An improved two-way continuous-variable quantum key distribution protocol with added noise in homodyne detection

Maozhu Sun, Xiang Peng and Hong Guo

The State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, People’s Republic of China
E-mail: xiangpeng@pku.edu.cn and hongguo@pku.edu.cn

Received 31 August 2012, in final form 29 January 2013
Published 27 March 2013
Online at stacks.iop.org/JPhysB/46/085501

Abstract
We propose an improved two-way continuous-variable quantum key distribution (CV QKD) protocol by adding proper random noise on the receiver’s homodyne detection, the security of which is analysed against general collective attacks. The simulation result under the collective entangling cloner attack indicates that despite the correlation between two-way channels decreasing the secret key rate relative to the uncorrelated channels slightly, the performance of the two-way protocol is still far beyond that of the one-way protocols. Importantly, the added noise in detection is beneficial for the secret key rate and the tolerable excess noise of this two-way protocol. With the reasonable reconciliation efficiency of 90%, the two-way CV QKD with added noise allows the distribution of secret keys over 60 km fibre distance.

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

1. Introduction
Quantum key distribution (QKD) can enable two authentic parties, the sender (Alice) and the receiver (Bob), to obtain unconditional secret keys without restricting the power of the eavesdropper (Eve) [1, 2]. On the premise of unconditional security, the higher key rate and the longer distance are constantly pursued [3, 4]. To enhance the tolerable excess noise of the continuous-variable QKD (CV QKD) [5, 6], the two-way CV QKD protocols are proposed [7, 8], where Bob initially sends a mode to Alice and Alice encodes her information by applying a random displacement operator to the received mode and then sends it back to Bob. Bob detects both his original mode and received mode to decode Alice’s modulations. Although the two-way CV QKD protocols can remarkably enhance the tolerable excess noise [7, 8], it needs to implement the tomography of the quantum channels to analyse the security under general collective attack [7], which is complicated in practice. Therefore, we proposed a feasible modified two-way protocol by replacing the displacement operation of the original two-way protocol with a passive operation on Alice’s side [9]. However, the source noise [10–14] and both detection efficiency and detection noise [15, 16] on Bob’s side are not considered in the modified protocol.

It has been proved that adding a proper noise on Bob’s detection side in one-way CV QKD can enhance the tolerable excess noise and the secret key rate in reverse reconciliation [12, 17–21]. This idea has been applied to the original two-way protocol in [22], while the scheme did not consider the correlation between the two channels. The correlated noise affects the secret key rate [23, 24]. In this paper, we apply the idea of adding noise to our modified two-way protocol Hom2 [9] to enhance the tolerable excess noise and the secret key rate. Considering the correlation between the channels, the security of the two-way CV QKD with added noise against entangling cloner collective attacks [25, 26] is analysed and numerically simulated.
2. The two-way CV QKD with added noise in homodyne detection

The entanglement-based (EB) scheme of the two-way CV QKD protocol Hom2\textsubscript{N} with the added detection noise is shown in figure 1(a), where the dashed box at B\textsubscript{2} is the added noise and homodyne detection preceded by an EPR pair coupled by a beam splitter at B\textsubscript{2} is equivalent to Bob’s real homodyne detection with efficiency T\textsubscript{N} and electronic noise [17]. Note that x and p quadratures are randomly measured in homodyne detection and only x quadrature is analysed in the following.

3. The analysis of the security against general collective attack

First, we show that the Gaussian attack is optimal to the two-way protocol Hom2\textsubscript{N} in general collective attack. In figure 1(a), since all modes of Alice and Bob are measured, Eve can obtain the purification of the state of Alice and Bob. In addition, the x and p quadratures of Alice’s and Bob’s modes are not mixed via the heterodyne or homodyne detection and Alice and Bob use the second-order moments of the quadratures to bound Eve’s information. Therefore, the two-way protocol Hom2\textsubscript{N} can satisfy the requirement of the optimality of Gaussian collective attack (i.e. continuity, invariance under local Gaussian unitary and strong subadditivity) [29]. When the corresponding covariance matrix of the state B\textsubscript{2}B\textsubscript{1}N\textsubscript{2}N\textsubscript{1}A\textsubscript{2}A\textsubscript{1} is known for estimate the channel’s parameters and Bob uses x\textsubscript{B} = x\textsubscript{B\textsubscript{1}} - kx\textsubscript{B\textsubscript{1}} (p\textsubscript{B} = p\textsubscript{B\textsubscript{1}} + kp\textsubscript{B\textsubscript{1}}) to construct the optimal estimation to Alice’s corresponding variables x\textsubscript{A\textsubscript{1}} (p\textsubscript{A\textsubscript{1}}), where k is the channel’s total transmittance.
Alice and Bob, the Gaussian attack is optimal [30–33]. Therefore, only Eve’s Gaussian collective attack is needed to be considered in the following security analysis.

