International Journal of Quantum Information
Vol. 11, No. 4 (2013) 1350037 (18 pages)

DOI: 10.1142/S0219749913500378

DISCRETELY MODULATED CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH A NONDETERMINISTIC NOISELESS AMPLIFIER

JIAN FANG

State Key Laboratory of Advanced Optical Communication Systems and Networks,
Key Lab on Navigation and Location-Based Service,
Department of Electronic Engineering,
Shanghai Jiaotong University, Shanghai 200240, P. R. China
aceofspades@foxmail.com

YUAN LU

Next-Generation Communication Research Center,
Department of Wireless Communication,
Chongqing Communication Institute, Chongqing 400035, P. R. China
hawkfly_lu@163.com

PENG HUANG, GUANGQIANG HE and GUIHUA ZENG

State Key Laboratory of Advanced Optical Communication Systems and Networks,
Key Lab on Navigation and Location-Based Service,
Department of Electronic Engineering,
Shanghai Jiaotong University, Shanghai 200240, P. R. China

Received 20 March 2013
Revised 2 June 2013
Accepted 6 June 2013
Published 15 July 2013

In this paper, we first study a generalized protocol of discrete modulation for continuous-variable quantum key distribution with N coherent states in a Gaussian lossy and noisy channel and investigate its performance against collective attacks. We find that discrete modulation protocols with more than eight states do not perform better than the eight-state protocol. Then, we study the improvement of this protocol by using a nondeterministic noiseless linear amplifier (NLA) on Bob's detection stage. Results indicate that a NLA with gain g can extend the maximum transmission distance by $50\log_{10}g^2$ km and can increase the maximal tolerable excess noise. With the reconciliation efficiency β, we find the gain of NLA has a maximal value defined as $g_{\max}$ and by adjusting the gain to about $\beta g_{\max}$ one can have the best improvement on secret key rate.

Keywords: CV-QKD; discrete modulation; noiseless amplifier.

1. Introduction

Quantum key distribution (QKD), as an important practical application of quantum information, allows two distant parties (Alice and Bob) to share a common secret key for cryptography in an untrusted environment.[1,2] The security is guaranteed by the laws of quantum mechanics, exactly the no-cloning theorem which can be seen as a manifestation of Heisenberg uncertainty principle.[3] QKD with continuous-variable (CV), which encodes information in phase and amplitude quadratures of a coherent state,[4] is proven secure against collective attacks[5,6] and coherent attacks.[7] Any eavesdropping will introduce extra noise between two legal communication parties who will realize Eve's existence by detecting the excess noise.

The Gaussian-modulated CV-QKD protocol, which has been experimentally demonstrated in both laboratory[8−10] and field test,[11] is sensitive to the excess noise and has a limited range of transmission distance. With the increase of fiber length, the error-correction procedure will be rather difficult and complicated. There are two possible approaches to solve this problem. One is to design better reconciliation method[12,13] which still has a considerable efficiency at low signal-to-noise ratio (SNR). The other is to use discrete modulation, such as the four-state protocol[14] which has been studied both theoretically[15−17] and experimentally.[18] The four-state protocol has a high reverse reconciliation efficiency (at least 80%) at low SNR and permits longer transmission distance than Gaussian protocol.

To this day, two-, four- and eight-state protocols have been studied.[15,19,20] In fact, discrete modulation with more than eight states is possible. A generalized protocol using N coherent states $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$ was considered in Ref. 21 under the assumption of a lossy but noiseless quantum channel. In this paper, we study the security of this generalized protocol in a Gaussian lossy and noisy channel. By establishing the entanglement-based (EB) scheme of this general protocol, we investigate the lower bound of secret key rate against collective attacks.

To improve the performance of CV-QKD, one possible way is to add an amplifier on Bob's detection stage.[22] It has been shown that using a deterministic optical amplifier can compensate the imperfections of a detector, but the effect is limited. It is mainly because the amplification procedure of quantum signal will also introduce extra noise. Interestingly, a recent paper[23] indicates that by using a nondeterministic noiseless linear amplifier (NLA) one can dramatically extend the maximum transmission distance in Gaussian-modulated CV-QKD. Inspired by Ref. 23, here we investigate the improvement of NLA used in the discrete modulation protocols.

The paper is organized as follows: In Sec. 2, the general scheme for discrete-modulated CV-QKD protocol with N coherent states is theoretically studied. In Sec. 3, the effect of using NLA in the discrete modulation protocol is discussed with numerical simulations. The conclusions are given in Sec. 4.

2. General Scheme for Discrete Modulation Protocol

In this section, we first describe the general scheme for discrete modulation and present the notations and assumptions. Then, we derive the expression for secret key rate and discuss the performance of this protocol.

2.1. *Description of the generalized protocol*

In the prepare-and-measure (PM) version of the discrete modulation protocol, Alice randomly chooses one of the coherent states $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$ shown in Fig. 1, where α is a positive real number and $k \in \{0, 1, 2, \ldots, N-1\}$, and sends it to Bob with probability $1/N$. Hence, Bob sees a mixture ρ_N given by:

$$\rho_N = \frac{1}{N}\sum_{k=0}^{N-1}|\alpha_k\rangle\langle\alpha_k| = \frac{e^{-\alpha^2}}{N}\sum_{k=0}^{N-1}\sum_{m,n=0}^{\infty}\frac{\alpha^{m+n}e^{2ik(m-n)\pi/N}}{\sqrt{m!}\sqrt{n!}}|m\rangle\langle n|.$$

Notice that if $m - n \equiv 0 \pmod N$, $\sum_{k=0}^{N-1} e^{2ik(m-n)\pi/N}$ equals to N, otherwise equals to 0. Thus, we have:

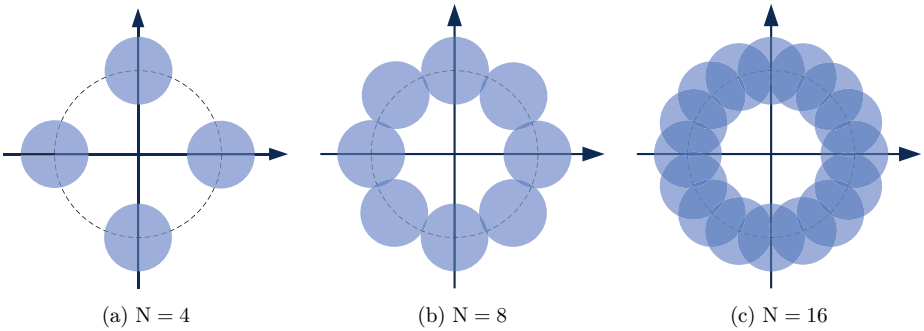
$$\rho_N = e^{-\alpha^2}\sum_{k=0}^{N-1}\sum_{m,n=0}^{\infty}\frac{\alpha^{Nm+Nn+2k}|Nm+k\rangle\langle Nn+k|}{\sqrt{(Nm+k)!}\sqrt{(Nn+k)!}} = \sum_{k=0}^{N-1}\lambda_k|\phi_k\rangle\langle\phi_k|, \tag{1}$$

where

$$\begin{aligned}\lambda_k &= e^{-\alpha^2}\sum_{n=0}^{\infty}\frac{(\alpha^2)^{Nn+k}}{(Nn+k)!},\\ |\phi_k\rangle &= \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}\frac{\alpha^{Nn+k}}{\sqrt{(Nn+k)!}}|Nn+k\rangle\end{aligned} \tag{2}$$

for $k \in \{0, 1, 2, \ldots, N-1\}$. A particular purification $|\Phi_N\rangle$ of the state ρ_N can be obtained by Schmidt decomposition[14]

$$|\Phi_N\rangle = \sum_{k=0}^{N-1}\sqrt{\lambda_k}|\phi_k\rangle|\phi_k\rangle \tag{3}$$



(a) N = 4 (b) N = 8 (c) N = 16

Fig. 1. Discrete modulation with N coherent states.

such that $\rho_N = \mathrm{Tr}_A(|\Phi_N\rangle\langle\Phi_N|)$. As the states $|\alpha_k\rangle$ could be expressed as linear combinations of $|\phi_k\rangle$, we have:

$$|\Phi_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |\psi_k\rangle|\alpha_k\rangle, \tag{4}$$

where the states

$$|\psi_k\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{2ikn\pi/N}|\phi_n\rangle \tag{5}$$

are orthogonal non-Gaussian states. The covariance matrix γ_{AB} has the following form

$$\gamma_{AB} = \begin{bmatrix} X\mathbb{I}_2 & Z_N\sigma_z \\ Z_N\sigma_z & Y\mathbb{I}_2 \end{bmatrix}, \tag{6}$$

where $\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The diagonal elements of the covariance matrix γ_{AB} can be calculated as follows[24]:

$$\begin{aligned} X &= \langle\Phi_N|(\hat{a}^\dagger + \hat{a})^2|\Phi_N\rangle = \underbrace{\langle\Phi_N|(\hat{a}^\dagger)^2 + \hat{a}^2|\Phi_N\rangle}_{0} + \langle\Phi_N|\underbrace{\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger}_{=1+2\hat{a}^\dagger\hat{a}}|\Phi_N\rangle \\ &= \langle\Phi_N|1 + 2\hat{a}^\dagger\hat{a}|\Phi_N\rangle = \mathrm{Tr}[(1 + 2\hat{a}^\dagger\hat{a})\rho_N] \\ &= 1 + 2\sum_{k=0}^{N-1} \lambda_k\langle\phi_k|\hat{a}^\dagger\hat{a}|\phi_k\rangle = 1 + 2\alpha^2, \end{aligned} \tag{7}$$

$$\begin{aligned} Y &= \langle\Phi_N|(\hat{b}^\dagger + \hat{b})^2|\Phi_N\rangle = \underbrace{\langle\Phi_N|(\hat{b}^\dagger)^2 + \hat{b}^2|\Phi_N\rangle}_{0} + \langle\Phi_N|\underbrace{\hat{b}^\dagger\hat{b} + \hat{b}\hat{b}^\dagger}_{=1+2\hat{b}^\dagger\hat{b}}|\Phi_N\rangle \\ &= \langle\Phi_N|1 + 2\hat{b}^\dagger\hat{b}|\Phi_N\rangle = \mathrm{Tr}[(1 + 2\hat{b}^\dagger\hat{b})\rho_N] \\ &= 1 + 2\sum_{k=0}^{N-1} \lambda_k\langle\phi_k|\hat{b}^\dagger\hat{b}|\phi_k\rangle = 1 + 2\alpha^2, \end{aligned} \tag{8}$$

where $\hat{a}$, $\hat{a}^\dagger$ and $\hat{b}$, $\hat{b}^\dagger$ are the annihilation and creation operators of Alice's and Bob's modes, respectively. The correlation term of covariance matrix is

$$\begin{aligned} Z_N &= \langle\Phi_N|(\hat{a}^\dagger + \hat{a})(\hat{b}^\dagger + \hat{b})|\Phi_N\rangle = \underbrace{\langle\Phi_N|\hat{a}\hat{b}^\dagger + \hat{a}^\dagger\hat{b}|\Phi_N\rangle}_{0} + \langle\Phi_N|\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger|\Phi_N\rangle \\ &= \langle\Phi_N|\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger|\Phi_N\rangle = 2\mathrm{Re}\langle\Phi_N|\hat{a}\hat{b}|\Phi_N\rangle \\ &= 2\mathrm{Re}\left[\langle\Phi_N|\alpha^2\sum_{n=0}^{N-1}\frac{\lambda_{n-1}}{\sqrt{\lambda_n}}|\phi_{n-1}\rangle|\phi_{n-1}\rangle\right] = 2\alpha^2\sum_{k=0}^{N-1}\sqrt{\frac{\lambda_{k-1}^3}{\lambda_k}}. \end{aligned} \tag{9}$$

When $N = 2, 4$ and 8, the values of Z_N coincide with previous results in Refs. 14 and 20. The covariance matrix in Eq. (6) has a similar form with the one in Gaussian-modulated protocol, which uses the Gaussian distributed random numbers with

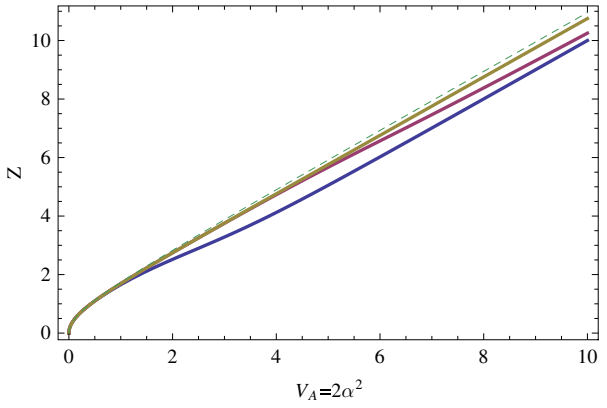


Fig. 2. Comparison of the correlation Z_N for discrete modulation and Z_G for Gaussian modulation as a function of V_A. Curves from top to bottom are Z_G, Z_{16}, Z_8, Z_4.

