Numerical simulation of the optimal two-mode attacks for two-way continuous-variable quantum cryptography in reverse reconciliation

Yichen Zhang\textsuperscript{1}, Zhengyu Li\textsuperscript{2}, Yijia Zhao\textsuperscript{1}, Song Yu\textsuperscript{1} and Hong Guo\textsuperscript{2}

\textsuperscript{1}State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, People’s Republic of China
\textsuperscript{2}State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Center for Quantum Information Technology, Peking University, Beijing 100871, People’s Republic of China

E-mail: yusong@bupt.edu.cn

Received 22 June 2016, revised 23 November 2016
Accepted for publication 29 November 2016
Published 13 January 2017

Abstract
We analyze the security of the two-way continuous-variable quantum key distribution protocol in reverse reconciliation against general two-mode attacks, which represent all accessible attacks at fixed channel parameters. Rather than against one specific attack model, the expression of secret key rates of the two-way protocol are derived against all accessible attack models. It is found that there is an optimal two-mode attack to minimize the performance of the protocol in terms of both secret key rates and maximal transmission distances. We identify the optimal two-mode attack, give the specific attack model of the optimal two-mode attack and show the performance of the two-way protocol against the optimal two-mode attack. Even under the optimal two-mode attack, the performances of two-way protocol are still better than the corresponding one-way protocol, which shows the advantage of making double use of the quantum channel and the potential of long-distance secure communication using a two-way protocol.

Keywords: quantum cryptography, quantum key distribution, continuous variable, optimal two-mode attack

(Some figures may appear in colour only in the online journal)

1. Introduction
Quantum key distribution (QKD) [1, 2] is one of the most practical applications of quantum information. Its goal is to establish a secure key between two legitimate partners, usually named Alice and Bob. Continuous-variable quantum key distribution (CV-QKD) [3–5] has attracted much attention in the past few years [5–9] mainly because it only uses standard telecommunications components. A CV-QKD protocol based on Gaussian-modulated coherent states [10, 11] has been proved to be secure against arbitrary general attacks [12–17] and experimentally demonstrated [6, 18–21].

To enhance the tolerable excess noise of CV-QKD, compared to typical one-way schemes, the two-way CV-QKD protocol was proposed [22]. Afterward, a more feasible two-way CV-QKD protocol was proposed by replacing Alice’s displacement operation with a beam splitter, which leads to a protocol that is easier to analyze when considering channel estimation [23]. In standard CV-QKD protocols the quantum communication is one way, i.e., quantum systems are sent from Alice to Bob. While in two-way protocols, this process is bidirectional, with the systems transformed by Alice and sent back to Bob. The use of two-way quantum communication can increase the secure key rate, transmission
distance, and the robustness to noise [22, 23]. As a result, bosonic channels which are too noisy for one-way protocols may become secure for two-way protocols [5].

However, when comparing the performance of a two-way CV-QKD protocol with a one-way protocol in numerical simulations, all of the works assumed the eavesdropper performs two independent attacks [22, 23, 27] or give a specific attack model [24–26]. It makes us wonder, does the outperformance of the two-way protocol against a specific attack mean that it is really more advantageous than the one-way protocol? Is it a fair comparison? Or is it just because the chosen attack model is powerless?

Recently, it has been very interesting to see that the security of the original two-way CV-QKD protocol against two-mode attacks has been studied assuming direct reconciliation [28], and the general immunity and superadditivity of the original protocol has also been studied [29]. Inspired by the method of [28], in this paper, we analyze the security of the modified two-way CV-QKD protocol in reverse reconciliation against general two-mode attacks, including two independent attacks, all separable attacks and all entangled attacks. Normally, reverse reconciliation is more useful than direct reconciliation in practice [5]. Against all accessible two-mode attacks, the expression of secret key rates of the two-way CV-QKD protocol using coherent states is derived in this paper.

The entanglement-based scheme of two-way CV-QKD protocol using Gaussian-modulated coherent states against two-mode attacks, where the quantum channel is fully controlled by Eve. However, Eve has no access to the apparatuses in Alice’s and Bob’s stations.

In this section, we present the basic notions of the entanglement-based scheme of the two-way CV-QKD protocol using coherent states. Then we describe the general two-mode attacks and identify different types of attacks.