In figure 1(a), the secret key rate of the two-way protocol Hom_{\text{VAM}} in reverse reconciliation is [16, 34–36]

$$K_R = \beta I(B : A) - I(B : E)$$

$$= \frac{1}{2} \log_2 \frac{V_{AB}}{V_{AB|x_B}} - S(E) + S(E|x_B),$$

(1)

where $\beta$ is the reconciliation efficiency, $I(B : A) [I(B : E)]$ is the mutual information between Bob and Alice (Eve), $V_{AB}$ and $V_{AB|x_B}$ are Alice’s variance and conditional variance, $S(E)$ and $S(E|x_B)$ are Eve’s von Neumann entropy and conditional von Neumann entropy on Bob’s data, respectively. In the following, $S(E)$ and $S(E|x_B)$ are calculated by the methods in [37].

For the Gaussian state, the entropy can be calculated from its corresponding covariance matrix [38]. Since the state $\rho_{B_2B_1N_2N_1A_2A_1}$ is a pure state, $S(E) = S(B_2B_1N_2N_1A_2A_1)$. The corresponding covariance matrix of the state $\rho_{B_2B_1N_2N_1A_2A_1}$ is

$$\Gamma_{B_2B_1N_2N_1A_2A_1} = \left( \begin{array}{cccccc}
\gamma_{B_1} & C_1 & C_2 & C_3 & C_4 & C_5 \\
C_1 & V_1 & 0 & 0 & 0 & 0 \\
C_2 & 0 & V_2 & 0 & 0 & 0 \\
C_3 & 0 & 0 & V_3 & 0 & 0 \\
C_4 & 0 & 0 & 0 & V_4 & 0 \\
C_5 & 0 & 0 & 0 & 0 & V_5
\end{array} \right),$$

(2)

where $I$ is a $2 \times 2$ identity matrix, the diagonal elements correspond to the variances of $x$ and $p$ quadratures of the modes $B_2, B_1, N_2, N_1, A_2$ and $A_1$ in turn, e.g. $\gamma_{B_2} = \text{diag}((\bar{x}_B^2), (\bar{p}_B^2))$, and the nondiagonal elements correspond to the covariances between modes, e.g. $C_1 = \text{diag}((x_{B_2}x_{B_1}), (p_{B_2}p_{B_1}))$. Therefore, Eve’s entropy [39]

$$S(E) = \sum_{i=1}^{6} G(\lambda_i) = \sum_{i=1}^{6} G(f_{\lambda_i}(\alpha_{mn})),$$

(3)

where $G(\lambda_i) = \frac{\lambda_i+1}{2} \log \frac{\lambda_i+1}{2} - \frac{\lambda_i-1}{2} \log \frac{\lambda_i-1}{2}$, and $\lambda_i = f_{\lambda_i}(\alpha_{mn})$ is the symplectic eigenvalue of $\Gamma_{B_2B_1N_2N_1A_2A_1}$, which is the function of the element $\alpha_{mn}$ of $\Gamma_{B_2B_1N_2N_1A_2A_1}$ [40, 41], see the appendix.

Bob uses $x_B = x_B - k x_B$ to estimate Alice’s variable, which is equivalent to a symplectic transformation $\Gamma_k$ that Bob uses to change modes $B_2$ and $B_1$ into modes $B_4$ and $B_3$, respectively, where the $x$ quadrature of mode $B_4$ is $x_{B_4} = x_B - k x_B$ [9], as shown in figure 1(b). Since figure 1(b) is equivalent to figure 1(a) with postprocessing, we use figure 1(b) to calculate $S(E|x_B)$ in the following.