variance V_A to complete a continuous modulation. In the covariance matrix of Gaussian protocol, the diagonal elements are $X = Y = 1 + V_A$ and the correlation term Z_N is replaced by $Z_G = \sqrt{V_A^2 + 2V_A}$. Comparison between discrete modulation Z_N and Gaussian modulation $Z_G = \sqrt{V_A^2 + 2V_A}$ as a function of α is shown in Fig. 2. When $V_A = 2\alpha^2$ is small enough, Z_N is indistinguishable from Z_G, meaning that in this region the mutual information between Bob and Eve is very similar with Gaussian protocol. With the increment of V_A, covariance Z_4 and Z_8 begin to deviate from Z_G, while Z_{16} is still close to Gaussian modulation.

Alice's modulated states are sent to Bob through the quantum channel and Bob performs the heterodyne detection.[36] He divides the signal into two beams by a balanced beam splitter and applies homodyne detection on each of them, measuring the amplitude quadrature $\hat{q}$ on one of the signal beams and the phase quadrature $\hat{p}$ on the other. In order to measure the quadrature $\hat{p}$, Bob dephases the local oscillator by $\pi/2$. He uses both of the outcomes to infer the state Alice sends. For example, if Alice sends the state $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$ to Bob, the measurement results (B_q, B_p) of quadratures $\hat{q}$ and $\hat{p}$ are relevant to the corresponding quadratures of $|\alpha_k\rangle$. That means Alice and Bob share two correlated vectors $(A_q, A_p) = (\alpha \cos\frac{2k\pi}{N}, \alpha \sin\frac{2k\pi}{N})$ and (B_q, B_p). Notice that there is no active basis choice in the measurement and no data is discarded, so both of the quadratures can be used for key distribution.

2.2. *Notations and assumptions*

The PM version of the general discrete modulation protocol is described as follows:

- Alice randomly chooses a number $k \in \{0, 1, 2, \ldots, N-1\}$ with equal probability and sends the coherent states $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$ to Bob through a Gaussian lossy and noisy quantum channel. The channel is characterized by a transmission

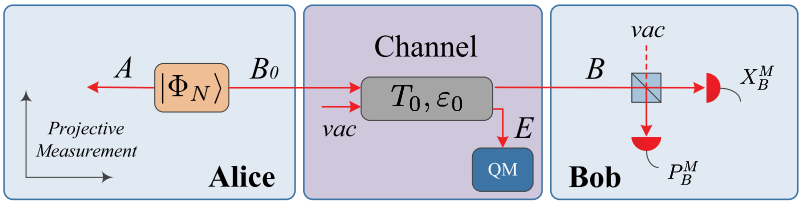


Fig. 3. EB scheme of discrete modulation protocol.

efficiency T_0 and an excess noise ε_0, resulting in a noise variance of $1 + T_0\varepsilon_0$ at Bob's input. She then records the quadrature information of this coherent state as a vector $(A_q, A_p) = (\mathrm{Re}(\alpha_k), \mathrm{Im}(\alpha_k)) = (\alpha\cos(\frac{2k\pi}{N}), \alpha\sin(\frac{2k\pi}{N}))$.

- When Bob receives the state, he splits it into two beams by using a 50:50 beam splitter and performs heterodyne detection. One output is directly measured by homodyne detection and the other one is homodyned after dephased with $\pi/2$. Both the results are kept by Bob as a vector (B_q, B_p).

The PM scheme described above is equivalent to the EB version shown in Fig. 3. In the EB scheme:

- Alice prepares two-mode entanglement states $|\Phi_N\rangle$ defined in Eq. (4). She performs projective measurements $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|, \ldots, |\psi_{N-1}\rangle\langle\psi_{N-1}|\}$ on her half of the states and sends the other half to Bob through the quantum channel. Since the state $|\Phi_N\rangle$ can be written as $\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|\psi_k\rangle|\alpha_k\rangle$, Alice projects a coherent state $|\alpha_k\rangle$ on Bob's mode with equal probability when her measurement results in a number $k \in \{0, 1, 2, \ldots, N-1\}$. She then records her measurement as a vector $(A_q, A_p) = (\alpha\cos(\frac{2k\pi}{N}), \alpha\sin(\frac{2k\pi}{N}))$.
- Bob's heterodyne detector is modeled by a beam splitter with transmission $\eta = 0.5$ and coupled with a vacuum state $|0\rangle$. Bob measures the quadrature $\hat{q}$ on one output and the $\hat{p}$ on another simultaneously. The results of the measurements are B_q and B_p, which Bob writes them as a vector (B_q, B_p).

After the quantum transmission phase, Alice and Bob share two correlated vectors $x = (A_{q_1}, A_{p_1}, \ldots, A_{q_m}, A_{p_m})$ and $y = (B_{q_1}, B_{p_1}, \ldots, B_{q_m}, B_{p_m})$, where m is the number of pulses they used for key distillation. The elements (A_{q_i}, A_{p_i}) in x have the discrete values from $\{(\alpha\cos(\frac{2k\pi}{N}), \alpha\sin(\frac{2k\pi}{N}))\}$, $k \in \{1, 2, \ldots, N-1\}$. The quantum channel considered here is a normal linear model with the relation between Alice and Bob such that,

$$\begin{aligned} B_{q_i} &= tA_{q_i} + z_{q_i}, \\ B_{p_i} &= tA_{p_i} + z_{p_i}, \end{aligned} \tag{10}$$

where $t = \sqrt{T_0}$, z_{q_i} and z_{p_i} following a centered normal distribution with variance $1 + T_0\varepsilon_0$ where ε_0 is the channel excess noise. The main merit of a normal linear

channel is that it can be featured by a transmission T_0 and an added noise. These parameters can be determined even when the modulation is discrete and can have the same values as Gaussian modulation. Under this assumption, the covariance matrix could be easily obtained and Eve's information can be bounded by using the Gaussian optimality theorem.[15]

Finally, Alice and Bob perform classical data processing, including the reconciliation and privacy amplification. Since the reverse reconciliation has been proven more advantageous than direct one in CV-QKD performance,[25] we mainly consider the reverse reconciliation in this paper.