**2. Entanglement-based model of two-way CV-QKD protocols against two-mode attacks**

In this section, we present the basic notions of the entanglement-based scheme of the two-way CV-QKD protocol using coherent states. Then we describe the general two-mode attacks and identify different types of attacks.

**2.1. Entanglement-based model of two-way CV-QKD protocols**

The entanglement-based scheme of the two-way CV-QKD protocol using coherent states is illustrated in Figure 1 and can be described as follows:

**Step 1:** Bob initially prepares an EPR pair (EPR1 with variance $V_B$, where the shot noise variance is normalized to 1), keeps the mode $B_1$ and sends the other mode $B_2$ to Alice through the channel where Eve may perform her attack.

**Step 2:** Alice prepares another EPR pair (EPR2 with variance $V_A$). She keeps the mode $A_1$ and measures it using heterodyne detection to get the variables $x_{A_1}$ and $p_{A_1}$. She then couples mode $A_2$ and the received mode $A_{in}$ from Bob with a beam splitter (transmittance: $T_A \in [0, 1]$). Alice then sends mode $A_{out}$ back to Bob where Eve may perform her attack. Alice measures another mode $A_3$ with homodyne detection for parameter estimation [23].

**Step 3:** Bob measures his original mode $B_1$ using heterodyne detection to get the variables $x_{B_1}$ and $p_{B_1}$. He also measures the received mode $B_3$ with heterodyne detection to get $x_{B_3}$ and $p_{B_3}$.

**Step 4:** Bob uses $x_{B_3} = x_{B_1} - kx_{B_1}$ and $p_{B_3} = p_{B_1} - kp_{B_1}$ to construct the estimator to Alice’s corresponding variable $x_{A_1}$ and $p_{A_1}$, where $k$ is the parameter used to optimize Bob’s estimator of Alice’s corresponding value. Then Alice and Bob proceed with classical data postprocessing including
reconciliation and privacy amplification. Here we use reverse reconciliation [18].

The most general eavesdropping strategy of two-way CV-QKD protocol is coherent attacks, which involve a unitary applied to all modes over all uses of the protocol. However, this could be reduced to collective attacks by assuming that Alice and Bob perform random permutations on their data [15]. When the eavesdropper performs collective attacks, she interacts independently and identically with each quantum signal over every use. In the entanglement-based representation of the two-way CV-QKD protocol, this means that the joint state \( \rho_{AB^{n}} \) has an identical and independently distributed (i.i.d.) structure \( \rho_{AB^{n}} = \rho_{AB}^n \), where \( n \) is the number of the uses of the protocol.

Furthermore, the most general collective attack against the two-way CV-QKD protocol is a joint attack involving two channels, the forward and backward channels. In each use of the protocol, Eve could intercept the two modes, one is the output of Bob’s side in the forward channel (mode \( B_2 \) in figure 1) and the other is the output of Alice’s side in the backward channel (mode \( A_{\text{out}} \) in figure 1), and make them intercept with an ensemble of ancillary vacuum modes via a general unitary \( U \). The remaining modes are stored in a quantum memory which will be measured at the end of the protocol.

The description of this attack can be further simplified. Since the protocol is based on the Gaussian modulation, its optimal eavesdropping attack is based on a Gaussian unitary \( U \). Thus, the security of the protocol can be reduced to studying a two-mode Gaussian attack against two channels, which is depicted in figure 1.

### 2.2. Two-mode attack strategy

In this two-mode Gaussian attack, the two output modes, \( B_2 \) and \( A_{\text{out}} \), are mixed with two ancillary modes, \( E_1 \) and \( E_2 \), by two beam splitters with transmissivities \( T_1 \) and \( T_2 \), respectively. These ancillary modes belong to a reservoir of ancillas \( (E_1, E_2, e) \) which is globally described by a pure Gaussian state. The reduced state \( \rho_{E_1E_2} \) of the injected ancillas is a correlated thermal state with zero mean and covariance matrix in the normal form

\[
\gamma_{E_1E_2} = \begin{pmatrix} V_{E_1} \cdot I_2 & C_{E_1E_2} \\ C_{E_1E_2} & V_{E_2} \cdot I_2 \end{pmatrix}
\]

where \( V_{E_1} \) and \( V_{E_2} \) are the variances of the thermal noise affecting each channel, \( C_{E_1E_2} = \text{diag}(C_1, C_2) \) is the correlation parameters between two ancillas. The various parameters \( V_{E_1}, V_{E_2}, C_1 \) and \( C_2 \) must satisfy the physical constraints [9, 30–32]:

\[
\gamma_{E_1E_2} > 0, \quad \nu \geq 1,
\]

where the positivity \( \gamma_{E_1E_2} > 0 \) is equivalent to the positivity of the principal minors of the matrix of equation (1),

\[
\nu = \sqrt{0.5(\Delta(\gamma_{E_1E_2}) - \sqrt{\Delta(\gamma_{E_1E_2})^2 - 4 \det \gamma_{E_1E_2}})},
\]

and \( \Delta(\gamma_{E_1E_2}) := V_{E_1}^2 + V_{E_2}^2 + 2C_1C_2 \).

In the two-way CV-QKD protocols, normally the excess noises of two channels are fixed, which means the variances, \( V_{E_1} \) and \( V_{E_2} \), are fixed for every transmissivity \( T_1 \) and \( T_2 \). Thus, the remaining degrees of freedom in the two-mode Gaussian attack are the correlation parameters \( C_1 \) and \( C_2 \), which can be represented as a point on a correlation plane. Each point of this plane describes an attack. Among all these accessible attacks, those satisfying the further condition

\[
\nu \geq 1,
\]

are separable attacks \( (\gamma_{E_1E_2} \text{ separable}) \), while those violating the condition of equation (3) are entangled attacks \( (\gamma_{E_1E_2} \text{ entangled}) \), where

\[
\nu = \sqrt{0.5(\Delta(\gamma_{E_1E_2}) - \sqrt{\Delta(\gamma_{E_1E_2})^2 - 4 \det \gamma_{E_1E_2}})},
\]

and \( \Delta(\gamma_{E_1E_2}) := V_{E_1}^2 + V_{E_2}^2 + 2C_1C_2 \). Figure 2 shows a numerical representation of the correlation plane under fixed variances: \( V_{E_1} = 3 \) and \( V_{E_2} = 3 \). Then we can identify the following attacks: separable attack, independent attack and entangled attack, which are described in [9, 32]. Here we just give the some basic knowledge which will be used in the following analysis. As illustrated in figure 2, point (1) represents an independent attack; points (2), (3), (4) and (5) represent separable attacks \( (C_{\text{sep}} = 2) \); points (6) and (7) represent entangled attacks \( (C_{\text{ent}} = \sqrt{2}) \).

![Correlation plane for different types of attacks under fixed variances](image)

**Figure 2.** Correlation plane for different types of attacks under fixed variances \( V_{E_1} = V_{E_2} = 3 \), where the inner are corresponds to separable attacks, while the two peripheral areas correspond to entangled attacks. The number points represent the specific attacks: point (1) represents an independent attack; points (2), (3), (4) and (5) represent separable attacks \( (C_{\text{sep}} = 2) \); points (6) and (7) represent entangled attacks \( (C_{\text{ent}} = \sqrt{2}) \).

2.3. Security analysis of the two-way CV-QKD protocol against two-mode attacks

In this subsection, we will derive the secure bound of the two-way protocol using coherent states against two-mode Gaussian attacks.
From the information-theoretic perspective, the asymptotic secret key rate $K$ against two-mode Gaussian attacks in reverse reconciliation is given by [33]

$$K = \beta I(A : B) - \chi(B : E),$$

where $\beta$ is the reconciliation efficiency, $I(A : B)$ is the classical mutual information between Alice and Bob, $\chi(B : E)$ is the Holevo bound between Eve and Bob [34]

$$\chi(B : E) = S(\rho_E) - \sum_{m_B} p(m_B) S(\rho_E^{m_B}),$$

where $S(\rho)$ is the von Neumann entropy of the quantum state $\rho$, $m_B$ is Bob’s measurement result, and it can take the form $m_B = x_B$ for homodyne detection or the form $m_B = x_B, p_B$ for heterodyne detection. $p(m_B)$ is the probability density of the measurement result, $\rho_E^{m_B}$ is the corresponding state of Eve’s ancillary conditioned on Bob’s measurement result.

