Quantum Information Processing (2019) 18:73
https://doi.org/10.1007/s11128-018-2167-4

Longer distance continuous variable quantum key distribution protocol with photon subtraction at the receiver

Kyongchun Lim[1] · Changho Suh[1] · June-Koo Kevin Rhee[1]

Received: 6 August 2018 / Accepted: 26 December 2018 / Published online: 28 January 2019

Abstract
One of the limitations of continuous variable quantum key distribution is the relatively short transmission distance of secure keys. Some solutions have been proposed to overcome the limitation including reverse reconciliation, trusted noise concept, and non-Gaussian operation. In this paper, we propose a protocol using photon subtraction at the receiver, which combines the synergetic benefits of the aforementioned approaches. Using simulations, we show that the performance of the proposed protocol outperforms other conventional protocols. The results showed that an improvement in secure key distance can be obtained using a non-Gaussian operation, depending on the position where the operation is performed, similar to the trusted noise concept. Furthermore, the result implies existence of some Gaussian operations which increases security without using a beam splitter.

Keywords Quantum cryptography · Continuous variable quantum key distribution · Non-Gaussian state · Quantum information and processing

1 Introduction

Quantum key distribution (QKD) is one of the realistic applications that have been developed for quantum technologies. Technically, QKD provides shared secret keys between two remote parties, such as Alice and Bob. Because of its unconditional secu-

✉ Kyongchun Lim
lim.kc@kaist.ac.kr

Changho Suh
chsuh@kaist.ac.kr

June-Koo Kevin Rhee
rhee.jk@kaist.ac.kr

[1] School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, Korea

rity, QKD has attracted broad research interest since the introduction of the first QKD protocol, the BB84 protocol, which was invented in 1984 [1]. In the early days, many studies actively focused on discrete variable QKD (DVQKD). Following the proposal by [2], continuous variable QKD (CVQKD), which encoded secret key information on a continuous degree of freedom in the phase space of a quantum state, started to gain interest [2–4]. Unlike DVQKD, CVQKD has high secure key rates at short distances due to the high dimensionality of the continuous variable, but it was difficult to achieve key sharing over a long distance currently. One of the main reasons for the limited distance is the low error correction efficiency at a long distance under Gaussian-based CVQKD protocols [5]. In order to overcome the hurdle, a variety of post-processing methods have been proposed, such as post-selection [6], multi-dimensional reconciliation [5], and reverse reconciliation [7]. The reverse reconciliation method in particular can overcome the limit using the simple approach of changing the reference of error correction, which provides importance on the receiver side in the CVQKD protocols. There are also many proposals which modify the quantum channel. Some proposals utilize amplifiers, including a noiseless amplifier [8–10], while others change the transmitter to use four-state or eight-state Gaussian states [11–13]. The protocol changing the transmitter has been also proposed based on a different approach where it simplifies the transmitter to increase practicality of a system of CVQKD [14,15]. As a way to increase distance, the trusted noise concept was proposed, in which a noise is added in a specific way to increase security [16]. For example, noise added by the receiver, Bob, can increase security in a CVQKD protocol with reverse reconciliation.

In a departure from Gaussian state protocols, non-Gaussian state protocols have been investigated because of their potential to provide high security in terms of secure key rate and distance [17–20]. One of the representative non-Gaussian operations used in a CVQKD protocol is photon subtraction, which is implemented with a beam splitter and a photon counter [19–21]. This approach shows that distance can be improved using photon-subtracted states. In case of [19–21], those works are similar to the work of this paper in terms of using photon subtraction. Here, Huang et al. [19] and Li et al. [20] studied the CVQKD protocol using photon subtraction at a transmitter where an entangled source is placed, while [21] studied the both cases for photon subtraction at a transmitter and a receiver with a different network structure where the entangled source is located at the third part which is not a transmitter or a receiver. However, we provide the CVQKD protocol using photon subtraction at a receiver with an entangled source in a transmitter as in [19,20], but we find different results based on more adequate analyses.

In this paper, we propose a CVQKD protocol utilizing the aforementioned properties. Specifically, the protocol is a reverse reconciliation-based CVQKD protocol adopting a photon subtraction operation on the receiver side. Here, the photon subtraction operation is non-Gaussian and can be considered an operation that adds noise. Through numerical simulations, we show that the proposed protocol outperforms conventional CVQKD protocols. This result coincides with other current research results that demonstrate the positive potentials of non-Gaussian operations, and trusted noise, in terms of security, which provided further confirmation that our approach is quite reasonable.

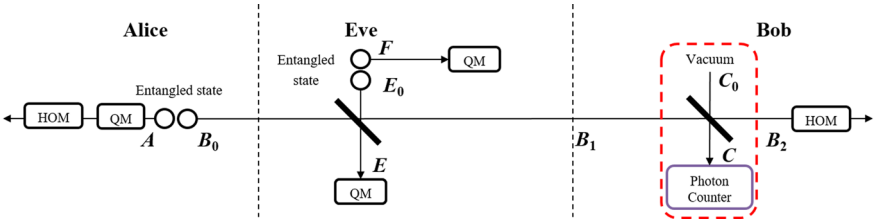

Fig. 1 A model for CVQKD with photon subtraction under a collective attack. HOM and QM stand for homodyne detection and quantum memory, respectively

The paper is organized as follows. We introduce a target system model in Sect. 2. A secure key rate based on the model is obtained in Sect. 3. Section 4 provides numerical simulations for secure key rates under the model. We finalize the paper in Sect. 5 with some concluding remarks.

2 System model

In this section, we introduce a system model for a CVQKD protocol with photon subtraction at a receiver, Bob, as shown in Fig. 1. Here, a transmitter, Alice prepares a two mode squeezed vacuum (TMSV) state $|\psi\rangle_{AB_0}$ which is an entangled state in a continuous variable domain.

$$|\psi\rangle_{AB_0} = \sum_{n=0}^{\infty} \alpha_n \, |n, n\rangle_{AB_0}, \tag{1}$$

where $\alpha_n = \sqrt{\alpha^{2n}/\left(1+\alpha^2\right)^{n+1}}$ and $\alpha = \sinh r$. Here, r, α^2 and $|n\rangle$ represent a squeezing parameter, mean photon number, and number state, respectively.

