

Quantum communication exploiting above threshold OPO intensity correlations and polarization encoding

A. Porzio^{a,*}, V. D'Auria^{a,b}, P. Aniello^{b,c}, M.G.A. Paris^d, S. Solimeno^{a,b}

^a*Coherentia—INFN unità di Napoli, Italy*

^b*Dipartimento di Scienze Fisiche, Università "Federico II", Italy*

^c*INFN sez. Napoli Complesso Universitario di Monte Sant'Angelo, via Cintia, 80126 Napoli, Italy*

^d*INFN and Dipartimento di Fisica, Università degli studi di Milano, Italia, via Celoria 16 I-20133, Milano, Italy*

Available online 26 July 2006

Abstract

We present a continuous variable quantum communication protocol based on bright continuous-wave twin-beams generated by a type-II OPO. Intensity correlation between the beams is used in conjunction with a binary randomization of polarization to guarantee security and reveal eavesdropping actions. The scheme presented is asymmetric. Bob (the receiver) retains one of the beams and sends the other one to Alice after a random rotation of its polarization. The cryptographic key elements are encoded through amplitude modulation by Alice, who sends back her beam to Bob after a second rotation of the polarization. Eventually, the beams are detected by Bob after a further random polarization rotation. The security of the system and the possibility of revealing the eavesdropping action in the case of an individual attack are demonstrated by evaluating the bit error rates.

© 2006 Elsevier Ltd. All rights reserved.

Keywords: Quantum communication; Twin-beams; Optical parametric oscillator

1. Introduction

In recent years there has been an increasing interest in exploiting typical features of quantum mechanical systems in order to implement communication schemes showing a high level of security. Such secure schemes can be employed for implementing a quantum key distribution (QKD) protocol: a way for safely sharing a secret key between two distant parties (say, Alice and Bob) [1,2].

Since the first proposal of Bennett and Brassard [3], there has been an increasing number of experimental realizations of QKD with discrete variables, essentially based upon single photon systems [2]. In these systems the information is randomly encoded on a couple of non-commuting variables. By this strategy, one obtains that any *eavesdropper* (say, Eve) is forced to *guess* which observable has to be measured. Eve is likely to make the wrong guess half of the times, thus revealing her presence to Alice and Bob through back-action.

QKD concepts have been extended to continuous variable (CV) systems [4,5]. It has been argued that a general CV secure quantum communication protocol should be discussed in terms of the bit error rate (BER). In particular, the quantum mechanical limits to the minimum extra-disturbance that Alice and Bob are able to detect on their data have been established. It has also been shown that entanglement is a precondition for realizing secure communication schemes [6].

EPR CV beams—i.e. twin-beam—have already been employed in two quantum communication experiments [7,8]. The Caltech group [7] has shown that EPR CV correlations improve the signal-to-noise ratio (SNR) in transmitting a coherent message. A simplified version of this scheme [8] uses a single EPR beam traveling between Alice and Bob.

More recently, it has been shown that it is possible to realize QKD by using coherent beams [9–11]. In these schemes, two random Gaussian variables are encoded in two non-commuting observables by means of both phase and amplitude modulation.

In all the above-mentioned CV schemes the measurements at the receiver are implemented by homodyne

*Corresponding author. Tel.: +39 081 676188; fax: +39 081 676346.

E-mail address: alberto.porzio@na.infn.it (A. Porzio).

detectors, requiring the remote control of the local oscillator (LO) phase, or the transmission of both the LO and the carrier beams.

In addition to these experiments, there have been some further proposals for CV QKD [12–14]. The scheme of Ref. [12] is based on simultaneous homodyne detection at the two stations, whereas the very recent proposal [13] avoids homodyne detection and exploits quantum dense coding on EPR beams [15], together with the possibility of changing EPR correlation in an OPA working randomly either as an amplifier or a de-amplifier. In Ref. [14], a scheme employing the photon number correlation in a seeded OPA is discussed. This scheme exploits both polarization entanglement and photon number correlation of the down-converted pulses, with the difference in the signal and idler photons used for coding. A photodiode with a high dynamical range is needed at the receiver, in order to discriminate a relative difference in the photon number of the order of 10^{-3} to -10^{-4} . The latter scheme has been recently object of a preliminary feasibility experiment [16].