After the symplectic transformation $\Gamma_k$, the corresponding covariance matrix of the mode $\rho_{B_4B_3N_2N_1A_2A_1}$ is

$$\Gamma_{B_4B_3N_2N_1A_2A_1} = [I_k \otimes L_k] \Gamma_{B_2B_1N_2N_1A_2A_1} [I_k \otimes L_k]^T,$$

(4)

where $L_k = \otimes^k_1 I$, $I_k$ is a $2 \times 2$ identity matrix, $k$ is a continuous-variable C-NOT gate [29, 42, 43]:

$$\Gamma_k = \begin{pmatrix}
1 & 0 & -k & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & k & 0 & 1
\end{pmatrix}. $$

(5)

Since the state $\rho_{B_4N_1A_2A_1N_2}E$ is a pure state when Bob obtains $x_B$ by measuring the modes $B_4$, $S(E|x_B) = S(B_4N_1A_2A_1|x_B)$. The corresponding covariance matrix of the state $\rho_{B_4N_1A_2A_1}$ conditioned on $x_B$ is $[29, 44]$

$$\Gamma_{B_4N_1A_2A_1} = \gamma_{B_4N_1A_2A_1} - C_{B_4}[X_{B_4}X_{B_4}]^{\text{MP}}C_{B_4},$$

(6)

where $\gamma_{B_4N_1A_2A_1}$ and $\gamma_{B_4}$ are the corresponding reduced matrices of the states $\rho_{B_4N_1A_2A_1}$ and $B_4$. In $\Gamma_{B_4N_1A_2A_1}$, respectively, $C_{B_4}$ is their correlation matrix, $X_{B_4} = \text{diag}(1, 0)$. The secret key rate of the two-way protocol is obtained:

$$K_R = \frac{1}{2} \log_2 \frac{V_{AB}}{V_{AB|x_B}} - \sum_{i=1}^{5} G(f_{\lambda_i}(\alpha_{mn})) + \sum_{i=1}^{5} G(f_{\lambda_i}(\alpha_{mn}')),$$

(8)

In experiment, Alice and Bob can calculate the element $\alpha_{mn}$ and $\alpha_{mn}'$ of equations (2) and (6) by the measurement values of the modes $B_2, B_1, N_2, N_1, A_2$ and $A_1$. Therefore, according to equation (8), the secret key rate in general collective attack is obtained without the assumption that the two channels are uncorrelated. The analytic representations of equation (8) are too complex to give here. We give a numerical simulation in the following.

### 4. Numerical simulation and discussion of collective entangling cloner attacks on correlated and uncorrelated channels

For simplicity in numerical simulation, when there is no Eve, the forward and backward channels are assumed to be independent with the identical transmittances $T$ and noises referred to the input $\chi = \varepsilon + (1 - T)/T$, where $\varepsilon$ is the channel excess noises referred to the input. It is equivalent to Eve implementing two independent collective entangling cloner attacks which are a Gaussian collective attack investigated in detail in [45, 46]. When Eve implements a more complicated two-mode attack [7], the correlation between the two channels is induced. Figure 2 shows that Eve implements two correlated entangling cloner attacks. Under the condition that Eve introduces the equivalent variances of modes $E_2$ and $E_2'$ into the two channels, the noise referred to the input of the backward channel is $\chi_2 = \chi + 2n_e \sqrt{T_2}T$, where the second item on the right-hand side is induced additionally by the correlation between the two channels, i.e. the part of the mode introduced into the backward channel correlating with the forward channel interferes with the mode from Alice; $n_e = \sqrt{1 - T_2}$ is the coefficient representing the degree of the correlation, e.g., $n_e = 0$ represents that the two channels are uncorrelated.
Figure 2. The EB scheme of the Hom₂ protocol against entangling cloner attacks on correlated channels. $E_1$, $E_2$: the modes introduced into the channels; $T_{1/2}$: half-beam splitter; $T_c$: beam splitter. Alice and Bob are the same as in figure 1(a).

Figure 3. (a) Tolerable excess noise as a function of the transmission distance for the Hom₂, Hom, Het protocols, where $\beta = 90\%$. (b) Tolerable excess noise as a function of the transmission distance for the Hom₂ protocol, where $\beta = 100\%, 90\%, 80\%, 70\%$. The curves of (a) and (b) are plotted for $n_c = 0$, $T_A = 0.8$ and $V_A = V = 20$.

