Commun. Theor. Phys. (Beijing, China) **46** (2006) pp. 61–64
© International Academic Publishers Vol. 46, No. 1, July 15, 2006

Quantum Encryption Protocol Based on Continuous Variable EPR Correlations*

HE Guang-Qiang† and ZENG Gui-Hua‡
The State Key Laboratory of Fibre-Optic Local Area Networks and Advanced Optical Communication Systems, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200030, China

(Received October 1, 2005)

Abstract *A quantum encryption protocol based on Gaussian-modulated continuous variable EPR correlations is proposed. The security is guaranteed by continuous variable EPR entanglement correlations produced by nondegenerate optical parametric amplifier (NOPA). For general beam splitter eavesdropping strategy, the mutual information $I(\alpha,\epsilon)$ between Alice and Eve is calculated by employing Shannon information theory. Finally the security analysis is presented.*

PACS numbers: 03.67.Dd, 03.67.Hk
Key words: quantum cryptography, quantum encryption, EPR correlations, NOPA

Quantum cryptography[1] provides secret communication, where the security is guaranteed by the law of quantum mechanics.[2−4] Most of quantum cryptography schemes are about key distribution.[5−11] These schemes are nondeterministic, thus can only distribute random key instead of transmitting useful message. Recently several novel deterministic communication schemes based on discrete variable (DV) entanglement states[12,13] or the nonorthogonal states[14] are proposed, which can transmit useful message, but both the discrete variable entanglement and single quanta are neither generated nor detected easily. The continuous variable (CV) can be more easily generated and manipulated than DV, and the channel capacity of CV communication can be enhanced. Thus designing the CV quantum direct communication is a very interesting problem. In this region, Reid provided a means to distribute a discrete predetermined key[15] based on CV entanglements produced by NOPA, but the binary modulation on CV limits its efficient.

In this paper, we propose a quantum encryption protocol based on Gaussian-modulated CV EPR correlations, which can quasi securely transmit the useful message by the shared keys obtained by quantum key distribution. By adding the key-controlled noise into useful message, the information obtained by the eavesdropper (Eve), i.e., $I(\alpha,\epsilon)$ is close to 0. In addition, the channel capacity of the protocol is much higher than that of DV protocol. We firstly present the protocol in details. For the general beam splitter eavesdropping strategy, the mutual information between Alice and Eve i.e., $I(\alpha,\epsilon)$, is calculated by employing Shannon information theory. Finally, the method for detecting Eve is given.

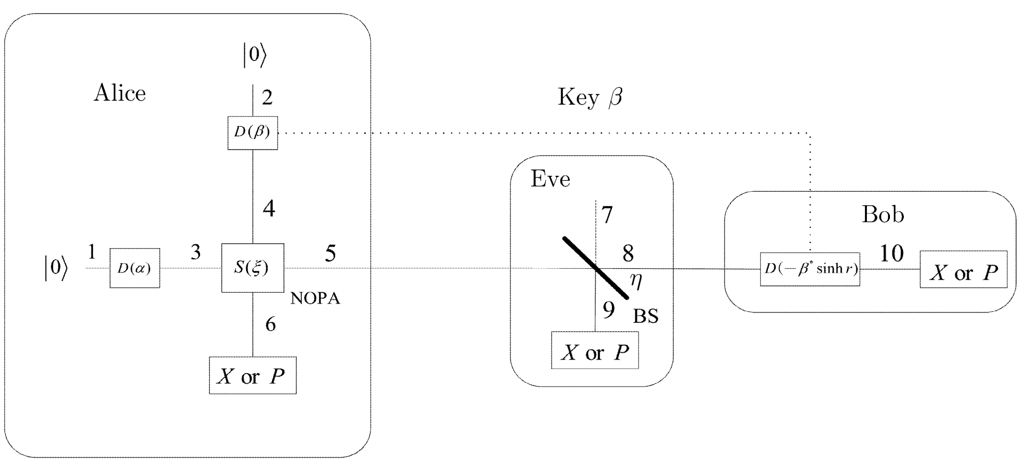

Fig. 1 Schematic representation of quantum encryption protocol based on Gaussian-modulated continuous variable EPR correlations. NOPA: nondegenerate optical parametric amplifier, LA: linear amplifier, BS: beam splitter, $D(\alpha)$: displacement operator, $S(\xi)$: two mode squeezing operator of NOPA, G: the gain of LA, η: the transmittance parameter of BS.

