0)\cdot P_{\mathrm{E}}(0) + P_{\mathrm{A|E}}(0|1)\cdot P_{\mathrm{B|E}}(0|1)\cdot P_{\mathrm{E}}(1)\\ &= \frac{P_{\mathrm{A,E}}(0,\,0)}{P_{\mathrm{E}}(0)}\frac{P_{\mathrm{B,E}}(0,\,0)}{P_{\mathrm{E}}(0)}P_{\mathrm{E}}(0) + \frac{P_{\mathrm{A,E}}(0,\,1)}{P_{\mathrm{E}}(1)}\frac{P_{\mathrm{B,E}}(0,\,1)}{P_{\mathrm{E}}(1)}P_{\mathrm{E}}(1)\\ &= \frac{P_{\mathrm{A,E}}(0,\,0)P_{\mathrm{B,E}}(0,\,0)}{P_{\mathrm{E}}(0)} + \frac{P_{\mathrm{A,E}}(0,\,1)P_{\mathrm{B,E}}(0,\,1)}{P_{\mathrm{E}}(1)}.\end{aligned} \tag{36}$$

Futhermore, we can obtain the error-rates, e_{Bob} and e_{Eve}, from these joint probabilities. From table 1, Bob's original error-rate, e_{Bob}, is given by

$$e_{\mathrm{Bob}} = \frac{P_{\mathrm{A,B}}(0,\,1) + P_{\mathrm{A,B}}(1,\,0)}{P_{\mathrm{A,B}}(0,\,0) + P_{\mathrm{A,B}}(0,\,1) + P_{\mathrm{A,B}}(1,\,0) + P_{\mathrm{A,B}}(1,\,1)}. \tag{37}$$

Similarly, Eve's error-rate, e_{Eve}, is estimated from table 3.

4. Simulations and discussion

Based on the above discussions, we simulated the system performance of the present scheme for BSA or IRA.

For the simulations, we first experimentally measured the proportionality constants for noise, a, b, and c, in (4), using the setup shown in figure 7. A continuous lightwave generated from a DFB-LD module (NTT Electronics, NLK1551HSC) was passed through a variable attenuator, and incident to an optical 3 dB coupler,

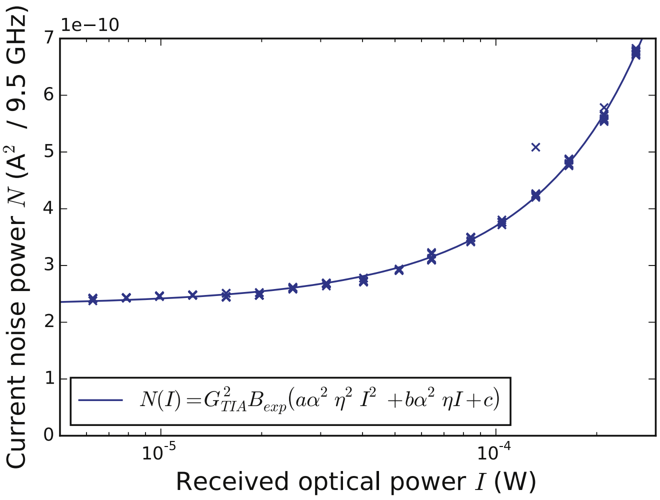

Figure 8. Measured current noise power. Crosses are measured data and solid line is a fitting curve of *N*(*I*) given by (38).

the outputs of which were connected to an optical power meter and an optical receiver module (Sevensix Inc., SSR002), respectively. The receiver was composed of a PIN photodiode and a transimpedance amplifier (TIA) with a 1.2 kΩ transimpedance. The received signal was amplified, and its noise power was measured by a spectrum analyzer. We measured the noise power in a frequency range from 500 MHz to 10 GHz for various optical power levels coupled to the receiver. Besides, the quantum efficiency of the receiver was measured as $\eta = 0.62$. Figure 8 plots the measured noise power, as a function of the optical received power, by crosses. Also shown by the solid line in the same figure is a fitting curve of *N*(*I*) given by

$$N(I) = G_{\mathrm{TIA}}^2 B_{\exp}\left(a\alpha^2\eta^2 I^2 + b\alpha^2\eta I + c\right), \quad (38)$$

where *I* is the received optical power, $G_{\mathrm{TIA}} = 24$ is the TIA current gain, $B_{\exp} = 9.5$ GHz is the band-width in this measurement, and *a*, *b*, and *c* are constants. From this fitting curve, we evaluated the proportional constants as $a = (5.664 \pm 0.345) \times 10^{-16}$ /Hz, $b = (2.288 \pm 0.052) \times 10^{-19}$ W Hz^{-1}, and $c = (4.196 \pm 0.019) \times 10^{-23}$A^2/Hz. These values would be used in our simulations.

Other parameter values used in the simulations are as follows. The bandwidth of the intensity modulation is $B = 10$ GHz and the maximum laser output power is 2 mW. The sifted key length *n* in IRA is assumed to be either 1 kbit or 1 Mbit for examining the effect of key length. Bob's error-rate e_{Bob} is assumed to be less than 0.15. The fiber transmission loss is 0.20 dB km^{-1}. Alice's transmitted signal power I_0, the modulation depth δ, Bob's bit creation threshold d_0, and Bob's error-rate threshold e_{th} were chosen so as to maximize the final key creation rate at each transmission length. The intercepting ratio *r* was chosen such that Eve obtained the highest net eavesdropping information R_{netE}.

Figure 9 shows the final key creation rate R_f in bidirectionally error-correcting systems. The system performance under IRA largely depends on the sifted key length: a longer length results in a higher key creation rate. This is because a longer key-bit length makes the error-rate variance smaller, reducing Eve's probability to mask her IRA using error-rate fluctuation. Figure 9 indicates that BSA is much more powerful than IRA in our present scheme.