Figure 4. (a) Secret key rate as a function of the transmission distance for the Hom₂, Hom, Het protocols, where $n_c = 0$, $\varepsilon = 0.06$, $\beta = 90\%$, $T_A = 0.8$ and $V_A = V = 20$. (b) Optimal choice of the added noise $x_D$.

The added noise is $x_D = (1 - T_N)V_N/T_N$. We can calculate the elements of equation (2),

\[
\begin{align*}
\gamma_h &= [V_N - T_NV_N + TT_N[V_A - T_AV_A + TT_A(V + \chi) + \chi_2]\mathbb{I}], \\
\gamma_N &= [T_NV_N + T(1 - T_N)[V_A - T_AV_A + TT_A(V + \chi) + \chi_2]\mathbb{I}], \\
\gamma_A &= [T_AV_A + T(1 - T_A)(V + \chi)\mathbb{I}], \\
C_1 &= -\eta C_6 = T\sqrt{T_NV_N - T\sqrt{T_N(V + \chi)} - n_c\sqrt{T\varepsilon}}\mathbb{I}, \\
C_2 &= (1 - T_N)\sqrt{T_NV_N - T[V_A - T_AV_A + TT_A(V + \chi) + \chi_2]\mathbb{I}},
\end{align*}
\]

\[
\begin{align*}
C_3 &= -\eta C_8 = \sqrt{(1 - T_N)(V_N^2 - 1)}\sigma_z, \\
C_4 &= -\eta C_9 = \sqrt{T(1 - T_A)T_NV_N} \\
&\times [\sqrt{T_NV_N} - T\sqrt{T_N(V + \chi)} - n_c\sqrt{T\varepsilon}]\mathbb{I}, \\
C_5 &= -\eta C_{10} = \sqrt{T(1 - T_N)TV_A(V_A^2 - 1)}\sigma_z, \\
C_7 &= -\sqrt{T(1 - T_N)(V_A^2 - 1)}\sigma_z, \\
C_{11} &= \sqrt{T_A(V_A^2 - 1)}\sigma_z,
\end{align*}
\]
Figure 5. (a) Secret key rate as a function of the transmission distance for the Hom2 N protocol, where $\varepsilon = 0.06$, $\beta = 90\%$, $T_A = 0.8$, $V_A = 20$ and $n_c = 0, 0.5, 1$. (b) Optimal choice of the added noise $\chi_D$.

Figure 6. (a) Tolerable excess noise as a function of the transmission distance for high modulation for the Hom2 N protocol. (b) Secret key rate as a function of the transmission distance for high modulation for the Hom2 N protocol, where $\varepsilon = 0.2$. The curves of (a) and (b) are plotted for $V_A = V = 1000$, $n_c = 0$, $T_A = 0.8$ and $\beta = 1$.

and

\[ I(B : A) = \frac{1}{2} \log_2 \left( \frac{T^2 T_A F + T (V_A - T_A V_A + \chi_2) + \chi_D}{T (1 - T_A + \chi_2) + T^2 T_A F + \chi_D} \right). \tag{10} \]

where $\sigma_\varepsilon = \text{diag}(1, -1)$, $\eta = \sqrt{\eta/\eta}$, $F = 2V - 2\sqrt{V^2 - 1} + \chi$. The typical fibre channel loss is assumed to be 0.2 dB km$^{-1}$. $V$ and $\varepsilon$ are in shot-noise units. Substituting equations (9) and (10) into equation (8), the optimal secret key rate $K_R$ and the optimal tolerable excess noise $\varepsilon$ of the two-way protocol Hom2 N can be obtained by adjusting the added noise $\chi_D$.