In this model, we assume a collective attack where an Eve's initial state is prepared as a TMSV state $|\psi\rangle_{E_0F}$. Similar to $|\psi\rangle_{AB_0}$, $|\psi\rangle_{E_0F}$ can be expressed with a mean photon number of noise from a channel, β^2.

$$|\psi\rangle_{E_0F} = \sum_{m=0}^{\infty} \beta_m \, |m, m\rangle_{E_0F}, \tag{2}$$

where $\beta_m = \sqrt{\beta^{2m}/\left(1+\beta^2\right)^{m+1}}$. After preparing $|\psi\rangle_{AB_0}$, Alice transmits a quantum state $\rho_{B_0} = \mathrm{Tr}_A\left(|\psi\rangle\langle\psi|_{AB_0}\right)$ of $|\psi\rangle_{AB_0}$ to Bob through a quantum channel, while the other quantum state $\rho_A = \mathrm{Tr}_{B_0}\left(|\psi\rangle\langle\psi|_{AB_0}\right)$ is kept in a quantum memory. The transmitted ρ_{B_0} is mixed with Eve's state $\rho_{E_0} = \mathrm{Tr}_F\left(|\psi\rangle\langle\psi|_{E_0F}\right)$ in the channel. Here, the channel is based on the standard telecommunication optical fiber, with a per unit length loss of $\mu = 0.2\,\mathrm{dB/km}$ for a wavelength of around 1550 nm. Therefore, the channel can be modeled as a beam splitter with transmittance T represented as $T = \eta 10^{-\mu d/10}$ where η and d are detector efficiency and distance, respectively.

Before finding a quantum state after a channel, we first look into the principle of a beam splitter. Assume there is a beam splitter characterized by transmittance T, where there are two input creation operators $\hat{i}_1^\dagger$, $\hat{i}_2^\dagger$ and two output creation operators $\hat{o}_1^\dagger$, $\hat{o}_2^\dagger$. In this setup, the input operators can be expressed based on the output operators as follows:

$$\hat{i}_1^\dagger = \sqrt{T}\hat{o}_1^\dagger - \sqrt{1-T}\hat{o}_2^\dagger, \tag{3}$$

$$\hat{i}_2^\dagger = \sqrt{T}\hat{o}_2^\dagger + \sqrt{1-T}\hat{o}_1^\dagger. \tag{4}$$

Now, we can find a quantum state after a channel $|\psi\rangle_{AB_1EF}$ based on the initial states of Alice and Eve by applying a beam splitter operation to them. The relation between the number state and the creation operator such that $\hat{a}^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle$ and the beam splitter operation results in the following equation.

$$|\psi\rangle_{AB_0E_0FB_1E} = \sum_{n=0}^{\infty} \alpha_n |n,n\rangle_{AB_0} \sum_{m=0}^{\infty} \beta_m |m,m\rangle_{E_0F} |0,0\rangle_{B_1E}, \tag{5}$$

$$= \sum_{n=0}^{\infty} \alpha_n \frac{\left(\hat{b}_0^\dagger\right)^n}{\sqrt{n!}} |n,0\rangle_{AB_0} \sum_{m=0}^{\infty} \beta_m \frac{\left(\hat{e}_0^\dagger\right)^n}{\sqrt{m!}} |0,m\rangle_{E_0F} |0,0\rangle_{B_1E}, \tag{6}$$

$$= \sum_{n=0}^{\infty} \alpha_n \frac{\left(\sqrt{T}\hat{b}_1^\dagger - \sqrt{1-T}\hat{e}^\dagger\right)^n}{\sqrt{n!}} |n,0\rangle_{AB_0} \otimes \sum_{m=0}^{\infty} \beta_m \frac{\left(\sqrt{T}\hat{e}^\dagger + \sqrt{1-T}\hat{b}_1^\dagger\right)^n}{\sqrt{m!}} |0,m\rangle_{E_0F} |0,0\rangle_{B_1E}, \tag{7}$$

$$= \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^{n} (-1)^k \sqrt{\binom{n}{k}} \left(\sqrt{T}\right)^{n-k} \left(\sqrt{1-T}\right)^k |n,0\rangle_{AB_0} \otimes \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \sqrt{\binom{m}{l}} \left(\sqrt{T}\right)^{m-l} \left(\sqrt{1-T}\right)^l \sqrt{\binom{n-k+l}{l}} \sqrt{\binom{k+m-l}{k}} |0,m\rangle_{E_0F} |n-k+l, k+m-l\rangle_{B_1E}, \tag{8}$$

where $\hat{a}^\dagger$ indicates the creation operator of quantum state ρ_A. We can easily obtain $|\psi\rangle_{AB_1EF}$ by tracing out and rearranging $|\psi\rangle_{AB_0E_0FB_1E}$.

$$|\psi\rangle_{AB_1EF} = \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^{n} (-1)^k \gamma_{n,k}^T \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \gamma_{m,l}^T \zeta_{n,k,m,l} |n, n-k+l, k+m-l, m\rangle_{AB_1EF}, \tag{9}$$

where

$$\gamma_{n,k}^{T} = \sqrt{\binom{n}{k}} \left(\sqrt{T}\right)^{n-k} \left(\sqrt{1-T}\right)^{k}, \tag{10}$$

$$\zeta_{n,k,m,l} = \sqrt{\binom{n-k+l}{l}} \sqrt{\binom{k+m-l}{k}}. \tag{11}$$

In a similar way, the quantum state after photon subtraction, represented as a beam splitter with transmittance T_1, $|\psi\rangle_{AB_2EFC}$, can be obtained as follows:

$$|\psi\rangle_{AB_2EFC} = \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^{n} (-1)^k \gamma_{n,k}^{T} \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \gamma_{m,l}^{T} \zeta_{n,k,m,l} \sum_{s=0}^{n-k+l} (-1)^s \gamma_{n-k+l,s}^{T_1} |n, n-k+l-s, k+m-l, m, s\rangle_{AB_2EFC}. \tag{12}$$