2.3. *Performance of the protocol*

Now we turn to consider the performance of the general discrete modulation protocol with heterodyne detection. According to the fact that coherent attacks are the most powerful eavesdropping attacks and are not more efficient than collective attacks,[5,6] we will analyze the security against collective attacks.

After passing through the Gaussian lossy and noisy channel, the covariance matrix between Alice and Bob becomes

$$\begin{aligned}\gamma_{AB} &= \begin{bmatrix} \gamma_A & C_{AB} \\ C_{AB}^T & \gamma_B \end{bmatrix} = \begin{bmatrix} a\mathbb{I}_2 & c\,\sigma_z \\ c\sigma_z & b\mathbb{I}_2 \end{bmatrix} \\ &= \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T_0}Z_N\sigma_z \\ \sqrt{T_0}Z_N\sigma_z & (T_0V_A+1+T_0\varepsilon_0)\mathbb{I}_2 \end{bmatrix},\end{aligned} \tag{11}$$

where

$$\begin{aligned} Z_N &= 2\alpha^2\sum_{k=0}^{N-1}\sqrt{\frac{\lambda_{k-1}^3}{\lambda_k}}, \\ \lambda_k &= e^{-\alpha^2}\sum_{n=0}^{\infty}\frac{(\alpha^2)^{Nn+k}}{(Nn+k)!} \end{aligned} \tag{12}$$

and $V_A = 2\alpha^2$ is Alice's modulation variance in PM scheme. According to the optimality of Gaussian attacks, the secret key rate K of a bipartite quantum state ρ_{AB} with a covariance matrix γ_{AB} (even non-Gaussian) is always larger than Gaussian state ρ_{AB}^G with the identical covariance matrix.[5,6] So, we can establish a corresponding Gaussian scheme with covariance matrix γ_{AB}^G such that

$$\gamma_{AB}^G = \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T}Z_G\sigma_z \\ \sqrt{T}Z_G\sigma_z & (TV_A+1+T\varepsilon)\mathbb{I}_2 \end{bmatrix}. \tag{13}$$

To make $\gamma_{AB}^G = \gamma_{AB}$, we have

$$\begin{aligned} T &= T_0(Z_N/Z_G)^2, \\ \varepsilon &= (Z_G/Z_N)^2(V_A+\varepsilon_0) - V_A. \end{aligned} \tag{14}$$

With a reverse reconciliation efficiency β, the secret key rate of the discrete modulation protocol is

$$K \geq K_G = \beta I(x;y) - \chi(y;E) \tag{15}$$

that means K_G is a lower bound on secret key rate for discrete modulation protocol. The mutual information between Alice and Bob $I(x;y)$ with heterodyne detection can be obtained from elements of the covariance matrix and given by:

$$I(x;y) = \log_2\left[\frac{(a+1)(b+1)}{(a+1)(b+1)-c^2}\right] = \log_2\left[1+\frac{TV_A}{2+TV_A+T\varepsilon}\right]. \tag{16}$$

Eve's information on Bob's measurement is given by the Holevo bound[26]:

$$\chi(y;E) = S(E) - S(E|X_B), \tag{17}$$

where $S(\cdot)$ denotes the von-Neumann entropy and E denotes Eve's state at the end of the quantum channel shown in Fig. 3. For a n mode Gaussian state ρ, the von-Neumann entropy can be calculated with its symplectic eigenvalues[27]:

$$S(\rho) = \sum_{k=1}^{n} G(\nu_k), \tag{18}$$

where ν_k is the symplectic eigenvalue of the kth mode and $G(\nu)$ is defined as,

$$G(\nu) = \left[\frac{\nu+1}{2}\right]\log_2\left[\frac{\nu+1}{2}\right] - \left[\frac{\nu-1}{2}\right]\log_2\left[\frac{\nu-1}{2}\right]. \tag{19}$$

Notice the fact that Eve has the ability to purify the states shared by Alice and Bob, and after Bob's measurement the state ρ_{AE} collapses into a pure state. Hence, Eve's information on Bob's measurement can be calculated by

$$\chi(y;E) = G(\nu_1) + G(\nu_2) - G(\nu_3). \tag{20}$$

The first two symplectic eigenvalues $\nu_{1,2} \geq 1$ are given by

$$\nu_{1,2} = \sqrt{\frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D}]}, \tag{21}$$

where Δ and D are defined as

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= (ab - c^2)^2. \end{aligned} \tag{22}$$

The third symplectic eigenvalue $\nu_3 \geq 1$ is obtained from the covariance matrix of mode A after Bob's measurements and can be expressed as[28]

$$\nu_3 = a - \frac{c^2}{b+1}. \tag{23}$$

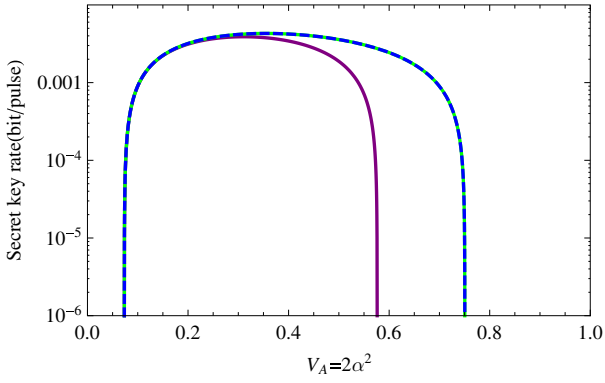


Fig. 4. (Color online) Heterodyne detection for discrete-modulated protocols with different $V_A = 2\alpha^2$ at 10dB channel loss. Curves from left to right represent $N = 4$ (purple), $N = 8$ (green), $N = 16$ (blue, dashed). $\varepsilon_0 = 0.005$, $\beta = 80\%$.

Based on the above discussions, we calculate the theoretical secret key rate of discrete-modulated protocol with heterodyne detection. Figures 4 and 5 show the secret key rate of $N = 4,\ 8,\ 16$ states. The curve of 16 states is almost the same with the eight-state protocol. In Fig. 4, eight-state protocol can always achieve larger secret key rate than four-state protocol at each modulation variance. Figure 5 shows that with the same V_A, eight-state protocol has the longer transmission distance and higher secret key rate than the $N < 8$ states while protocols with $N > 8$ states will not perform better than $N = 8$. Considering the coding issue, the most efficient modulating method is to use $N = 2^n$ states which needs only $\log_2(N)$ binary random number generators to equiprobably produce the decimal number $\{0, 1, \ldots, N-1\}$ without redundancy. In this point of view, the most suitable discrete modulation protocol is $N = 8$.