When $n_c = 0$, the two channels are uncorrelated, which is equivalent to Eve implementing two independent Gaussian cloner attacks. For comparison, the heterodyne protocol (Het) [47] and the homodyne protocol (Hom) [36] of the one-way CV QKD protocol with the coherent state and the original modified two-ways protocols Hom2 M and Hom-HetM [9] are also given in figures 3(a) and 4(a). Figure 3(a) shows the tolerable excess noise as a function of the transmission distance, where $V_A = V = 20$, $T_A = 0.8$, $\varepsilon = 0.06$, $\beta = 90\%$ and $n_c = 0$. To make the secret key rate of Hom2 N optimal, the proper added noise $\chi_D$ is chosen, as shown in figure 4(b). In figure 4(a), the simulation result indicates that the two-way protocol with the added noise has a higher secret key rate than that without added noise. In particular, the achievable transmission distance of the two-way protocol Hom2 N is over 60 km when $\beta = 90\%$, which is much longer than that of the one-way protocol. The reason is that the added noise not only lowers the mutual information between Alice and Bob, but also lowers that between Bob and Eve. When the effect on Eve is more than that on Alice and Bob, the secret key rate is enhanced.
When $n_c \neq 0$, the two channels are correlated. Figure 5(a) shows the secret key rate as a function of the transmission distance for the Hom$_2$ protocol with different $n_c$. Considering the practical experiment [15, 16, 48], we choose $\varepsilon = 0.06$, $\beta = 90\%$, $T_A = 0.8$, $V_A = V = 20$ and $n_c = 0, 0.5, 1$. To make $K_R$ optimal, the proper added noise $\chi_D$ is chosen, as shown in figure 5(b). In figure 5(a), the simulation result indicates that the distance of the secret key distribution decreases with the increase of $n_c$. The reason is that the correlation between the two channels induces the change of the excess noise in the backward channel, which affects the secret key rate. Figure 5(a) shows that the decrease of the secret key rate induced by this effect is small. In addition, comparing with the one-way protocol in figure 4(a), despite the transmission distance of the two-way protocol decreases slightly due to the correlation, the performance of the two-way protocol is still far beyond that of the one-way protocols. Figure 5(b) shows that the optimal added noise decreases with the decrease of $n_c$.

In the following, we compare the two-way protocol with the one-way protocols in high modulation. Figures 6(a) and (b) show the tolerable excess noise and the secret key rate as a function of the transmission distance for high modulation, where $V_A = V = 1000$, $T_A = 0.8$, $\beta = 1$ and $n_c = 0$. The proper added noise $\chi_D$ is chosen to make the tolerable excess noise and the secret key rate of the Hom$_2$ protocol optimal. The numerical simulation result indicates that both the tolerable excess noise and the secret key rate of the two-way protocol with added noise are much more than that of the one-way CV QKD protocols for high modulation.

5. Conclusion

In conclusion, we improve the two-way CV QKD protocol by adding a proper noise on Bob’s detection side. The security of the two-way CV QKD protocol with the added noise in homodyne detection against general collective attack is analysed. The numerical simulation under the collective entangling cloner attack is given for the correlated and the uncorrelated channels. The simulation result indicates that despite the secret key rate for the correlated channels is slightly lower than that for the uncorrelated channels when Eve inputs the equivalent variance of the modes into the two channels, the performance of the two-way protocol is still far beyond that of the one-way protocols. In addition, the properly added noise is beneficial for enhancing the secret key rate and the tolerable excess noise of the two-way CV QKD. The optimal tolerable excess noise of the two-way CV QKD with added noise is much more than that of the one-way CV QKD. With the reasonable reconciliation efficiency of 90\%, the two-way CV QKD with the added noise allows the distribution of secret keys over 60 km fibre distance, which is difficult to reach for the one-way CV QKD protocols with Gaussian modulation in experiment.

Acknowledgments

This work is supported by the National Science Fund for Distinguished Young Scholars of China (grant no. 61225003), National Natural Science Foundation of China (grant no. 61101081), and the National Hi-Tech Research and Development (863) Program.

Appendix. The calculation of eigenvalues

We use $\alpha''_{mn}$ to denote the elements of the corresponding covariance matrix $\Gamma_n$ of an $n$-mode state. The symplectic invariants $\{\Delta_{n,j}\}$ of $\Gamma_n$ for $j = 1, \ldots, n$ are defined as [40]

$$\Delta_{n,j} = M_{2j}(\Omega\Gamma_n), \quad \Omega = \bigoplus_{j=1}^{n}\sigma_j$$

where $\sqrt{\Omega}\Gamma_n^\dagger\sqrt{\Omega}$ is the principal minor of order $2j$ of the $2n \times 2n$ matrix $\Omega\Gamma_n$ which is the sum of the determinants of all the $2j \times 2j$ submatrices of $\Omega\Gamma_n$ [40, 41].