The overall state can be described by the covariance matrix, which is defined by

$$\gamma_{ij} = \text{Tr}[\hat{\rho} \{ (\hat{r}_i - d_i)(\hat{r}_j - d_j) \}] ,$$

where $\hat{r}_{2i-1} = \hat{x}_i, \hat{r}_{2i} = \hat{p}_i, d_i = \langle \hat{r}_i \rangle = \text{Tr}[\hat{\rho}\hat{r}_i]$, $\hat{\rho}$ is the density matrix, and denotes the anticommutator. Before channel transmission, the covariance matrix $\gamma_{B,A_1A_2B_1}$ is

$$\begin{bmatrix}
V_B & 0 & 0 & 0 \\
0 & V_A & 0 & 0 \\
0 & 0 & V_A & 0 \\
0 & 0 & 0 & V_B
\end{bmatrix}$$

where $V_B$ is the variance of EPR1 and $V_A$ is the variance of EPR2. The channel transmission relations are as follows

$$\begin{cases}
\hat{r}_{2n} = \sqrt{T_f} r_{2n} + \sqrt{1 - T_f} r_{2n+1} \\
\hat{r}_{2n+1} = -\sqrt{1 - \eta} r_{2n+1} + \sqrt{\eta} r_{2n+2} \\
\hat{r}_{2n+2} = \sqrt{T_f} r_{2n+2} + \sqrt{1 - T_f} r_{2n+3}
\end{cases}$$

After two-mode Gaussian attacks, the covariance matrix $\gamma_{B,A_1A_2B_1}$ is changed into $\gamma_{B,A_1A_2B_1}'$ which is given by

$$\begin{bmatrix}
V_B & 0 & -T'C_B\sigma_2 & \sqrt{\eta} T'C_B\sigma_2 \\
0 & V_A & 0 & 0 \\
-T'C_B\sigma_2 & 0 & V_A & C_{A_2B_1} \\
\sqrt{\eta} T'C_B\sigma_2 & -T'C_B\sigma_2 & C_{A_2B_1} & V_B
\end{bmatrix}$$

where the forward and backward channels are assumed to have identical transmissivity $T_f = T_s = T$ and same excess noise $V_B = V_{B_1} = V_{E}$. The parameters $T' = \sqrt{T(1 - \eta)}$, $C_A = \sqrt{(V_A^2 - 1)}$, $C_B = \sqrt{(V_B^2 - 1)}$. The matrices $V_{A_i} = [\eta V_A + (1 - \eta)(TV_{E_0} + (1 - T)V_{E})] I$, $V_{B_i} = \text{diag}(V_{B_i}^a, V_{B_i}^p)$ and $C_{A_iB_i} = \text{diag}(C_{A_iB_i}^a, C_{A_iB_i}^p)$, which is given by

$$\begin{bmatrix}
V_{B_1} & V' + 2C_p(1 - T)\sqrt{T_f} \\
V' + 2C_p(1 - T)\sqrt{T_f} & V_{B_1} \\
C_{A_2B_1} & C' - C(1 - T)\sqrt{1 - \eta} \\
C_{A_2B_1} & C' - C(1 - T)\sqrt{1 - \eta}
\end{bmatrix}$$

where

$$V' = T(1 - \eta)V_A + T_f\eta V_B + [1 - T(1 - \eta)(1 - T)] V_E$$

and

$$C' = \sqrt{T_f(1 - \eta)} V_A - T_f\sqrt{T}(1 - \eta) V_B - (1 - T)\sqrt{T_f}(1 - \eta) V_E.$$
Figure 3. (a) Secret key rates of the two-way CV-QKD protocol using coherent states against all accessible attacks under 10 km, where different colors correspond to different values of the rate. The secret key rate is symmetric with respect to the bisector $C_x = C_p$. (b) Specific case of the left figure where $C_x = C_p$. (c) Specific case of the left figure where $C_x = -C_p$. Here we use the reconciliation efficiency $\beta = 0.95$ [6], modulation variance $V_{A} = V_{B} = 20$, $\varepsilon = 0.2$ and $\eta = 0.75$. Point (1) represents an independent attack; points (2), (3), (4) and (5) represent separable attacks; points (6) and (7) represent entangled attacks. The various attacks (1)–(7) are classified in section 2 and displayed in figure 2.

3. Optimal two-mode attack strategy

In this section, to find the optimal two-mode attack strategy against two-way CV-QKD protocols, the performances of two-way CV-QKD protocols are compared under different types of two-mode attack strategies.