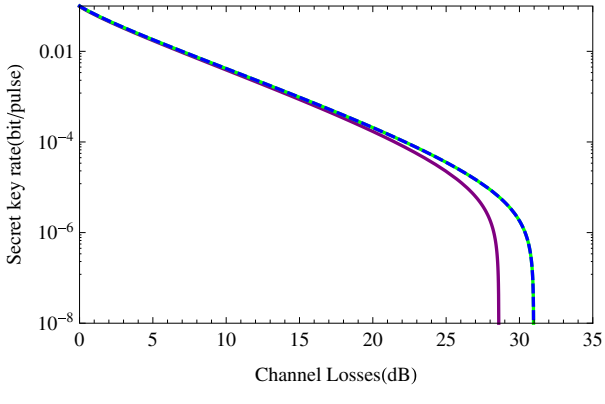


Fig. 5. (Color online) Maximized secret key rates with optimal V_A. Curves from left to right represent $N = 4$ (purple), $N = 8$ (green), $N = 16$ (blue, dashed). $\varepsilon_0 = 0.005$, $\beta = 80\%$.

Finally, let us discuss the reconciliation efficiency β in Eq. (15). In the calculations above we choose $\beta = 0.8$. In fact, the reverse reconciliation of two-state and four-state protocols can achieve more than 80% efficiency at low SNR by using a capacity-achieving code and a repetition code.[14] In eight-state protocol, although the modulation of each quadrature is nonuniform, one can still have a good error-correction code, such as the *Raptor codes* at low SNR conditions.[29,30,37] In strong loss cases, a repetition code can be combined to raptor code to achieve the desired reconciliation efficiency.[20]

3. Improved Discrete-Modulated Protocol with a NLA

A NLA is a probabilistic device, which can amplify a coherent state without introducing extra noise. In recent years, NLA has been approximately implemented in experiments[31–33] and proved useful for quantum communications. In this section, we will investigate the improvement of discrete-modulated protocol by using the NLA on Bob's detection stage.

3.1. *Nondeterministic noiseless amplification*

The nondeterministic noiseless amplifier is described as a transformation of a coherent state $|\alpha\rangle$ such that

$$|\alpha\rangle\langle\alpha| \to P_s|g\alpha\rangle\langle g\alpha| + (1 - P_s)|0\rangle\langle 0|, \tag{24}$$

where $g \geq 1$ is the gain of amplifier and P_s is the success probability. An ideal NLA can be defined as an Fock basis operator

$$g^{\hat{n}}|n\rangle = g^n|n\rangle, \tag{25}$$

where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the photon number operator.

Consider a covariance matrix γ_{AB} in the Gaussian modulation protocol

$$\gamma_{AB} = \begin{bmatrix} a\mathbb{I}_2 & c\sigma_z \\ c\sigma_z & b\mathbb{I}_2 \end{bmatrix}. \tag{26}$$

Since the noiseless operator $g^{\hat{n}}$ is in the Fock basis, we cannot directly apply this transformation on γ_{AB}. However, inspired by Refs. 34 and 35, the elements of γ_{AB} and the density matrix ρ_{AB} in Fock basis could be associated by Husimi Q-function

$$Q(\mathbf{R}) = \frac{\sqrt{\det \Gamma_{AB}}}{\pi^2} e^{-\mathbf{R}^T\Gamma_{AB}\mathbf{R}}, \tag{27}$$

where

$$\Gamma_{AB} = (\gamma_{AB} + \mathbb{I}_4)^{-1} \tag{28}$$

and the matrix Γ_{AB} can be written as

$$\Gamma_{AB} = \begin{bmatrix} A\mathbb{I}_2 & C\sigma_z \\ C\sigma_z & B\mathbb{I}_2 \end{bmatrix}, \tag{29}$$

where A, B, C are functions of a, b, c. One can establish a relationship between elements of Γ_{AB} and normalized density matrix elements in Fock basis. The NLA transformation then can be simply written as,

$$\hat{G} = \hat{\mathbb{I}}_A \otimes g^{\hat{n}_B}. \tag{30}$$

Since $g^{\hat{n}}$ is a Gaussian operator, it transforms a Gaussian state to another Gaussian one. With straightforward calculation, the matrix Γ'_{AB} after the amplification is[35]

$$\Gamma'_{AB} = \begin{bmatrix} A\mathbb{I}_2 & gC\sigma_z \\ gC\sigma_z & \left(g^2 B - \dfrac{g^2-1}{2}\right)\mathbb{I}_2 \end{bmatrix}. \tag{31}$$

Using the relation in Eq. (28), finally we obtain the covariance matrix γ'_{AB} after amplification

$$\gamma'_{AB} = \begin{bmatrix} a'\mathbb{I}_2 & c'\sigma_z \\ c'\sigma_z & b'\mathbb{I}_2 \end{bmatrix}, \tag{32}$$

where

$$\begin{aligned} a' &= a + \frac{c^2(g^2-1)}{2+(1-b)(g^2-1)}, \\ b' &= \frac{2+(b+1)}{2+(1-b)(g^2-1)} - 1, \\ c' &= \frac{2cg}{2+(1-b)(g^2-1))}. \end{aligned} \tag{33}$$

In experiments the success probability P_s depends on many factors, but it can be upper bounded by $1/g^2$.[23] In fact, the implementation of a perfect NLA would be quite difficult. In recent experiments,[31–33] researchers have used different methods to approximately realize the NLA. So, the experimental success probability is lower than the theoretical prediction due to various limitations and imperfections. In this paper, we use the upper bound $P_s = 1/g^2$ to investigate the best performance of an ideal NLA, while in experiments the improvement of secret key rate may be reduced.