For easy understanding, we first analyze a single-photon-subtracted case where C is a single-photon state. Then, the photon-subtracted state $|\psi\rangle \langle\psi|_{AB_2EF}^{\mathrm{PS}} = \mathrm{Tr}_C \left(|\psi\rangle \langle\psi|_{AB_2EFC}^{\mathrm{PS}} |_{s=1}\right)$ has the following expression.

$$|\psi\rangle_{AB_2EF}^{\mathrm{PS}} = -\frac{1}{\sqrt{P_1}} \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^{n} (-1)^k \gamma_{n,k}^{T} \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^{m} \gamma_{m,l}^{T} \zeta_{n,k,m,l} \gamma_{n-k+l,1}^{T_1} |n, n-k+l-1, k+m-l, m\rangle_{AB_2EF}, \tag{13}$$

where $P_1 = \langle\psi|\psi\rangle_{AB_2EF}^{\mathrm{PS}}$, based on unnormalized $|\psi\rangle_{AB_2EF}^{\mathrm{PS}}$, a normalization parameter, defined as the probability that C is in a single-photon state.

$$P_1 = \sum_{n=0}^{\infty} \alpha_n^2 \sum_{k=0}^{n} \sum_{m=0}^{\infty} \beta_m^2 \sum_{l=0}^{m} \left(J_{(n,k,m,l),(n,k,m,l)}^{+} + J_{(n,k,m,l)(n,k,m,l)}^{-}\right), \tag{14}$$

where

$$J_{(n_1,k_1,m_1,l_1)(n_2,k_2,m_2,l_2)}^{+} = \sum_{j=0}^{\min\{n_2-k_2,m_2-l_2\}} (-1)^j \gamma_{n_1,k_1}^{T} \gamma_{n_2,k_2+j}^{T} \gamma_{m_1,l_1}^{T} \gamma_{m_2,l_2+j}^{T} \zeta_{n_1,k_1,m_1,l_1} \zeta_{n_2,k_2+j,m_2,l_2+j} \gamma_{n_1-k_1+l_1,1}^{T_1} \gamma_{n_2-k_2+l_2,1}^{T_1}, \tag{15}$$

$$J_{(n_1,k_1,m_1,l_1)(n_2,k_2,m_2,l_2)}^{-} = \sum_{j=1}^{\min\{k_2,l_2\}} (-1)^j \gamma_{n_1,k_1}^{T} \gamma_{n_2,k_2-j}^{T} \gamma_{m_1,l_1}^{T} \gamma_{m_2,l_2-j}^{T} \zeta_{n_1,k_1,m_1,l_1} \zeta_{n_2,k_2-j,m_2,l_2-j} \gamma_{n_1-k_1+l_1,1}^{T_1} \gamma_{n_2-k_2+l_2,1}^{T_1}. \tag{16}$$

Finally, we obtain the quantum state after photon subtraction $|\psi\rangle^{\mathrm{PS}}_{AB_2EF}$ which is not a Gaussian state anymore. Then, $|\psi\rangle^{\mathrm{PS}}_{AB_2EF}$ can be measured by a homodyne detector with respect to q or p quadrature with equal probability. After the choice of quadrature is publicly announced to Alice, the ρ_A kept in a quantum memory is measured by the homodyne detector with respect to the quadrature. Here, we can consider the time required to implement the quantum memory on Alice's side. Because our proposed protocol can transmit about 100 km with optical fiber, as will be shown in Sect. 4, the quantum memory requires approximately more than 1 ms. This required time can be sufficiently satisfied with current technologies [22,23] where a quantum memory has more than 10 min coherence time. In practice, the measurement of an entangled pair can be replaced equivalently by a random Gaussian modulation on a squeezed state transmitted toward Bob without loss of generality. On the other hand, the quantum memory can be removed by losing the secure key rate. In this case, the secure key rate becomes half because the bases of Alice and Bob match with 1/2. In succession, Alice and Bob perform reverse reconciliation and privacy amplification to generate the final secure keys.

3 Secure key rate

In this section, we calculate the secure key rate of our system model, corresponding to a one-photon subtraction case based on an infinite key length. This approach is generally conducted for newly proposed protocols as in [10,16–20,24]. Under a collective attack, the secure key rate K can be calculated as follows:

$$K = P_1 \{ f I(A\colon B_2) - \chi(B_2\colon EF) \}, \tag{17}$$

where f is reconciliation efficiency. Here, $I(A\colon B_2)$ represents mutual information between Alice and Bob, while $\chi(B_2\colon EF)$ refers to the Holevo information, defined as the maximum information extracted by Eve from Bob's data. Calculating $I(A\colon B_2)$ and $\chi(B_2\colon EF)$ starts from a photon-subtracted state with a density matrix $\rho^{\mathrm{PS}}_{AB_2EF} = |\psi\rangle\langle\psi|^{\mathrm{PS}}_{AB_2EF}$. In the case of $\chi(B_2\colon EF)$, it can be calculated by

$$\chi(B_2\colon EF) = S\left(\rho^{\mathrm{PS}}_{EF}\right) - S\left(\rho^{\mathrm{PS}}_{EF|B_2}\right), \tag{18}$$

$$= -\sum_i \lambda_i^{EF} \log_2 \lambda_i^{EF} + \sum_i \lambda_i^{EF|B_2} \log_2 \lambda_i^{EF|B_2}, \tag{19}$$

where $S(\cdot)$ represents von Neumann entropy. Here, the density matrix for an Eve's state is denoted as ρ^{PS}_{EF} having eigenvalues $\{\lambda_i^{EF}\}$, while a density matrix for an Eve's state given Bob's measurement on B_2 is represented as $\rho^{\mathrm{PS}}_{EF|B_2}$ with eigenvalues $\{\lambda_i^{EF|B_2}\}$. Note that there are an infinite number of $\{\lambda_i^{EF}\}$ and $\{\lambda_i^{EF|B_2}\}$ due to the infinite dimensions of ρ^{PS}_{EF} and $\rho^{\mathrm{PS}}_{EF|B_2}$. Therefore, infinite eigenvalues and their infinite sum make calculation of $\chi(B_2\colon EF)$ intractable.