In the present paper, we propose a CV communication protocol whose security relies on quantum correlations between continuous-wave (CW) twin-beam generated in an above threshold type-II OPO [17–20]. The main features of this scheme are:

- (1) intrinsically asymmetric with the receiver ruling the transmission;
- (2) direct detection, which avoids drawbacks of homodyne detectors;
- (3) a single beam travels back and forth Alice–Bob;
- (4) data encoded by sub-shot-noise amplitude modulation, and protected by random polarization rotations.

The proposed scheme can be regarded as a base for a QKD protocol. Its nature will be discussed in terms of transmission BER and the possibility of revealing interceptions will be evaluated for the single attack scheme.

2. Quantum communication using bright twin beams

The present CV protocol is schematically depicted in Fig. 1. Before the transmission starts the two communicating parties agree on a public channel on modulation/demodulation frequency Ω and fix the bit duration time (referred to in the follows as “time slot”).

Bob (receiver) generates a twin-beams by a type-II OPO and spatially separates the two orthogonally polarized components (“signal” and “idler”) by a polarizing beam-splitter (PBS₁). One of the beams (f.i. the idler) is retained by Bob while the other one travels back and forth the two parties. Once the beams are separated Bob rotates the signal polarization by an angle ϕ randomly chosen and sends it to Alice.

On her side Alice (sender) encodes each bit as follows. For every time slot she decides to apply or not an

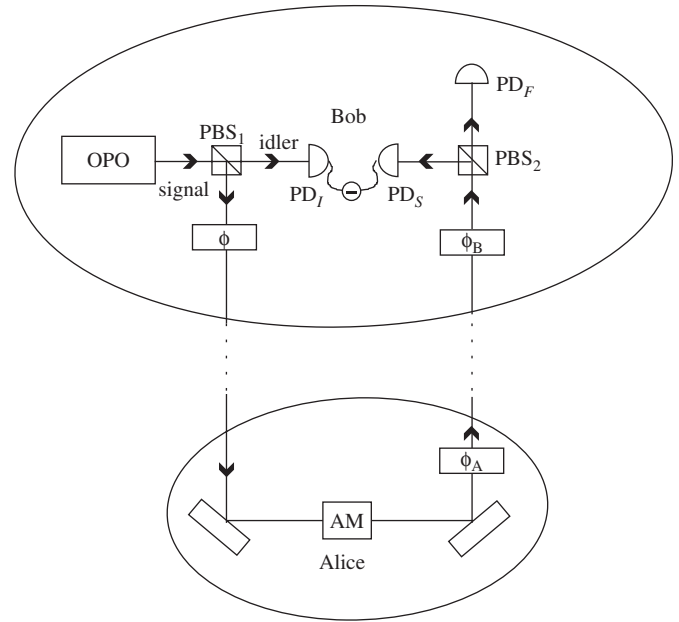


Fig. 1. Schematic of the quantum cryptographic protocol. Bob generates CW twin-beam and sends one of them to Alice's station where the key bits are encoded by means of amplitude modulation. The beam travels back to Bob where intensity difference measurements are implemented. The random polarization changes, indicated by the angles ϕ , ϕ_A , and ϕ_B , are used to protect data.

amplitude modulation, at frequency Ω , to the signal (say: bit 1 \Leftrightarrow modulation “on”, bit 0 \Leftrightarrow modulation “off”). She tunes the modulation depth so as to hide its effects below the shot-noise-level (SNL). At the end, Alice changes once again the beam polarization by choosing at random between 0 and $\pi/2$. Eventually, the beam carrying the bit value, is sent back toward the receiver station.

Bob recovers the bit value by detecting simultaneously the signal + idler beams and exploiting their quantum correlation. As a first step he rotates randomly the polarization ($\phi_B = -\phi$ or $\phi_B = \pi/2 - \phi$). Next, if the total polarization change $\phi + \phi_A + \phi_B$ is equal to 0 or π , the signal impinging on PBS₂ is totally reflected toward the photodiode (PD_S) and the paired beams are detected and the bit recovered from the difference photocurrent. On the contrary, if $\phi + \phi_A + \phi_B = \pi/2$ the signal is transmitted toward PD_F which measures a non-zero mean photocurrent. In the latter case, occurring on average half of the times, Bob marks the corresponding time slot as no-data.