We first analyze the secret key rates of the protocol against all accessible attacks at fixed transmission distance $d = 10$ km, 20 km, 30 km, where we only put the result at $d = 10$ km here and put the results at $d = 20$ km, 30 km in the appendix. The parameters affecting the value of the secret key rate are the reconciliation efficiency $\beta$, the variance of Alice’s and Bob’s modulation: $(V_{A} - 1)$ and $(V_{B} - 1)$, the transmittance of the beam splitter at Alice’s side $\eta$ and the transmission efficiency $T$. The parameters $V_{A}$, $V_{B}$, $\beta$, $\eta$ and $\varepsilon_{cl}$ are fixed in all simulations. Here, we choose the variance $V_{A} = V_{B} = 20$, $\beta = 1$, $\eta = 0.75$ as the value of the beam splitter transmittance at Alice’s side and channel noise $\varepsilon = 0.2$. As illustrated in figure 3(a), different colors correspond to different values of the secret key rate, where red corresponds to higher value of the rate, while blue corresponds to lower value of the rate. It is found that the secret key rate is symmetric with respect to the bisector $C_x = C_p$, which is coincident with the security analysis in section 2.3. Furthermore, in order to be more clear, we plot the specific cases where $C_x = -C_p$ and $C_x = C_p$ in figures 3(b) and (c), respectively. The minimum key rate associated with the optimal attack correspond to the two-mode symmetric separable attack with $C_x = C_p = C_{opt} = 0.0078$ when we
This covariance matrix represents a specific two-mode attack model, which is illustrated in figure 5. Eve initially prepares two EPR pairs (EPR1 with variance \(V_0 = V_E + C_{opt}\) and EPR2 with variance \(V_2 = V_E - C_{opt}\)), keeps one mode of each EPR pairs and then she couples the other mode of the two EPR pairs with a 50 : 50 beam splitter. The output modes of the beam splitter, mode \(E_1\) and \(E_2\), are two ancillary injected modes of two-mode attack. Finally, Eve mixes modes \(E_1\) and \(E_2\) with the modes in the forward and backward channels, by two beam splitters with transmissivity \(T\), respectively. The remaining modes are stored in the quantum memory which will be measured at the end of the protocol. We note that, no matter what specific model of Eve is, the optimal two-mode attack has the feature that \(V_E = V_E, C_x = C_{p}\), which is symmetric for \(x\)-quadrature and \(p\)-quadrature.

### 4. Outperformance of two-way CV-QKD protocols

In the following, we compare the two-way CV-QKD protocol with their one-way counterpart to examine whether the two-way protocol remains advantageous when the optimal two-mode attack strategy is used against the two-way protocol. To reveal the advantage of the two-way CV-QKD protocol more explicitly, the relationship between the tolerable excess noise and the transmission distance are shown in figure 6. When using ideal reconciliation efficiency \(\beta = 1\), the upper limit of the tolerable excess noise of the two-way CV-QKD protocol is almost the double that of the upper limit of the one-way protocol at a short transmission distance. As the transmission distance increases, this advantage would be reduced. But the tolerable excess noise of the two-way protocol is still higher than that of the one-way protocol. As the reconciliation efficiency decreases from an ideal value to a more practical one [8], the advantage of two-way protocols still holds and becomes more obvious. The results in figure 6(b) show that the two-way CV-QKD could tolerate more channel excess noise than the one-way protocol.

Thus, from the above discussion, it is found that even under optimal two-mode attacks, which cause a lower secret key rate and shorter transmission distance, the performances of the two-way protocol are still better than the one-way protocol. The two-way protocol is able to distribute secret keys in communication lines which are too noisy for the one-way protocol.

### 5. Conclusion

In this paper, we analyze the security of the two-way CV-QKD protocol against general two-mode attacks, including two independent attacks, all separable attacks and all entangled attacks. Against all accessible two-mode attacks, the expression of secret key rates of the two-way CV-QKD protocol is derived under the reverse reconciliation. Then we evaluate and compare the performance of the two-way protocol against different attacks and it is found that there is an
optimal two-mode attack to minimize the performance of the protocol in terms of both key rates and maximal transmission distances. We identify the optimal two-mode attack, give the specific attack model of the optimal two-mode attack and show the performance of the two-way protocol against the optimal two-mode attack.

The performances of the two-way CV-QKD protocols against the optimal attack are compared with the performance of the one-way version of the scheme and show that the two-way CV-QKD protocols still achieve a higher secret key rate and tolerate more excess noise than the one-way protocol, which shows the advantage of making double use of the quantum channel and addressing the question—is the two-way protocol really more advantageous than the one-way protocol?