If we remove one of the two calculations, the intractability of $\chi(B_2{:}EF)$ can be improved. Removing the calculation of infinite eigenvalues can be done if all states are Gaussian states, because $S(\cdot)$ of a Gaussian state can be calculated based on its covariance matrix having finite dimension. In order to do that, we substitute a photon subtraction operation with a Gaussian unitary operation making the same covariance matrix with $\Gamma^{\mathrm{PS}}_{AB_2EF}$ of $\rho^{\mathrm{PS}}_{AB_2EF}$. This provides a lower bound of the original protocol in terms of performance by the theorem of Gaussian optimality [25]. Define a state made by the Gaussian unitary operation as $\rho^{\mathrm{G}}_{AB_2EF}$ with $\Gamma^{\mathrm{G}}_{AB_2EF} = \Gamma^{\mathrm{PS}}_{AB_2EF}$. Then, by the theorem,

$$K \geq P_1 \left\{ f I_G(A{:}B_2) - \chi_G(B_2{:}EF) \right\}, \tag{20}$$

where $I_G(A{:}B_2)$ and $\chi_G(B_2{:}EF)$ represent mutual information between Alice and Bob and the Holevo information obtained from $\rho^{\mathrm{G}}_{AB_2EF}$, respectively. Since $\rho^{\mathrm{G}}_{AB_2EF}$ is a Gaussian state, $I_G(A{:}B_2)$ and $\chi_G(B_2{:}EF)$ can be easily obtained from a covariance matrix of $\Gamma^{\mathrm{G}}_{AB_2EF}$.

In order to calculate $\Gamma^{\mathrm{PS}}_{AB_2EF}$, we first look into the structure of a covariance matrix. Define an operator vector $\hat{x}$ as $\hat{x} = \left(\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N\right)^\top$, where $\hat{q}_i$ and $\hat{p}_i$ are quadrature operators of the ith mode out of N modes. Then, an element of the covariance matrix Γ is defined as

$$\Gamma_{ij} = \frac{1}{2} \left\langle \Delta\hat{x}_i \Delta\hat{x}_j + \Delta\hat{x}_j \Delta\hat{x}_i \right\rangle, \tag{21}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle \hat{x}_i \rangle$. In general, Γ_{ij} indicates a correlation between modes i and j, while a diagonal element Γ_{ii} indicates a variance of mode i. From now on, for easy understanding, we substitute Γ_{ii} and Γ_{ij} for V_i and C_{ij}, respectively.

Since $\rho^{\mathrm{G}}_{AB_2EF}$ is a Gaussian state, $I_G(A{:}B_2)$ is calculated as follows:

$$I_G(A{:}B_2) = \frac{1}{2} \log_2 \frac{V_{B_2}}{V_{B_2|A}}, \tag{22}$$

where $V_{B_2|A}$ is a conditional variance of Bob's data given Alice's data. Since the q and p quadrature operators are independent and symmetric in terms of probability distribution, V_{B_2} is invariant with respect to the quadratures.

$$\begin{aligned} V_{B_2} &= \frac{1}{2} \left\langle \Delta\hat{q}_{B_2} \Delta\hat{q}_{B_2} + \Delta\hat{q}_{B_2} \Delta\hat{q}_{B_2} \right\rangle, && (23) \\ &= \langle \psi | 1 + 2\hat{b}_2^\dagger \hat{b}_2 | \psi \rangle^{\mathrm{PS}}_{AB_2EF}, && (24) \\ &= 1 + \frac{2}{P_1} \sum_{n=0}^{\infty} \alpha_n^2 \sum_{k=0}^{n} \sum_{m=0}^{\infty} \beta_m^2 \sum_{l=0}^{m} (n-k+l-1) \\ &\quad \times \left(J^{+}_{(n,k,m,l),(n,k,m,l)} + J^{-}_{(n,k,m,l)(n,k,m,l)} \right) u(n-k+l-1), && (25) \end{aligned}$$

where $u(\cdot)$ is a step function defined as

$$u(x) = \begin{cases} 1, & \text{if } x \geq 1 \\ 0, & \text{otherwise.} \end{cases} \tag{26}$$

The second equality holds since $\langle \hat{q}_{B_2} \rangle = 0$ and the relations that $\hat{q} = \hat{b}_2^\dagger + \hat{b}_2$ and $\hat{b}_2 \hat{b}_2^\dagger - \hat{b}_2^\dagger \hat{b}_2 = 1$.

In the case of $V_{B_2|A}$ where B_2 given A follows a Gaussian distribution, this can be obtained as follows:

$$V_{B_2|A} = V_{B_2} - \frac{C_{AB_2}}{V_A}, \tag{27}$$

where

$$V_A = 1 + \frac{2}{P_1} \sum_{n=0}^{\infty} \alpha_n^2 \sum_{k=0}^{n} \sum_{m=0}^{\infty} \beta_m^2 \sum_{l=0}^{m} n \left(J^+_{(n,k,m,l),(n,k,m,l)} + J^-_{(n,k,m,l)(n,k,m,l)} \right), \tag{28}$$

and

$$C_{AB_2} = \frac{1}{2} \langle \Delta \hat{q}_A \Delta \hat{q}_{B_2} + \Delta \hat{q}_{B_2} \Delta \hat{q}_A \rangle, \tag{29}$$

$$= \frac{2}{P_1} \sum_{n=0}^{\infty} \alpha_n \alpha_{n+1} \sum_{k=0}^{n} \sum_{m=0}^{\infty} \beta_m^2 \sum_{l=0}^{m} \sqrt{n+1} \sqrt{n-k+l} \times \left(J^+_{(n,k,m,l),(n+1,k,m,l)} + J^-_{(n,k,m,l)(n+1,k,m,l)} \right). \tag{30}$$

In the case of Eve's information, for a Gaussian state, the Holevo information becomes

$$\chi_G(B_2 : EF) = \sum_i g\left(v_i^{EF}\right) - \sum_j g\left(v_j^{EF|B_2}\right), \tag{31}$$

where

$$g(x) = \left(\frac{x+1}{2}\right) \log_2 \left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right) \log_2 \left(\frac{x-1}{2}\right) \tag{32}$$