*The project supported by National Natural Science Foundation of China under Grant No. 60472018
†E-mail: gqhe@sjtu.edu.cn
‡E-mail: ghzeng@sjtu.edu.cn

The protocol is depicted as in Fig. 1. Alice firstly modulates $\hat{a}_1$ and $\hat{a}_2$ by applying displacement operators $\hat{D}$ ($\alpha = x + \mathrm{i}x$) and $\hat{D}$ ($\beta = y + \mathrm{i}y$) respectively, where x is useful message that will be transmitted, $X \sim N(0, \Sigma^2)$. Here we have used $Z \sim N(\mu, \sigma^2)$ to denote that the random variable Z follows Gaussian probability distribution with the average value μ and the variance σ^2. y is a shared key obtained by key distribution process, e.g. quantum key distribution, $Y \sim N(0, \sigma^2)$. The modes $\hat{a}_3 = \hat{D}^\dagger(\alpha)\hat{a}_1\hat{D}(\alpha) = \hat{a}_1 + \alpha$ and $\hat{a}_4 = \hat{D}^\dagger(\beta)\hat{a}_2\hat{D}(\beta) = \hat{a}_2 + \beta$ are two input modes of NOPA, where $\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is the displacement operator. The output modes of NOPA are $\hat{a}_5 = \hat{S}^\dagger(\xi)\hat{a}_3\hat{S}(\xi)$ and $\hat{a}_6 = \hat{S}^\dagger(\xi)\hat{a}_4\hat{S}(\xi)$, where $\hat{S}(\xi) = \exp[\kappa t(\hat{a}_3^\dagger\hat{a}_4^\dagger - \hat{a}_3\hat{a}_4)]$ is two-mode squeezed operator. As the squeezed parameter $r = \xi = \kappa t$ increases, $\hat{a}_5$ becomes increasingly correlated with $\hat{a}_6$. Alice calculates the entanglement parameter F between $\hat{a}_5$ and $\hat{a}_6$, and measures either X or P of $\hat{a}_6$ during some time slots, and writes down both the measurement results and the corresponding time slots for detecting Eve after finishing transmission. $\hat{a}_5$ is sent to Bob. Bob applies $D[-\beta^*\sinh(r)]$ to $\hat{a}_8$, ($\hat{a}_8$ is $\hat{a}_5$ without the presence of Eve), then he measures either X or P of $\hat{a}_{10}$. After finishing transmission, Alice tells Bob both her measurement results and the corresponding time slots through the classical public channel. Bob estimates $F_{\rm cal}$ by comparing Alice's measurement results with his own during the corresponding time slots. If $F_{\rm cal} > F$, Eve exists, while if $F_{\rm cal} = F$, Eve does not exist. Let us give an explicit algorithm for the protocol. The useful plain text is divided into blocks with each block consisting of l useful messages, and m random authentication codes are randomly inserted into a block to form a transmittable block with the length being $l + m$. The protocol is introduced step by step.

(p.1) Alice divides plaintext into n blocks with the length of each block being l.

(p.2) $p = 0$.

(p.3) Alice transmits the p-th block $B^{(p)} = \{\alpha_0^{(p)}, \ldots, \alpha_r^{(p)}, \ldots, \alpha_{l+m-1}^{(p)}\}$, where $\alpha_r^{(p)} = x_r^{(p)} + \mathrm{i}x_r^{(p)}$, $0 \le r \le l + m - 1$, $X \sim N(0, \Sigma^2)$, l numbers are the useful messages in the p-th block, the additional m random authentication codes are inserted randomly for detecting Eve.

(p.4) The key block $K = \{\beta_0, \ldots, \beta_s, \ldots, \beta_{l+m-1}\}$ shared by Alice and Bob serves as the encryption-decryption key in quantum encryption protocol.

(p.5) $r = 0$, $s = 0$.

(p.6) Alice modulates $\hat{a}_1$ and $\hat{a}_2$ by applying $D(\alpha_r^{(p)})$ and $D(\beta_s)$ respectively, and obtains $\hat{a}_3$ and $\hat{a}_4$.