3.2. *Modified secret key rate*

The improved EB scheme of discrete modulation protocol using a NLA is shown in Fig. 6. In this scheme, a NLA is placed at Bob's detection stage. After passing through the quantum channel, the covariance matrix γ_{AB_1} can be written as

$$\gamma_{AB_1} = \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T_0}Z_N\sigma_z \\ \sqrt{T_0}Z_N\sigma_z & (T_0V_A + 1 + T_0\varepsilon_0)\mathbb{I}_2 \end{bmatrix}. \tag{34}$$

As we discussed in Sec. 2, the lower bound of secret key rate in discrete-modulated protocol can be estimated by an equivalent Gaussian protocol which has the identical

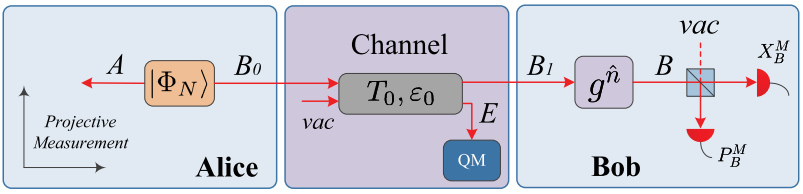


Fig. 6. Improved discrete modulation EB scheme with a NLA.

covariance matrix that

$$\gamma_{AB_1}^G = \begin{bmatrix} a\mathbb{I}_2 & c\sigma_z \\ c\sigma_z & b\mathbb{I}_2 \end{bmatrix} = \begin{bmatrix} (V_A+1)\mathbb{I}_2 & \sqrt{T}Z_G\sigma_z \\ \sqrt{T}Z_G\sigma_z & (TV_A+1+T\varepsilon)\mathbb{I}_2 \end{bmatrix}, \tag{35}$$

where $T = T_0/F$ and $\varepsilon = 2(F-1)\alpha^2 + F\varepsilon_0$. Parameter F is defined as $F = (Z_G/Z_N)^2$. Since the NLA always transforms a Gaussian state into another Gaussian state, the covariance matrix after NLA can be obtained by using Eq. (33) and finally we have

$$\gamma_{AB}^G = \begin{bmatrix} a'\mathbb{I}_2 & c'\sigma_z \\ c'\sigma_z & b'\mathbb{I}_2 \end{bmatrix}, \tag{36}$$

where

$$\begin{aligned} a' &= V_A\left[\frac{4-(g^2-1)T(V_A+2\varepsilon-2)}{2-(g^2-1)T(V_A+\varepsilon)}\right], \\ b' &= \frac{2+(g^2+1)T(V_A+\varepsilon)}{2-(g^2-1)T(V_A+\varepsilon)}, \\ c' &= \frac{2g\sqrt{T(V_A+2V_A)}}{2-(g^2-1)T(V_A+\varepsilon)}. \end{aligned} \tag{37}$$

Parameters T and ε are defined in Eq. (14). According to the optimality of Gaussian attacks, when the noiseless amplification is successful, the secret key rate will be lower bounded by the following equation

$$K' \geq \beta I'(x;y) - \chi'(y;E), \tag{38}$$

where the mutual information between Alice and Bob is

$$I'(x;y) = \log_2\left[\frac{(a'+1)(b'+1)}{(a'+1)(b'+1)-c^2}\right] \tag{39}$$

and $\chi'(y;E)$ can be calculated by

$$\chi'(y;E) = G(\nu_1) + G(\nu_2) - G(\nu_3), \tag{40}$$

where $G(x)$ is defined in Eq. (19). Symplectic eigenvalues $\nu_{1,2} \geq 1$ are determined by the covariance matrix γ_{AB} and can be calculated by the following equations

$$\nu_{1,2} = \sqrt{\frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D}]}, \tag{41}$$

where

$$\begin{aligned} \Delta &= a'^2 + b'^2 - 2c'^2, \\ D &= (a'b' - c'^2)^2. \end{aligned} \tag{42}$$

The third eigenvalue $\nu_3 \geq 1$ can be calculated using the same method described in Sec. 2 and is given by

$$\nu_3 = a' - c'^2/(b' + 1) \tag{43}$$

As the amplification is nondeterministic, the final secret key rate K_{nd} should include the success probability such that

$$K_{\text{nd}} = P_s K' \geq \frac{1}{g^2}[\beta I'(x;y) - \chi'(y;E)]. \tag{44}$$

To make all the parameters have physical interpretations, for example, the symplectic eigenvalues $\nu_{1,2,3}$ must be larger than 1, the NLA gain should ensure $\Delta^2 - 4D \geq 0$ and $\Delta \leq D + 1$, where Δ and D are defined in Eq. (42). The full expression of maximum NLA gain is quite long. However, at small modulation variance (e.g. $\alpha \leq 0.5$) $Z_N \approx Z_G = 2\alpha\sqrt{\alpha^2 + 1}$. Hence, the expression of $g_{\max}$ can be simply written as

$$g_{\max} = \sqrt{\frac{(1+\alpha^2)[2 - \sqrt{2 - (2-\varepsilon)T\varepsilon}]^2}{T\alpha^2(2-\varepsilon)^2}}. \tag{45}$$

The maximum NLA gain as a function of losses with different α is shown in Fig. 7. We can find that $g_{\max}$ increases with the channel losses and smaller α permits higher maximum gain values.

3.3. *Results and discussion*

Now we will evaluate the performance of discrete-modulated CV-QKD using a nondeterministic noiseless amplifier. As modulating with eight states is sufficient, here we will investigate the secret key rate of the eight-state protocol with heterodyne detection.

As we discussed in Sec. 3.2, Alice's modulation variance is an important parameter in discrete modulation protocol. We find that with the increase of NLA gain, the optimal V_A will also gradually increase at a certain channel loss, shown in Fig. 8. That means for different NLA gain, we need to adjust V_A legitimately to achieve the maximum secret key rates.

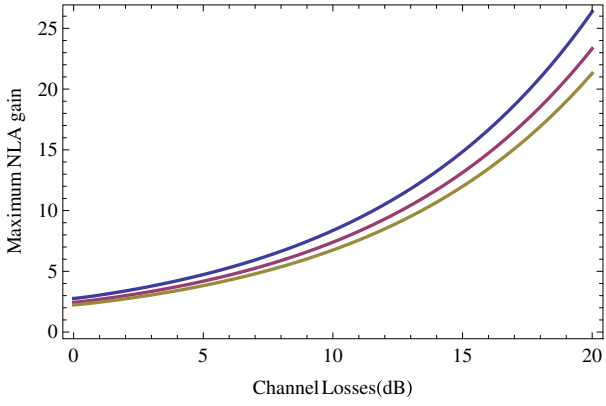


Fig. 7. Maximum NLA gain as a function of channel losses. Curves from bottom to top: $\alpha = 0.5$, $\alpha = 0.4$ and $\alpha = 0.3$. $\varepsilon_0 = 0.005$.