Here, v_i^{EF} and $v_j^{EF|B_2}$ indicate an ith symplectic eigenvalue of a covariance matrix for Eve's state Γ_{EF}^G and a jth symplectic eigenvalue of a covariance matrix for Eve's state given Bob's measurement $\Gamma_{EF|B_2}^G$, respectively. Specifically, v_i^{EF} and $v_i^{EF|B_2}$ are calculated as absolute eigenvalues of $\sqrt{-1}\Omega\Gamma_{EF}^G$ and $\sqrt{-1}\Omega\Gamma_{EF|B_2}^G$, where $\Omega =$

$\bigoplus_{i=1}^{N}\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$. For the symplectic eigenvalues, it is necessary to find the structures of Γ_{EF}^{G} and $\Gamma_{EF|B_2}^{G}$, which are obtained from $\Gamma_{EFB_2}^{G}$. Elements of $\Gamma_{EFB_2}^{G}$ can be directly calculated by using Eq. (21), which provides the following form.

$$\Gamma_{EFB_2}^{G}=\begin{bmatrix}\Gamma_{EF}^{G} & \mathbf{L}_{EFB_2}\\ \mathbf{L}_{EFB_2} & \Gamma_{B_2}^{G}\end{bmatrix}, \tag{33}$$

where

$$\Gamma_{EF}^{G}=\begin{bmatrix}V_E\mathbf{I}_2 & C_{EF}\sigma_z\\ C_{EF}\sigma_z & V_F\mathbf{I}_2\end{bmatrix}, \tag{34}$$

$$\mathbf{L}_{EFB_2}=\begin{bmatrix}C_{EB_2}\mathbf{I}_2\\ C_{FB_2}\sigma_z\end{bmatrix}, \tag{35}$$

where $\mathbf{I}_2$ and σ_z represent the two dimensional identity matrix and Pauli z operator, respectively. Γ_{EF}^{G} is directly obtained from $\Gamma_{EFB_2}^{G}$, while $\Gamma_{EF|B_2}^{G}$ is obtained from it by using the following relation [26].

$$\Gamma_{EF|B_2}^{G}=\Gamma_{EF}^{G}-\mathbf{L}_{EFB_2}\left(\Pi\Gamma_{B_2}^{G}\Pi\right)^{\mathrm{MP}}\mathbf{L}_{EFB_2}^{\top}, \tag{36}$$

where MP refers to the Moore–Penrose pseudoinverse [26].

Based on this, the elements of the covariance matrix in Eq. (34) are as follows:

$$\begin{aligned}V_E=1+\frac{2}{P_1}\sum_{n=0}^{\infty}\alpha_n^2\sum_{k=0}^{n}\sum_{m=0}^{\infty}\beta_m^2\sum_{l=0}^{m}(k+m-l)\\ \times\left(J^{+}_{(n,k,m,l),(n,k,m,l)}+J^{-}_{(n,k,m,l)(n,k,m,l)}\right),\end{aligned} \tag{37}$$

$$\begin{aligned}V_F=1+\frac{2}{P_1}\sum_{n=0}^{\infty}\alpha_n^2\sum_{k=0}^{n}\sum_{m=0}^{\infty}\beta_m^2\sum_{l=0}^{m}m\\ \times\left(J^{+}_{(n,k,m,l),(n,k,m,l)}+J^{-}_{(n,k,m,l)(n,k,m,l)}\right),\end{aligned} \tag{38}$$

$$\begin{aligned}C_{EF}=\frac{2}{P_1}\sum_{n=0}^{\infty}\alpha_n^2\sum_{k=0}^{n}\sum_{m=0}^{\infty}\beta_m\beta_{m+1}\sum_{l=0}^{m}\sqrt{m+1}\sqrt{k+m-l+1}\\ \times\left(J^{+}_{(n,k,m,l),(n,k,m+1,l)}+J^{-}_{(n,k,m,l)(n,k,m+1,l)}\right),\end{aligned} \tag{39}$$

$$\begin{aligned}C_{EB_2}=\frac{2}{P_1}\sum_{n=0}^{\infty}\alpha_n^2\sum_{k=0}^{n}\sum_{m=0}^{\infty}\beta_m^2\sum_{l=0}^{m}\sqrt{n-k+l}\sqrt{k+m-l}\\ \times\left(J^{+}_{(n,k,m,l),(n,k,m,l+1)}+J^{-}_{(n,k,m,l)(n,k,m,l+1)}\right),\end{aligned} \tag{40}$$

$$\begin{aligned}C_{FB_2}=\frac{2}{P_1}\sum_{n=0}^{\infty}\alpha_n^2\sum_{k=0}^{n}\sum_{m=0}^{\infty}\beta_m\beta_{m+1}\sum_{l=0}^{m}\sqrt{m+1}\sqrt{n-k+l}\\ \times\left(J^{+}_{(n,k,m,l),(n,k,m+1,l+1)}+J^{-}_{(n,k,m,l)(n,k,m+1,l+1)}\right).\end{aligned} \tag{41}$$

Equations (31) and (33) based on the above equations provide the corresponding Holevo information.

The aforementioned analysis deals with the one-photon subtraction case. In a similar way, general photon subtraction cases can also be analyzed by adjusting the summation of s in Eq. (12). Furthermore, instead of a photon counter for photon subtraction, it can be analyzed with a photon detector, such as Si or InGaAs single-photon avalanche photon diodes (SPAD). This case is analyzed by summing s from 1 to ∞ in Eq. (12) and normalizing it.

4 Simulation results

In this section, we perform three simulations. In order to check the feasibility of the proposed protocol, we compare the performances of a photon detector and photon counter. Based on the results of the first simulation, we then compare the performance of the proposed protocol with other conventional protocols. Finally, we simulate the maximum transmission distances for protocols with respect to the mean photon number of noise from a channel to analyze the effective region of the proposed protocol.

The proposed protocol is initially based on a photon counter for photon subtraction. However, a sophisticated photon counter is hard to implement and expensive. On the other hand, a photon detector with no photon number resolution is relatively easy to implement and costs less. For an analysis of a more practical case, we compare two cases, with a photon counter and a photon detector for photon subtraction.

Here, the photon counter case corresponds to a one-photon subtraction case. We set the reconciliation efficiency f, detector efficiency η, mean photon number of noise from a channel β^2, and transmittance T_1 of the beam splitter of Bob as 0.95, 0.68, 0.001, and 0.9, respectively. Here, detector efficiency is based on the detector [27], and Alice's modulation variance for each case is optimized for the distance. Note that the expressions of the results require infinite sums. For the simulation, we truncate the marginal portion of the summations by setting infinity to 30 in the summations.