(p.7) $\hat{a}_3$ and $\hat{a}_4$ interact with each other in NOPA, and the EPR entanglement beams $\hat{a}_5$ (travel beam) and $\hat{a}_6$ (home beam) are prepared by Alice.

(p.8) Alice sends $\hat{a}_5$ to Bob. Alice measures either X or P of $\hat{a}_6$ of m authentication codes, thus she obtains m measurement results, then she records these m measurement results and the corresponding time slots.

(p.9) Bob applies $D[-\beta_s^*\sinh(r)]$ on $\hat{a}_8$, where $\hat{a}_8$ is $\hat{a}_5$ without the presence of Eve.

(p.10) Bob measures either X or P of $\hat{a}_{10}$, recording both the measurement result and the corresponding time slot.

(p.11) $r = r + 1$, $s = s + 1$.

(p.12) If $r < l + m$, go to (p.6), otherwise go on.

(p.13) Alice calculates F according to the parameters r, Σ^2, and σ^2, and tells Bob the value of F through the classical channel.

(p.14) Alice tells Bob both her m measurement results and the corresponding time slots.

(p.15) Bob compares Alice's measurement results with his own during the corresponding time slots, calculating $F_{\rm cal}$.

(p.16) If $F = F_{\rm cal}$, go on to (p.17), otherwise Alice and Bob share new key block $K = \{\beta_0, \ldots, \beta_s, \ldots, \beta_{l+m-1}\}$ by quantum key distribution, then go to (p.3).

(p.17) $p = p + 1$.

(p.18) If $p < n$ go to (p.3), otherwise go on.

(p.19) End.

In quantum encryption protocol, what we concern is the mutual information $I(\alpha, \epsilon)$ between Alice and Bob, i.e. Alice's information obtained by Eve. In this paper, we only discuss the general beam splitter attack strategy. We firstly determine the probability distribution of X and P in all modes as depicted in Fig. 1, then calculate $I(\alpha, \epsilon)$ according to Shannon information theory.

Applying the displacement operator D ($\alpha = x + \mathrm{i}x$) and D ($\beta = y + \mathrm{i}y$) on $\hat{a}_1$ and $\hat{a}_2$ respectively, the modes $\hat{a}_3$ and $\hat{a}_4$ are given by the following equations,

$$X_3 = X_1 + X\,, \quad P_3 = P_1 + X\,,$$
$$X_4 = X_2 + Y\,, \quad P_4 = P_2 + Y\,. \tag{1}$$

$\hat{a}_3$ and $\hat{a}_4$ are two input modes of NOPA, while two output modes are given by the following equations,[16]

$$X_5 = X_3\cosh(r) + X_4\sinh(r)\,,$$
$$P_5 = P_3\cosh(r) - P_4\sinh(r)\,,$$
$$X_6 = X_4\cosh(r) + X_3\sinh(r)\,,$$
$$P_6 = P_4\cosh(r) - P_3\sinh(r)\,, \tag{2}$$

where $\hat{a}_5$ and $\hat{a}_6$ are entangle beams. As the squeezed parameter r increases, EPR correlation between $\hat{a}_5$ and $\hat{a}_6$ becomes increasingly prefect, and

$$F = \langle(\Delta(X_5 - k_1X_6))^2\rangle_{\min}\langle(\Delta(P_5 + k_2P_6))^2\rangle_{\min} \tag{3}$$

is close to 0, where k_1 and k_2 are parameters that can be modified to give the minimum variances of $\delta X = X_5 - k_1X_6$ and $\delta P = P_5 + k_2P_6$, respectively. When $F < 1/16$, the EPR correlation is obtained.[16]