Acknowledgments

This work was supported in part by the National Basic Research Program of China (973 Program) under Grant 2014CB340102, in part by the National Natural Science Foundation under Grants 61225003, 61531003, 61427813, 61401036, 61471051, in part by BUPT Excellent PhD
Appendix. Optimal two-mode attack strategy at different distances

In this appendix, we show the secret key rates of the two-way CV-QKD protocol against all accessible attacks at fixed transmission distance $d = 20\, \text{km}, 30\, \text{km}$. The parameters we use here keep the same with section 3. As illustrated in figures A1(a) and A2(a), different colors correspond to different values of the secret key rate, where red regions correspond to higher values of the rate, while blue regions correspond to lower values of the rate. Furthermore, we also plot the specific cases where $C_x = -C_y$ and $C_x = C_y$ in figures A1(b), (c), and A2(b), (c), respectively. The minimal key rate associated with the optimal attack correspond to the two-mode symmetric separable attack $C_x = C_y = C_{\text{opt}}^{30\, \text{km}} = 0.0073$ at $d = 20\, \text{km}$ and correspond to the two-mode symmetric separable attack $C_x = C_y = C_{\text{opt}}^{30\, \text{km}} = 0.0039$ at $d = 30\, \text{km}$.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[3] Braunstein S L and van Loock P 2005 Rev. Mod. Phys. 77 513
[4] Wang X B, Hiroshima T, Tomita A and Hayashi M 2007 Phys. Rep. 448 1
[5] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Rev. Mod. Phys. 84 621
[6] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Nat. Photon. 7 378
[7] Li Z, Zhang Y C, Xu F, Peng X and Guo H 2014 Phys. Rev. A 89 052301
[8] Zhang Y C, Li Z, Yu S, Gu W, Peng X and Guo H 2014 Phys. Rev. A 90 052325
[9] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 Nat. Photon. 9 397
[10] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
[11] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Phys. Rev. Lett. 93 170504
[12] Navascués M, Grosshans F and Acín A 2006 Phys. Rev. Lett. 97 190502
[13] García-Patrón R and Cerf N J 2006 Phys. Rev. Lett. 97 190503
[14] Pirandola S, Braunstein S L and Lloyd S 2009 Phys. Rev. Lett. 101 200504
[15] Renner R and Cirac J I 2009 Phys. Rev. Lett. 102 110504
[16] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 Phys. Rev. Lett. 110 030502
[17] Leverrier A 2015 Phys. Rev. Lett. 114 070501
[18] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 Nature 421 238
[19] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 Phys. Rev. Lett. 95 180503
[20] Lodewyck J et al 2007 Phys. Rev. A 76 042305
[21] Khan I, Wittmann C, Jain N, Killoran N, Lütkenhaus N, Marquardt C and Leuchs G 2013 Phys. Rev. A 88 010302
[22] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Nat. Phys. 4 726
[23] Sun M, Peng X, Shen Y and Guo H 2012 Int. J. Quantum Inform. 10 1250059
[24] Wang T, Yu S, Zhang Y C, Gu W and Guo H 2014 J. Phys. B: At. Mol. Phys. 47 215504
[25] Zhang Y C, Li Z, Weedbrook C, Yu S, Gu W, Sun M, Peng X and Guo H 2014 J. Phys. B: At. Mol. Phys. 47 035501
[26] Sun M, Peng X and Guo H 2013 J. Phys. B: At. Mol. Phys. 46 085501
[27] Weedbrook C, Ottaviani C and Pirandola S 2014 Phys. Rev. A 89 012309
[28] Ottaviani C, Mancini S and Pirandola S 2015 Phys. Rev. A 92 062323
[29] Ottaviani C and Pirandola S 2016 Sci. Rep. 6 22225
[30] Pirandola S, Serafini A and Lloyd S 2009 Phys. Rev. A 79 052327
[31] Spedalieri G, Ottaviani C and Pirandola S 2013 Open Syst. Inf. Dyn. 20 135001
[32] Ottaviani C, Spedalieri G, Braunstein S L and Pirandola S 2015 Phys. Rev. A 91 022320
[33] Devetak I and Winter A 2005 Proc. R. Soc. London Ser. A 461 207
[34] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Communication (Cambridge: Cambridge University Press)