The corresponding results are shown in Fig. 2. The blue dashed and red solid lines indicate the cases of the photon counter and photon detector, respectively. From the results, we determined that the photon detector case was slightly more secure than the photon counter. This indicates that the proposed protocol is rather more secure, even for a practical case. Furthermore, this trend in the results means that the one-photon subtraction occupies a dominant part of the performance in the photon detector case.

Next, we conduct performance comparisons between the proposed protocol with a photon detector and other conventional protocols. For the performance comparison, we simulate the secure key rates of a conventional CVQKD corresponding to a CVQKD without photon subtraction, and a CVQKD proposed in [28] where the trusted noise concept is used for better security. For comparison, we also simulate a CVQKD protocol using photon subtraction in Alice [19]. Here, we set the simulation parameters to be the same as those in the first simulation. The variance in modulation of each protocol is optimized in terms of secure distance. The ratio of the beam splitter of the protocol in [19] is also optimized for secure distance. The corresponding results are plotted in Fig. 3.

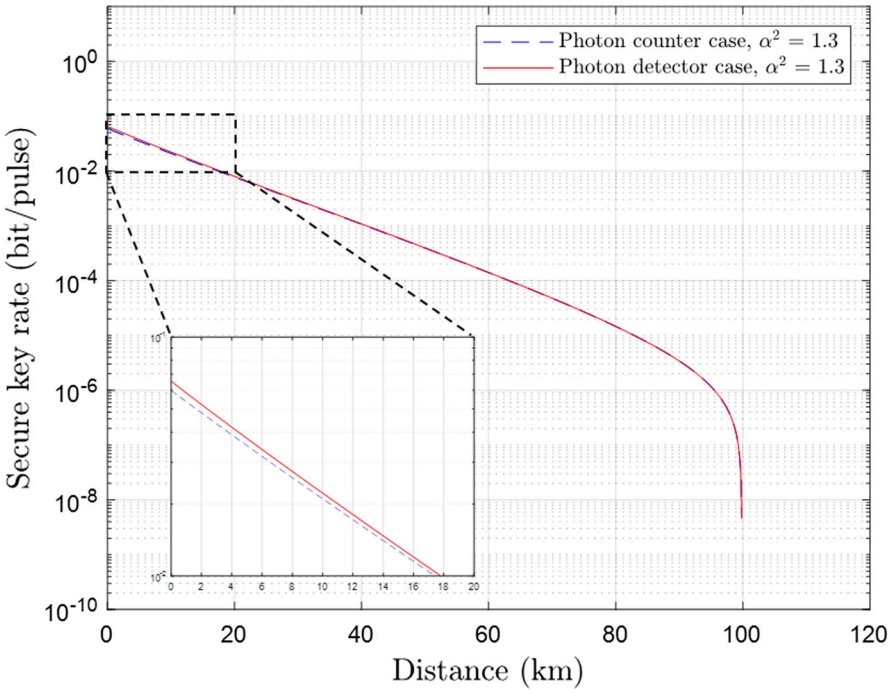

Fig. 2 Comparisons for secure key rate depending on devices used for photon subtraction

The red, green, blue, and black lines indicate a conventional CVQKD, a CVQKD with trusted noise, the proposed protocol, and a CVQKD with one-photon subtraction in Alice, respectively. From the results, we first find that the CVQKD protocol with the photon subtraction in Alice has the lowest performance. This is a different result than the results in [19]. The difference comes from the modulation variances that were used. We used optimized variances for each protocol, while the same variances were used in [19]. Therefore, the result indicates that a photon subtraction operation in Alice under a reverse reconciliation-based CVQKD protocol does not provide any advantages at all.

We also find that our proposed protocol can transmit secure keys at a longer distance, although it shows a lower secure key rate at extended distances. This means that photon subtraction can increase Eve's uncertainty more, even if it decreases the correlation between Alice and Bob, which is shown in Fig. 4. Since photon subtraction can be seen as an operation adding noise, this also indicates that a combination of reverse reconciliation, the trusted noise concept, and non-Gaussian operation has positive synergy in terms of security, compared with using partial properties.

The result provides one more interesting point. Note that the performance of the protocol was analyzed based on Gaussian states due to Gaussian optimality, and it shows more security than [28] in some distances. As [28] improves security by adding a beam splitter on a receiver of the conventional CVQKD protocol, the proposed protocol improves security by adding the non-Gaussian operation on receiver. The operation can be eventually seen as a Gaussian operation by Gaussian optimality

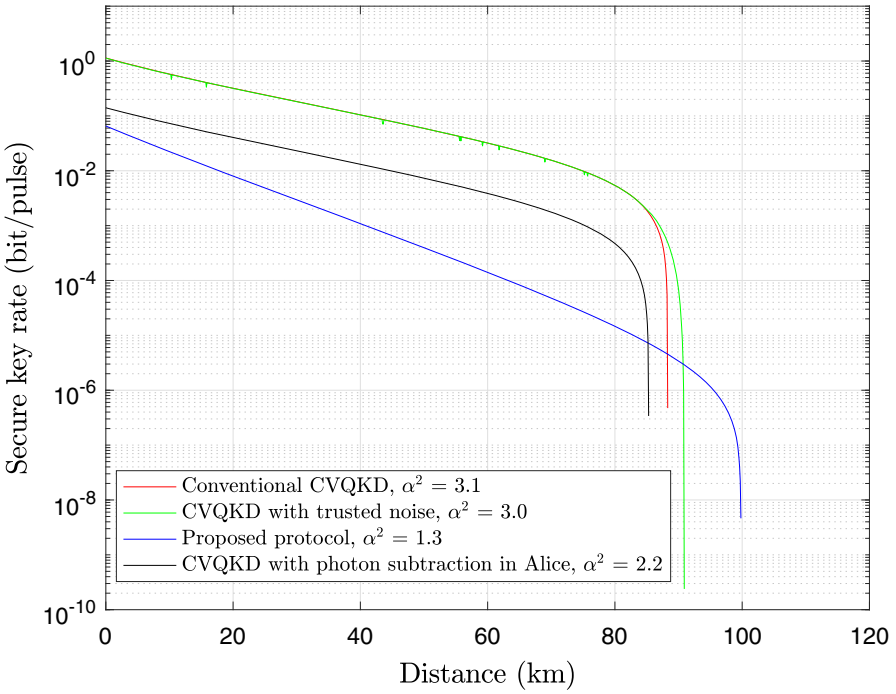

Fig. 3 Comparisons for secure key rate of CVQKD protocols. The mean photon number α^2 is optimized for each case to have the maximum secure key rate

theorem. This indicates that there can exist such Gaussian operation which is not a simple beam splitter.