The symplectic eigenvalues of the matrix corresponding to a four-mode state are the solution of the four-order equation on the symplectic invariants [9, 29, 40]

$$f^{(1,1)}_n(\alpha''_{mn}) = \frac{\Delta_{4,1}}{4} - \frac{1}{2}\sqrt{\xi + \Theta}, \quad \pm \frac{1}{2}\sqrt{2\xi - \Theta - \frac{\Delta^2_{4,1}}{4}\Delta_{4,2} + 8\Delta_{4,3}} \quad \frac{4\sqrt{\xi + \Theta}}{3},$$

$$f^{(1,1)}_n(\alpha''_{mn}) = \frac{\Delta_{4,1}}{4} + \frac{1}{2}\sqrt{\xi + \Theta}, \quad \pm \frac{1}{2}\sqrt{2\xi - \Theta + \frac{\Delta^2_{4,1}}{4}\Delta_{4,2} + 8\Delta_{4,3}} \quad \frac{4\sqrt{\xi + \Theta}}{3}.$$ 

where

$$\xi = \frac{\Delta^2_{4,1}}{4} - \frac{2\Delta_{4,2}}{3}, \quad \Theta = \frac{2H}{3J} + \frac{J}{3\cdot 2^5},$$

$$H = \Delta^2_{4,2} - 3\Delta_{4,1}\Delta_{4,3} + 12\Delta_{4,4},$$

$$L = 2\Delta^2_{4,2} - 9\Delta_{4,1}\Delta_{4,4} + 27\Delta^2_{4,3} + 27\Delta^2_{4,4} - 72\Delta_{4,2}\Delta_{4,4}.$$ 

From equation (2), the covariance matrix $\Gamma_{N_1N_2B_1B_2A_1}$ of the modes $N_1N_2B_1B_2A_1$ can be obtained by permuting the corresponding elements of $\Gamma_{B_1B_2N_1N_2A_1}$. Applying a unitary transformation $S = I \oplus \Gamma_{T_\theta} \oplus I \oplus I \oplus I$ to equation (2), we can obtain

$$S^T \Gamma_{N_1N_2B_1B_2A_1}S = \begin{pmatrix} \Gamma_{N_1N_2} & 0 \\ 0 & \Gamma_{B_1B_2A_1} \end{pmatrix},$$

where

$$\Gamma_{T_\theta} = \begin{pmatrix} V_{N_1} & \sqrt{V_{N_1}^{\dagger}} \\ \sqrt{V_{N_1}^{\dagger}} & V_{N_1} \end{pmatrix},$$

$$\Gamma_{N_1N_2} = \begin{pmatrix} \gamma_{B_1} & C_1^t & C_1^t & C_1^t & 0 \\ C_1^t & C_1^t & V_{N_1} & V_{N_1} & V_{N_1} \\ C_1^t & V_{N_1} & 0 & C_1^t & C_1^t \\ C_1^t & V_{N_1} & 0 & C_1^t & C_1^t \\ 0 & C_1^t & C_1^t & C_1^t & C_1^t \end{pmatrix},$$

and $\gamma_{B_i} = \frac{[y_{B_i} - (1 - T_{B_i})V_{N_1}]}{T_{B_i}}$, $C_i^t = C_i/\sqrt{T_N}$ for $i = 1, 4, 5$. Therefore, the eigenvalues of $\Gamma_{B_1B_2N_1N_2A_1}$ are
\[ \lambda_j = f_{s_{3,3}}(\alpha_{mn}), 1, 1, \text{where} f_{s_{3,3}}(\alpha_{mn}) \text{are the eigenvalues of} \Gamma_{B_i A_i A_i}. \]

The symplectic invariants of \( \Gamma_{B_i N_i A_i A_i} \) are denoted as \( \Delta s_i \) for \( j = 1, \ldots, 5 \). It can be proved that \( 1 - \Delta s_1 + \Delta s_2 - \Delta s_3 + \Delta s_4 - \Delta s_5 = 0 \). Therefore, one of the eigenvalues of \( \Gamma_{B_i N_i A_i A_i} \) is 1 and the others have the same forms of equation (A.2), which needs the replacement \( \Delta s_1 = 1 \) and \( \Delta s_2 = \Delta s_3, \ldots, \Delta s_5 \).