The input modes and the output modes of beam splitter have the following relation: $\hat{a}_8 = \sqrt{\eta}\hat{a}_5 + \sqrt{1-\eta}\hat{a}_7$, $\hat{a}_9 = \sqrt{\eta}\hat{a}_7 - \sqrt{1-\eta}\hat{a}_5$. The following equations are satisfied,

$$\begin{aligned}\hat{X}_8 &= \sqrt{\eta}\hat{X}_5 + \sqrt{1-\eta}\hat{X}_7\,,\\ \hat{P}_8 &= \sqrt{\eta}\hat{P}_5 + \sqrt{1-\eta}\hat{P}_7\,,\\ \hat{X}_9 &= \sqrt{\eta}\hat{X}_7 - \sqrt{1-\eta}\hat{X}_5\,,\\ \hat{P}_9 &= \sqrt{\eta}\hat{P}_7 - \sqrt{1-\eta}\hat{P}_5\,. \end{aligned}\tag{4}$$

Applying $D(-\beta^* \sinh(r))$ on $\hat{a}_8$, Bob obtains $\hat{a}_{10}$,

$$X_{10} = X_8 - \sinh(r)Y\,, \quad P_{10} = P_8 + \sinh(r)Y\,. \tag{5}$$

Using Eqs. (1) $\sim$ (4), we can easily calculate the expressions of X_9 and P_9,

$$\begin{aligned}X_9 &= \sqrt{\eta}X_7 - \sqrt{1-\eta}[(X_1+X)\cosh(r)\\ &\quad + (X_2+Y)\sinh(r)]\,,\\ P_9 &= \sqrt{\eta}P_7 - \sqrt{1-\eta}[(P_1+X)\cosh(r)\\ &\quad - (P_2+Y)\sinh(r)]\,.\end{aligned}\tag{6}$$

The expressions of X_{10} and P_{10} are given by the following equations,

$$\begin{aligned}X_{10} &= \sqrt{\eta}[(X_1+X)\cosh(r) + (X_2+Y)\sinh(r)]\\ &\quad + \sqrt{1-\eta}X_7 - \sinh(r)Y\,,\\ P_{10} &= \sqrt{\eta}[(P_1+X)\cosh(r) - (P_2+Y)\sinh(r)]\\ &\quad + \sqrt{1-\eta}P_7 + \sinh(r)Y\,,\end{aligned}\tag{7}$$

where all random variables follow Gaussian distribution,

$$\begin{aligned}&X \sim N(0,\Sigma^2)\,, \quad Y \sim N(0,\sigma^2)\,, \quad X_i\,,\\ &P_i \sim N\Big(0,\frac{1}{4}\Big)\,,\end{aligned}\tag{8}$$

$i = 1,2,7$, i.e. all input states are the vacuum states. According to Eqs. (6) and (8), we can easily calculate the variances of X_9 and P_9,

$$\begin{aligned}\langle(\Delta X_9)^2\rangle &= (1-\eta)\cosh^2(r)\Sigma^2 + (1-\eta)\\ &\quad\times\Big[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\Big]\\ &\quad+\frac{1}{4}\eta\,,\\ \langle(\Delta P_9)^2\rangle &= (1-\eta)\cosh^2(r)\Sigma^2 + (1-\eta)\\ &\quad\times\Big[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\Big]\\ &\quad+\frac{1}{4}\eta\,.\end{aligned}\tag{9}$$

Equations (9) show that no matter whether Eve measures X_9 or P_9, the variance of signal distribution is always

$$M = (1-\eta)\cosh^2(r)\Sigma^2\,, \tag{10}$$

the variance of noise is

$$\begin{aligned}N &= (1-\eta)\Big[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\Big]\\ &\quad + \frac{1}{4}\eta\,.\end{aligned}\tag{11}$$

The signal-noise-ratio between Alice and Eve is

$$\gamma_{\alpha\epsilon} = \frac{M}{N}\,. \tag{12}$$

According to Shannon information theory,[17] the channel capacity of the additive white Gaussian noise (AWGN) channel is

$$I = \frac{1}{2}\log_2(1+\gamma)\,, \tag{13}$$

where $\gamma = \Sigma^2/\sigma^2$ is the signal-noise ratio, Σ^2 and σ^2 are the variances of the signal and noise probability distributions, respectively. If the signal follows the Gaussian distribution, and the channel is AWGN channel, then the channel capacity is the mutual information of the communication parties.