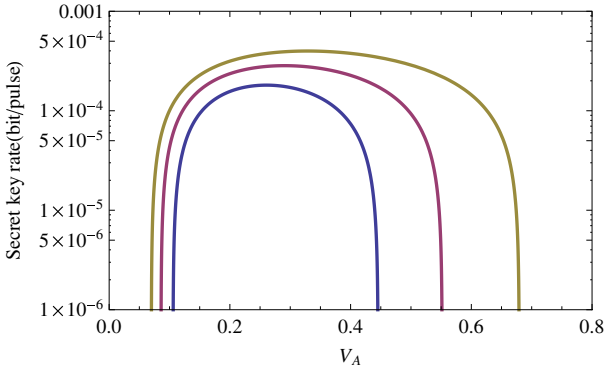


Fig. 8. Heterodyne detection with a noiseless amplifier at 20 dB channel loss. From bottom to top: $g = 1$, $g = 2$ and $g = 4$. $\varepsilon_0 = 0.005$, $\beta = 80\%$.

The maximized secret key rate of eight-state protocol with a NLA is displayed in Fig. 9. Alice's modulation variance V_A is adjusted to the optimal value. We find that there are two main improvements by using NLA: the prolongation of maximum transmission distance and the increase of secret key rate. We calculate the maximum channel losses and transmission distance of the eight-state protocol with NLA gain $g = 1, 2, 3, 4, 5$ with excess noise fixed to 0.005 and V_A optimized to maximize the secret key rate. Numerical results are shown in Table 1. When the secret key rate is below 10^{-10} bit/pulse, the eight-state protocol with NLA gain $g = 2$ and $g = 4$ correspond to the transmission of 1.63×10^{-4} (189.5 km) and 4.07×10^{-5} (219.5 km), respectively, which are approximately $1/g^2$ of the original (without NLA) transmission 6.48×10^{-4} (159.4 km). That means using NLA in discrete modulation protocol can increase the maximum transmission distance by $50 \log_{10} g^2$ km, where g is the gain of NLA.

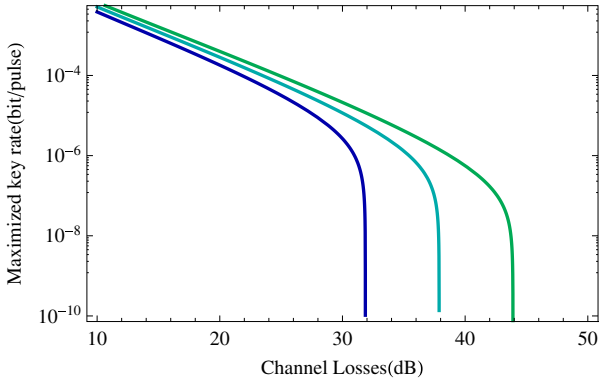


Fig. 9. Heterodyne detection for eight-state protocol with a NLA. From left to right: $g = 1$, $g = 2$ and $g = 4$. Secret key is maximized by adjusting V_A to the optimal value. $\varepsilon_0 = 0.005$, $\beta = 80\%$.

Table 1. Maximum transmission distance with a NLA.

g	Optimal V_A	$L_{\max}$/dB	$T_{\lim}$	$d_{\max}$/km
1	0.217	31.88	6.48×10^{-4}	159.4
2	0.200	37.89	1.63×10^{-4}	189.5
3	0.192	41.40	7.24×10^{-5}	207.0
4	0.186	43.90	4.07×10^{-5}	219.5
5	0.183	45.83	2.61×10^{-5}	226.5

The other main improvement is the secret key rate. When Alice and Bob ensure their locations, the length of quantum channel is seldom changed. A more realistic question is: at this distance, how should we adjust the NLA gain to obtain the best performance. To solve this problem, we vary the NLA gain at different channel losses and calculate the secret key rate. We find that there is an optimal NLA gain g_{opt} to maximize the secret key rate for any channel losses, which cannot exceed the $g_{\max}$ defined in Eq. (45). Interestingly, the optimal NLA gain is also associated with the reconciliation efficiency β. According to Fig. 10, g_{opt} increases with β, and reaches $g_{\max}$ when $\beta = 1$. A more detailed results are shown in Table 2. When the losses are 10 dB and 20 dB, the optimal NLA gain are changed with different reconciliation efficiency β and we can give a approximate expression that $g_{\text{opt}} \approx \beta g_{\max}$. Although the simulation results are not accurately equal to $\beta g_{\max}$, but the curves are quite flat around g_{opt} shown in Fig. 10, meaning that if β and $g_{\max}$ are known, one can approximately obtain the best performance by adjusting the gain to $\beta g_{\max}$.

In previous simulations, we assume the excess noise $\varepsilon_0 = 0.005$ which is a practical value in state-of-the-art implementations.[9,11] However, when the ε_0 increases, the quantum channel will be so noisy that one can hardly distill positive secret keys. We investigate the maximal tolerable excess noise for the eight-state protocol, which is shown in Fig. 11. Results indicate that using a NLA the tolerable excess noise can

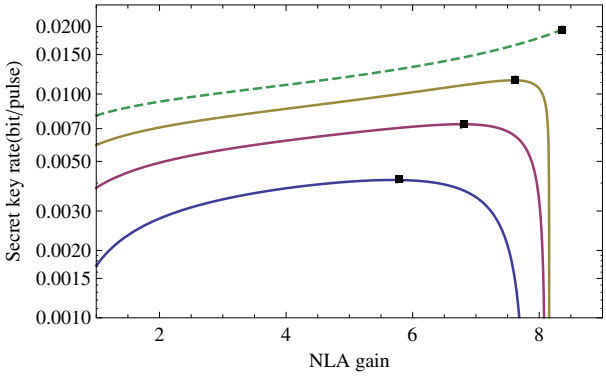


Fig. 10. (Color online) Heterodyne detection for eight-state protocol with a NLA at 10 dB loss. $V_A = 0.3$, $\varepsilon = 0.005$. From bottom to top: $\beta = 0.7$, $\beta = 0.8$, $\beta = 0.9$ and $\beta = 1$. Black points are the optimal gains.

Table 2. Optimal gain of the eight-state protocol with a NLA.