### References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Proceedings (New York: IEEE Press) pp 175–9
[3] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 Phys. Rev. Lett. 89 167901
[4] Blandino R, Leverrier A, Barbieri M, Etesses J, Grangier P and Tuille-Brouri R 2012 Phys. Rev. A 86 012327
[5] Hillery M 2000 Phys. Rev. A 61 022309
[6] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
[7] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Nature Phys. 4 726
[8] 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
[9] Sun M, Peng X, Shen Y and Guo H 2012 Int. J. Quantum Inform. 10 1250059
[10] Filip R 2008 Phys. Rev. A 77 022310
[11] Usenko V C and Filip R 2010 Phys. Rev. A 81 022318
[12] Weedbrook C, Pirandola S, Lloyd S and Ralph T C 2010 Phys. Rev. Lett. 105 110501
[13] Shen Y, Yang J and Guo H 2009 J. Phys. B: At. Mol. Opt. Phys. 42 235506
[14] Shen Y, Peng X, Yang J and Guo H 2011 Phys. Rev. A 83 025304
[15] Lodewyck J, Debuisschert T, Tuille-Brouri R and Grangier P 2009 Phys. Rev. A 72 050303
[16] Lodewyck J et al 2007 Phys. Rev. A 76 042305
[17] García-Patrón R and Cerf N J 2009 Phys. Rev. Lett. 102 130501
[18] Weedbrook C, Pirandola S and Ralph T C 2012 Phys. Rev. A 86 022318
[19] Pirandola S, García-Patrón R, Braunstein S L and Lloyd S 2009 Phys. Rev. Lett. 102 050503
[20] Renner R, Gisin N and Kraus B 2005 Phys. Rev. A 72 012332
[21] Renes J M and Smith G 2007 Phys. Rev. Lett. 98 020502
[22] Wang M and Fan W 2010 Phys. Lett. A 374 2434
[23] Huang P, Zhu J, He G and Zeng G 2012 J. Phys. B: At. Mol. Opt. Phys. 45 135501
[24] Huang P, He G, Lu Y and Zeng G 2011 Phys. Scr. 83 015005
[25] Grosshans F, Cerf N J, Wenger J, Tuille-Brouri R and Grangier P 2003 Quantum Inform. Comput. 3 535
[26] Weedbrook C, Grosse N B, Symul T, Lam P K and Ralph T C 2008 Phys. Rev. A 77 052313
[27] Assche G V 2006 Quantum Cryptography and Secret-Key Distillation (Cambridge: Cambridge University Press)
[28] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 IEEE Trans. Inform. Theory 41 1915
[29] García-Patrón R 2007 PhD Thesis Université Libre de Bruxelles
[30] García-Patrón R and Cerf N J 2006 Phys. Rev. Lett. 97 190503
[31] Navascués M, Grosshans F and Acín A 2006 Phys. Rev. Lett. 97 190502
[32] Wolf M M, Giedke G and Cirac J I 2006 Phys. Rev. Lett. 96 080502
[33] Leverrier A and Grangier P 2010 Phys. Rev. A 81 062314
[34] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 Phys. Rev. A 77 042325
[35] Holevo A S 1973 Probl. Inform. Transm. 9 177
[36] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 Nature 421 238
[37] Lu H, Fung C F, Ma X and Cai Q 2011 Phys. Rev. A 84 042344
[38] Serafini A, Illuminati F and De Siena S 2004 J. Phys. B: At. Mol. Opt. Phys. 37 L21
[39] Holevo A S, Sohma M and Hirota O 1999 Phys. Rev. A 59 1820
[40] Serafini A 2006 Phys. Rev. Lett. 96 110402
[41] Pirandola S, Serafini A and Lloyd S 2009 Phys. Rev. A 79 052327
[42] Yoshikawa J I, Miwa Y, Huck A, Andersen U L, van Loock P and Furusawa A 2008 Phys. Rev. Lett. 101 250501
[43] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[44] Eisert J and Plenio M B 2003 Int. J. Quantum Inform. 1 479
[45] Pirandola S, Braunstein S L and Lloyd S 2008 Phys. Rev. Lett. 101 200504
[46] Holevo A S 2007 Probl. Inform. Transm. 43 1
[47] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Phys. Rev. Lett. 93 170504
[48] Symul T, Alton D J, Assad S M, Lance A M, Weedbrook C, Ralph T C and Lam P K 2007 Phys. Rev. A 76 030303