Notice that in virtue of the EPR correlation the SNR of the signal-idler difference is better than that of the signal alone. On the other side, the polarization procedure randomizes the QKD protocol. In this way both the sender and the receiver do not know “a priori” if the bit sent (received) in a particular time slot would be or not part of the final bit array.

Once Alice has sent N bits to Bob, they need to distill the final array. To do this, using a public channel, Bob reveals to Alice, for each time slot, the value of the angle $\phi_B + \phi$. Alice, knowing ϕ_A , compute $\phi + \phi_B + \phi_A$ and discard the

Table 1

Bit table for different combinations of polarization random rotation and modulation

ϕ_A	$\phi + \phi_B$	Modulation	Bit value
0	0	On	1
0	0	Off	0
0	$\pi/2$	On	No-data
0	$\pi/2$	Off	No-data
$\pi/2$	0	On	No-data
$\pi/2$	0	Off	No-data
$\pi/2$	$\pi/2$	On	1
$\pi/2$	$\pi/2$	Off	0

Half of the times Bob and Alice will discard their data.

data labeled as no-data on Bob's side. On average, they will get a secure key element every two transmitted bits.

The randomization of polarization, which embeds the actual key in a larger array, forces any unauthorized receiver to make a guess. In this way the bare security of the quantum channel is enhanced. The choice of a binary polarization randomization is not mandatory. Indeed, the system works in an analogue way for an M -ary randomization of the polarization. In this case the security is further increased, at the price of a reduced transmission rate. In Table 1 we report the different possible combination of random polarization changes and modulation that would form the actual key.

At the end of the transmission reconciliation privacy amplification can be performed in a standard way [21].

3. BER analysis

The quality of a digital link can be evaluated in terms of bit error rate (BER), i.e. the ratio of the wrong bits to all the transmitted ones, related to the SNR [22] by

$$\text{BER} = \frac{1}{2} \left[1 - \text{Erf} \left(\frac{1}{2} \sqrt{\frac{1}{2} \text{SNR}} \right) \right], \quad (1)$$

where Erf denotes the error function. For a classical carrier beam the lower limit for the noise is the SNL. On the other hand, CW twin-beams exhibit intensity correlation [23,24], mirrored in a spectral density difference lying below the SNL with a Lorentzian profile, a rather good noise suppression at zero frequency and width related to the cavity bandwidth. On the contrary, each single beam, for moderate pump power, resembles a coherent one accompanied by its own SNL.

In order to evaluate the BER associated to the present communication scheme we use the following simple model for the modulation. Let E be a classic monochromatic beam oscillating at frequency ω_0 with amplitude A modulated at frequency Ω . E can be decomposed in a sum of monochromatic components each oscillating at frequency $\omega_0 + k\Omega$ ($k \in \mathcal{Z}$) with amplitude $A i^k J_k(m)$, m modulation depth and $J_k(m)$ the Bessel function of order k .

If m is small enough, the sum reduces to $k = 0, \pm 1$ (fundamental + two sidebands). In the frequency domain, the field is represented by a Lorentzian at $\omega = \omega_0$ of height $|A|^2$ and side bands at $\omega = \omega_0 \pm \Omega$ of height $|A|^2 m^2$. The Alice–Bob interaction is described by the following spectral densities:

- (1) S_{IA} spectrum of the signal leaving Bob's station;
- (2) $S_{IA}^{(m)}$ spectrum modified by Alice;
- (3) S_{dB} difference spectrum measured by Bob;
- (4) $S_{dB}^{(m)}$ difference spectrum in presence of modulation.

$S_{IA}^{(m)}$ and S_{IA} are related by

$$S_{IA}^{(m)}(\omega) = C_0^2 S_{IA}(\omega) + C_1^2 [S_{IA}(\omega - \Omega) + \mathcal{L}(\omega - \Omega)], \quad (2)$$

with

$$C_0 \simeq |1 - \varepsilon J_0(m)|^2, \quad C_1 \simeq |\varepsilon J_1(m)|^2,$$

where ε ($\ll 1$) takes into account the modulation process, and \mathcal{L} is a Lorentzian of unitary height. $C_0^2 S_{IA}$ represents the SN contribution while $C_1^2 (S_{IA} + \mathcal{L})$ stands for the modulation term. For $m \ll 1$, the classical sideband $C_1^2 \mathcal{L}(0)$ at Ω is partially overshadowed by the SN ($C_0^2 S_{IA}(\Omega) \gtrsim C_1^2 \mathcal{L}(0)$). Since $S_{IA}(0) \ll \mathcal{L}(0)$ and $C_1^2 \ll C_0^2$, hence $C_1^2 S_{IA}(\omega - \Omega)$ can be neglected.