Finally, we conduct simulations to determine the maximum transmission distances of the protocols with respect to the mean photon number of noise from a channel β^2. Here, the maximum distance is defined as the maximum distance with a positive secure key rate. Simulation parameters are the same as in the aforementioned simulations. As shown by the results in Fig. 5, the performance improvement from the proposed protocol decreases as β^2 increases, which means that the performance improvement of the proposed protocol is bounded within a certain channel noise region. Using this as a guide for system provisioning, we can utilize the proposed protocol depending on the conditions of a system.

5 Conclusion

In this paper, we investigated a method to improve the secure distance of CVQKD. As a result, we determined a protocol which increases Eve's uncertainty, even while it reduces the correlation between Alice and Bob over extended distances. The protocol utilizes a non-Gaussian operation, reverse reconciliation, and trusted noise concept, which leads to a new reverse reconciliation-based CVQKD protocol with photon-subtracted states at the receiver. In order to overcome the intractability of the calcu-

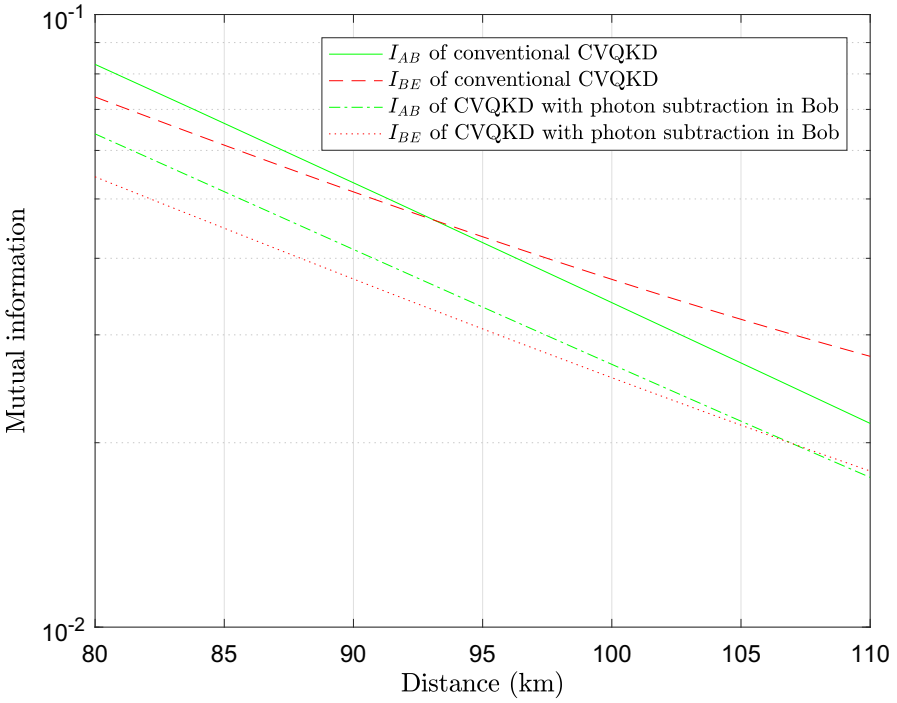

Fig. 4 Comparisons for mutual information depending presence of photon subtraction. Here, the mutual information is used to evaluate the secure key rate in Fig. 3

lation for secure key rate, we utilized the Gaussian optimality theorem, which yields a lower bound of secure key rate under the proposed protocol. From the simulation results, we found that the proposed protocol can improve secure distance. The proposed protocol outperformed even in a practical case where a photon detector was used.

The results for our protocol show that the combination of non-Gaussian operation, reverse reconciliation, and trusted noise concept can extend secure distance in the practical application regime with imperfect error correction, where optimal modulation variance is finite. In particular, the proposed protocol showed better performance than a CVQKD protocol with a photon subtraction in Alice. Furthermore, the result provided a clue that there can exist some Gaussian operations which increases security without using a beam splitter.

Furthermore, even with our protocol, the extended secure distance can be bounded by a range of channel noise, which can provide guidance in designing long distance CVQKD systems. Finally, we can expect a much longer distance by merging a quantum repeater protocol with our protocol. Since the final state of the currently proposed quantum repeater protocol makes a Gaussian state [29], our protocol can be easily applied to the quantum repeater protocol by just adding a photon subtraction operation in the last receiver. From this point of view, our protocol is more effective than the protocol using photon subtraction in Alice's side, since it requires a new quantum repeater protocol to distribute the desired state, corresponding to a photon-subtracted state.