According to Eq. (13), the mutual information between Alice and Eve is

$$I\alpha\epsilon = \frac{1}{2}\log_2(1+\gamma_{\alpha\epsilon})\,. \tag{14}$$

In quantum encryption process, what we concern is the mutual information $I(\alpha,\epsilon)$, i.e., how much information Eve eavesdrops from the Alice's useful message. For example, when $r=2$, $\Sigma=10$, $\sigma=30$, $I(\alpha,\epsilon)=0.08$ bits. $I(\alpha,\epsilon)$ will quickly decrease when σ increases while other parameters keep invariant. Thus, the parameter r and σ can be properly selected to achieve the security level demanded by the consumer. For example, the security level $I(\alpha,\epsilon) = 8.5\times10^{-6}$ bits can be obtained when the parameters are selected as $r=2$, $\Sigma=10$, $\sigma=3000$. As we can see, Alice and Bob implement secure quantum communication by intentionally adding the random noise, i.e., the useful message X hides in the big random noise Y. Bob can remove the intendedly-added random noise while Eve cannot. From the above discussion, we can see that quantum encryption process is quasi-secure.

Next, we will present a method for detecting Eve. Eve inevitably disturbs the probability distribution of travel beam $\hat{a}_5$ if he wants to obtain Alice's information, thus must destroy the entanglement relation between $\hat{a}_5$ and $\hat{a}_6$. After finishing communication, Alice and Bob can detect Eve by comparing the original F with the later calculated $F_{\rm cal}$. Now, we give the explicit detecting process.

We firstly construct two random variables

$$\delta X_{\rm Eve} = X_8 - k_1X_6\,, \quad \delta P_{\rm Eve} = P_8 + k_2P_6\,. \tag{15}$$

If Eve does not exist, i.e., $\hat{a}_8 = \hat{a}_5$, then equation (15) becomes

$$\delta X_{\text{no-Eve}} = X_5 - k_1X_6\,, \quad \delta P_{\text{no-Eve}} = P_5 + k_2P_6\,. \tag{16}$$

According to Eqs. (1), (2), and (8), we can easily calculate the variances of $\delta X_{\text{no-Eve}}$ and $\delta P_{\text{no-Eve}}$,

$$\begin{aligned}\langle(\Delta(\delta X_{\text{no-Eve}}))^2\rangle &= [\cosh(r) - k_1\sinh(r)]^2\Big(\Sigma^2+\frac{1}{4}\Big)\\ &\quad + [\sinh(r) - k_1\cosh(r)]^2\Big(\sigma^2+\frac{1}{4}\Big)\,,\end{aligned}$$

$$\langle(\Delta(\delta P_{\text{no-Eve}}))^2\rangle = [\cosh(r) - k_2\sinh(r)]^2\Big(\Sigma^2 + \frac{1}{4}\Big) + [\sinh(r) - k_2\cosh(r)]^2 \times \Big(\sigma^2 + \frac{1}{4}\Big)\,, \tag{17}$$

where we assume that two input states of NOPA are vacuum states.

When

$$k_1 = k_2 = \frac{R}{S}\,, \tag{18}$$

where

$$R = 2\sinh(r)\cosh(r)(1 + 2\Sigma^2 + 2\sigma^2)\,,$$
$$S = \sinh^2(r) + \cosh^2(r) + 4\sinh^2(r)\Sigma^2 + 4\cosh^2(r)\sigma^2\,, \tag{19}$$

$\langle(\Delta(\delta X_{\text{no-Eve}}))^2\rangle$ and $\langle(\Delta(\delta P_{\text{no-Eve}}))^2\rangle$ reach the minimal values,

$$\langle(\Delta(\delta X_{\text{no-Eve}}))^2\rangle_{\min} = \langle(\Delta(\delta P_{\text{no-Eve}}))^2\rangle_{\min} = \frac{W}{Z}\,, \tag{20}$$

where

$$W = 4\Sigma^2 + 16\Sigma^2\sigma^2 + 4\sigma^2 + 1\,,$$
$$Z = 8\cosh^2(r) + 16\cosh^2(r)(\Sigma^2 + \sigma^2) - 16\Sigma^2 - 4\,. \tag{21}$$

Alice can calculate

$$F = \langle(\Delta(\delta X_{\text{no-Eve}}))^2\rangle_{\min}\langle(\Delta(\delta P_{\text{no-Eve}}))^2\rangle_{\min}\,, \tag{22}$$

when Σ^2, σ^2, and r are specified.