Figure 10 shows the final key creation rate R_f in reverse reconciliation systems. Similar to in the above-described bidirectional system (figure 9), BSA is shown to be stronger than IRA. The possible QKD distance is longer than that in the bidirectional error-correcting system, and the achievable distance is approximately 90 km. Note that the final key creation rate estimated here assumes 100% error correction efficiency, thus the practical achievable distance would be shorter than this result. The 90 km achievable distance is moderate or short, compared to conventional single-photon-based QKD systems [8–11]. These results suggest that the present scheme is suitable for short- or middle-range QKD systems.

Figure 11 shows the assumed intensity modulation depth δ, used in figures 9 and 10, that maximizes the final key creation rate for each eavesdropping method. δ ranges from approximately 0.5 to approximately 2%. This small modulation depth may be an issue in practical implementations. When the resolution of the intensity modulator is not sufficient to realize this preciseness of the modulation depth, the modulation depth fluctuates, resulting in a large proportional constant for classical noise, i.e., *a* in (4). Thus, the correlation between Eve and Bob increases, and the transmission distance decreases. Quantitative analysis on this issue will be required for practical implementation.

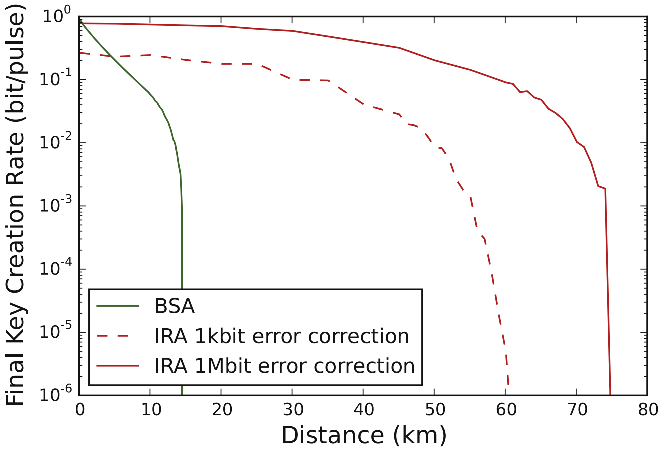

Figure 9. Final key creation rate for bidirectional error correction.

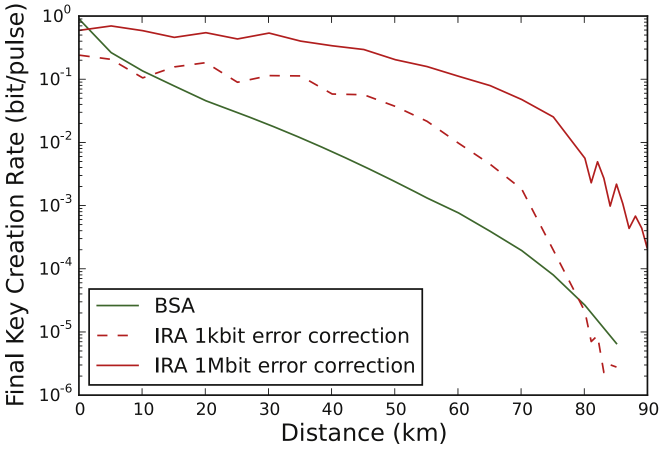

Figure 10. Final key creation rate for reverse reconciliation.

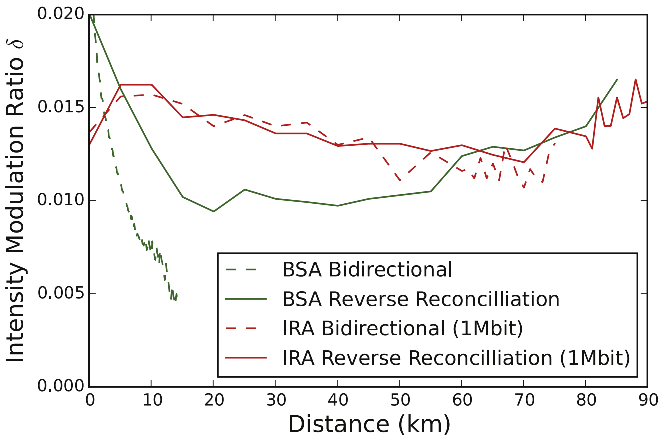

Figure 11. Intensity modulation depth δ for each eavesdropping method.

5. Conclusion

We presented a novel CVQKD scheme employing intensity-modulation and simple direct-detection. We described the setup and the protocol of our QKD scheme, and then, analyzed and calculated its system performance for both BSAs and IRAs. The results showed that short- or middle-range QKD is achievable with our scheme. With the features of use of conventional intensity-modulation/direct-detection technologies, our scheme is suitable for small- or moderate-size networks such as LANs and MANs.

References

[1] Bennett C H and Gilles B 1984 *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing. Bangalore, India* vol 175

[2] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 0379021

[3] Zhao Y, Heid M, Rigas J and Lütkenhaus N 2009 *Phys. Rev.* A **79** 012307

[4] Jouguet P, Kunz-Jacques S, Leverrier A and Grangier P 2013 *Nat. Photonics* **7** 378

[5] Inoue K and Hayashi S 2007 *Presented at QELS* QML7

[6] Kukita T, Takada H and Inoue K 2010 *Japan. J. Appl. Phys.* **49** 122801

[7] Shannon C E 1948 *Bell Syst. Tech. J.* **27** 623–56

[8] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photonics* **1** 343–8

[9] Shibata H, Honjo T and Shimizu K 2014 *Opt. Lett.* **39** 5078

[10] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[11] Manderbach T S *et al* 2007 *Phys. Rev. Lett.* **98** 010504