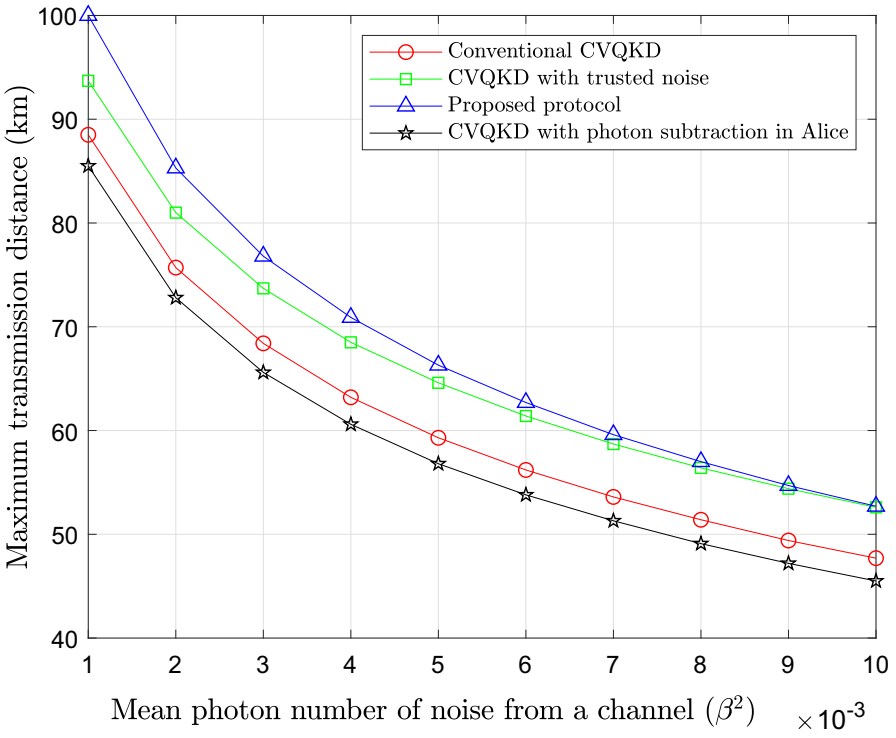

Fig. 5 Comparisons of the maximum transmission distance with respect to mean photon number of noise from a channel, for various CVQKD protocols

Acknowledgements This work was supported by the ICT R&D program of MSIT/IITP (1711073835, Reliable crypto-system standards and core technology development for secure quantum key distribution network) and the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2018-0-01402) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

1. Bennett, C., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE (1984)
2. Ralph, T.C.: Continuous variable quantum cryptography. Phys. Rev. A **61**, 010303 (1999)
3. Diamanti, E., Leverrier, A.: Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy **17**(9), 6072 (2015)
4. Li, Y.M., Wang, X.Y., Bai, Z.L., Liu, W.Y., Yang, S.S., Peng, K.C.: Continuous variable quantum key distribution. Chin. Phys. B **26**(4), 040303 (2017)
5. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., Grangier, P.: Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. A **77**, 042325 (2008)
6. Silberhorn, C., Ralph, T.C., Lütkenhaus, N., Leuchs, G.: Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys. Rev. Lett. **89**, 167901 (2002)
7. Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N., Grangier, P.: Quantum key distribution using Gaussian-modulated coherent states. Nature **421**(6920), 238 (2003)

8. Fiurášek, J., Cerf, N.J.: Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys. Rev. A **86**, 060302 (2012)
9. Zhang, Y.C., Li, Z., Weedbrook, C., Yu, S., Gu, W., Sun, M., Peng, X., Guo, H.: Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. J. Phys. B At. Mol. Opt. Phys. **47**(3), 035501 (2014)
10. Zhang, Y., Li, Z., Weedbrook, C., Marshall, K., Pirandola, S., Yu, S., Guo, H.: Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution. Entropy **17**(7), 4547 (2015)
11. Xuan, Q.D., Zhang, Z., Voss, P.L.: A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. Opt. Express **17**(26), 24244 (2009)
12. Hirano, T., Ichikawa, T., Matsubara, T., Ono, M., Oguri, Y., Namiki, R., Kasai, K., Matsumoto, R., Tsurumaru, T.: Implementation of continuous-variable quantum key distribution with discrete modulation. Quantum Sci. Technol. **2**(2), 024010 (2017)
13. Xu-Yang, W., Zeng-Liang, B., Shao-Feng, W., Yong-Min, L., Kun-Chi, P.: Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise. Chin. Phys. Lett. **30**(1), 010305 (2013)
14. Usenko, V.C., Grosshans, F.: Unidimensional continuous-variable quantum key distribution. Phys. Rev. A **92**(6), 062337 (2015)
15. Wang, X., Liu, W., Wang, P., Li, Y.: Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. Phys. Rev. A **95**(6), 062330 (2017)
16. Usenko, V.C., Filip, R.: Trusted noise in continuous-variable quantum key distribution: a threat and a defense. Entropy **18**(1), 20 (2016)
17. Borelli, L.F.M., Aguiar, L.S., Roversi, J.A., Vidiella-Barranco, A.: Quantum key distribution using continuous-variable non-Gaussian states. Quantum Inf. Process. **15**(2), 893 (2016)
18. Leverrier, A., Grangier, P.: Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Phys. Rev. A **83**, 042312 (2011)
19. Huang, P., He, G., Fang, J., Zeng, G.: Performance improvement of continuous-variable quantum key distribution via photon subtraction. Phys. Rev. A **87**, 012317 (2013)
20. Li, Z., Zhang, Y., Wang, X., Xu, B., Peng, X., Guo, H.: Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. Phys. Rev. A **93**, 012310 (2016)
21. Guo, Y., Liao, Q., Wang, Y., Huang, D., Huang, P., Zeng, G.: Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. Phys. Rev. A **95**(3), 032304 (2017)
22. Specht, H.P., Nölleke, C., Reiserer, A., Uphoff, M., Figueroa, E., Ritter, S., Rempe, G.: A single-atom quantum memory. Nature **473**(7346), 190 (2011)
23. Wang, Y., Um, M., Zhang, J., An, S., Lyu, M., Zhang, J.N., Duan, L.M., Yum, D., Kim, K.: Single-qubit quantum memory exceeding ten-minute coherence time. Nat. Photonics **11**(10), 646 (2017)
24. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., Grangier, P.: Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J. Phys. B At. Mol. Opt. Phys. **42**(11), 114014 (2009)
25. García-Patrón, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. **97**(19), 190503 (2006)
26. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**(2), 621 (2012)
27. General Photonics Corporation: Data Sheet of OEM Balanced Photodetector. Technical report. http://www.generalphotonics.com/wp-content/uploads/2015/04/BPD-003-4-27-15.pdf (2015). Accessed 23 Apr 2018
28. Ottaviani, C., Laurenza, R., Cope, T.P., Spedalieri, G., Braunstein, S.L., Pirandola, S.: Secret key capacity of the thermal-loss channel: improving the lower bound. In: Quantum Information Science and Technology II, vol. 9996, p. 999609. International Society for Optics and Photonics (2016)
29. Furrer, F., Munro, W.J.: Repeaters for Continuous Variable Quantum Communication. arXiv preprint arXiv:1611.02795 (2016)