When Eve does exist, Bob calculates δX_{Eve} and δP_{Eve} according to Eqs. (1), (2), (4), and (15),

$$\delta X_{\text{Eve}} = [\sqrt{\eta}\cosh(r) - k_1\sinh(r)](X_1 + X) + [\sqrt{\eta}\sinh(r) - k_1\cosh(r)](X_2 + Y) + \sqrt{1-\eta}X_7\,,$$
$$\delta P_{\text{Eve}} = [\sqrt{\eta}\cosh(r) - k_2\sinh(r)](P_1 + X) + [k_2\cosh(r) - \sqrt{\eta}\sinh(r)](P_2 + Y) + \sqrt{1-\eta}P_7\,. \tag{23}$$

The variances of δX_{Eve} and δP_{Eve} can be obtained according to Eqs. (8) and (23),

$$\langle(\Delta(\delta X_{\text{Eve}}))^2\rangle = [\sqrt{\eta}\cosh(r) - k_1\sinh(r)]^2\Big(\frac{1}{4} + \Sigma^2\Big) + [\sqrt{\eta}\sinh(r) - k_1\cosh(r)]^2\Big(\frac{1}{4} + \sigma^2\Big) + \frac{1}{4}(1-\eta)\,,$$
$$\langle(\Delta(\delta P_{\text{Eve}}))^2\rangle = [\sqrt{\eta}\cosh(r) - k_2\sinh(r)]^2\Big(\frac{1}{4} + \Sigma^2\Big) + [\sqrt{\eta}\sinh(r) - k_2\cosh(r)]^2\Big(\frac{1}{4} + \sigma^2\Big) + \frac{1}{4}(1-\eta)\,. \tag{24}$$

Substituting Eq. (18) into Eqs. (24), then Bob can obtain

$$F_{\text{cal}} = \langle(\Delta(\delta X_{\text{Eve}}))^2\rangle\langle(\Delta(\delta P_{\text{Eve}}))^2\rangle\,. \tag{25}$$

Thus after finishing communication, Bob can estimate F_{cal} according to both the statistics he accumulates and what Alice tells him. If $F_{\text{cal}} = F$, Eve does not exist. If $F_{\text{cal}} > F$, Eve exists. As we can see, Alice and Bob can detect whether Eve exists or not by the entanglement parameter F.

In conclusion, a quantum encryption protocol based on Gaussian-modulated continuous variable EPR entanglement correlations is proposed. By adding the key-controlled noise into the signal, Alice and Bob can implement the quasi secure direct communication, the security level can be obtained by adding the proper noise. The beam splitter attack strategy is analyzed in details by employing Shannon information theory. The entanglement parameter F serves as the method of detecting Eve.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74** (2002) 145, and references therein.

[2] H.K. Lo and H.F. Chau, Nature (London) **283** (1999) 2050.

[3] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85** (2000) 441.

[4] D. Mayers, J. Association for Computing Machinery **48** (2001) 351.

[5] T.C. Ralph, Phys. Rev. A **61** (1999) 010303.

[6] M. Hilery, Phys. Rev. A **61** (2000) 022309.

[7] D. Gottesman and J. Preskill, Phys. Rev. A **63** (2001) 022309.

[8] N.J. Cerf, M. Lévy, and G.V. Assche, Phys. Rev. A **63** (2001) 052311.

[9] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88** (2002) 057902.

[10] Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88** (2002) 167902.

[11] F. Grosshans, *et al.*, Nature (London) **421** (2003) 238.

[12] K. Boström and T. Felbinger, Phys. Rev. Lett. **89** (2002) 187902.

[13] A. Wójcik, Phys. Rew. Lett. **90** (2003) 157901; Q.Y. Cai, Phys. Rev. Lett. **91** (2003) 109801.

[14] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94** (2005) 140501.

[15] M.D. Reid, Phys. Rev. A **62** (2000) 062308.

[16] M.D. Reid, Phys. Rev. A **40** (1989) 913; M.D. Reid and P.D. Drummond, Phys. Rev. Lett. **60** (1989) 2731.

[17] C.E. Shannon, Bell. Syst. Tech. J. **27** (1948) 623.