Loss/dB	β	$g_{\max}$	g_{opt}	$g_{\text{opt}}/g_{\max}$
10	0.80	8.36	6.73	0.805
10	0.85	8.36	7.16	0.856
10	0.90	8.36	7.58	0.907
10	0.95	8.36	8.01	0.958
20	0.80	26.38	20.92	0.793
20	0.85	26.38	22.29	0.845
20	0.90	26.38	23.64	0.896
20	0.95	26.38	25.01	0.948

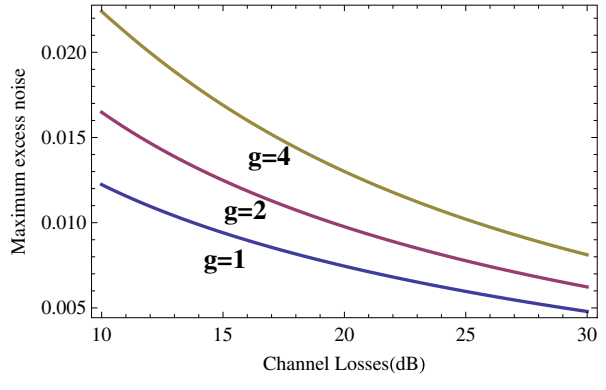


Fig. 11. Heterodyne detection for eight-state protocol with a NLA. $V_A = 0.3$, $\beta = 80\%$.

be increased, meaning that the improved protocol has a robustness against the excess noise.

4. Conclusion

In this paper, we first study the general scheme of discrete-modulated CV-QKD protocol and investigate its performance with different number of states in a lossy and noisy channel against collective attacks. Our results show that discrete modulation protocols with more than eight states do not perform better than eight-state protocol because their key rates are identical at low modulation variance ($\alpha < 0.5$). Concerning the efficiency of coding and reconciliation, we find the eight-state protocol is most suitable scenario.

Our results show that using a NLA in discrete-modulated protocol, the maximum distance can be extended by $50 \log_{10} g^2$ km, where g is the gain of NLA. With the increment of g, the maximal tolerable excess noise can also be increased. Interestingly, the NLA gain cannot be arbitrary large and has a maximum value $g_{\max}$ for each distance. We find there is an optimal NLA gain achieving the best performance, which is approximately equal to $\beta g_{\max}$. By adjusting NLA to the optimal gain, the improved scheme allows higher secret key rates than the original scenario.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61170228, 60970109, and 61102053).

References

1. N. Gisin, G. Ribordy, W. Tittle and H. Zbinden, *Rev. Mod. Phys.* **74** (2002) 145.
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkütkenhaus and M. Peev, *Rev. Mod. Phys.* **81** (2009) 1301.
3. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro and S. Lloyd, *Rev. Mod. Phys.* **84** (2012) 621.
4. F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88** (2002) 057902.
5. R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97** (2006) 190503.
6. M. Navascué, F. Grosshans and A. Acín, *Phys. Rev. Lett.* **97** (2006) 190502.
7. R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102** (2009) 110504.
8. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, *Nature (London)* **421** (2003) 238.
9. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri and P. Grangier, *Phys. Rev. A* **76** (2007) 042305.
10. B. Qi, L. Huang and H.-K. Lo, *Phys. Rev. A* **76** (2007) 052323.
11. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri and P. Grangier, *New J. Phys.* **11** (2009) 045023.
12. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor and P. Grangier, *Phys. Rev. A* **77** (2008) 042325.
13. P. Jouguet, S. Kunz-Jacques and A. Leverrier, *Phys. Rev. A* **84** (2011) 062317.

14. A. Leverrier and P. Grangier, *Phys. Rev. Lett.* **102** (2009) 180504.
15. A. Leverrier and P. Grangier, *Phys. Rev. A* **83** (2011) 042312.
16. J. Yang, B. Xu, X. Peng and H. Guo, *Phys. Rev. A* **85** (2012) 052302.
17. Y. Shen and H. Zou, *Acta Phys. Sin.* **59** (2010) 1473.
18. Y. Shen, H. Zou, L. Tian, P. Chen and J. Yuan, *Phys. Rev. A* **82** (2010) 022317.
19. Y. Zhao, M. Heid, J. Rigas and N. Lutkenhaus, *Phys. Rev. A* **79** (2009) 012307.
20. A. Becir, F. A. A. El-Orany and M. R. B. Wahiddin, *Int. J. Quantum Inform.* **10** (2012) 1250004.
21. D. Sych and G. Leuchs, *New J. Phys.* **12** (2010) 053019.
22. S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri and P. Grangier, *J. Phys. B* **42** (2009) 114014.
23. R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier and R. Tualle-Brouri, *Phys. Rev. A* **86** (2012) 012327.
24. A. Leverrier, Theoretical study of continuous-variable quantum key distribution, Ph.D. thesis, Ecole Nationale Supérieure des Télécommunications (2009).
25. F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri and P. Grangier, *Quantum Inf. Comput.* **3** (2003) 535.
26. A. S. Holevo, *Probl. Inf. Transm.* **9** (1973) 177.
27. A. S. Holevo, M. Sohma and O. Hirota, *Phys. Rev. A* **59** (1999) 1820.
28. R. García-Patrón, Quantum Information with Continuous Variables: from Bell Tests to Key Distribution, Ph.D. thesis, Université Libre de Bruxelles (2007).
29. A. Shokrollahi, Raptor Codes on Symmetric Channels, in *Proc. IEEE Int. Symp. Information Theory* (2004), p. 36.
30. A. Shokrollahi, *IEEE Trans. Inform. Theory* **52** (2006) 2551.
31. F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri and P. Grangier, *Phys. Rev. Lett.* **104** (2010) 123403.
32. A. Zavatta, J. Fiurášek and M. Bellini, *Nat. Photon.* **5** (2011) 52.
33. C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin and R. T. Thew, *Phys. Rev. A* **86** (2012) 023815.
34. J. Eisert, D. E. Browne, S. Scheel and M. B. Plento, *Ann. Phys.* **311** (2004) 431.
35. J. Fiurášek and N. J. Cerf, *Phys. Rev. A* **86** (2012) 060302.
36. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph and P. K. Lam, *Phys. Rev. Lett.* **93** (2004) 170504.
37. J. Castura and M. Yongi, A Rateless Coding and Modulation Scheme for Unknown Gaussian Channels, *CWIT'07. 10th Canadian Workshop on Information Theory* (Edmenton, Alberta, 2007).