On Bob's side the intensity difference spectrum reads

$$S_{dB}(\omega) = S_{dB}^{(m)}(\omega) + C_1^2 [S_{IA}(\omega - \Omega) + \mathcal{L}(\omega - \Omega)] \quad (3)$$

with $S_{dB}^{(m)}$ the intensity difference spectrum modified by the modulation. For $m = 0$ (modulation off) $S_{dB}^{(0)}$ is that given by OPO output. The modulation slightly reduces the intensity and so does the correlation, thus transforming $S_{dB}^{(0)}$ into $S_{dB}^{(m)}$.

The correlation makes the modulation side-bands more evident being $S_{dB}^{(m)}(\Omega)$ sensibly smaller than $C_0^2 S_{IA}(\Omega)$.

In the following, we report plots of the spectra in Eqs. (2), (3) obtained by using for S_{IA} and S_{dB} the expressions reported in Ref. [24], and assuming 5.2 dB of intensity correlation at 5 MHz (as in [19]), with Ω set to 5 MHz ($\approx \frac{1}{3}$ of the squeezing bandwidth).

The modulation depth m must be chosen in such a way to guarantee a low BER on Bob's intensity difference measurements and, at the same time, a high BER on data obtained by single beam detection (which corresponds to an intrusion in the communication channel, see below). In Fig. 2 we compare the BERs for single and difference detection versus m . In both cases BER decreases for increasing m . The intensity difference BER is always lower than single one; e.g., for $m = 0.052$, we have on single detection a BER of 22.5%, while on difference it is $\approx 1\%$. The dashed curves lying close to the intensity difference BER correspond to a variation of ± 1 dB of the squeezing. As it can be seen such a variation does not change dramatically the BER behavior.

The randomization of polarization allows Bob and Alice to embed their secret key in one half of the data array, which unauthorized parties cannot discriminate from the

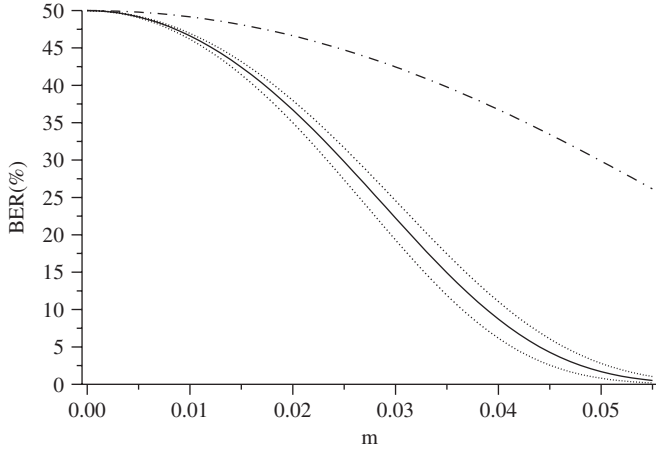


Fig. 2. Bit error rate (BER) versus modulation depth m in intensity difference measurements (lower curve) and single beam detection (upper dashed curve) at Bob's station. Thanks to the twin-beam intensity correlation, the BER is clearly lower in the case of balanced detection, due to the enhancement of the SNR. All the reported plots are calculated assuming a pump power $P = 1.7 \times P_{th}$, modulation frequency Ω one-third the cavity bandwidth, and a noise reduction of 5.2 dB. The dotted curves represent a noise reduction variation of ± 1 dB. The expressions used in the simulations are reported in Ref. [24].

full array. This procedure is necessary in view of the application of this quantum communication scheme to a QKD protocol.

Bob and Alice can get aware of an Eve's intrusion by checking their BER. Local attacks after Alice modulation with Eve to having a perfect detection system (unitary quantum efficiency, no added noise) are modeled as the insertion of a beam splitter (BS) and a subsequent photodetection of the reflected mode. In practice, Eve may use a BS to catch a fraction of the modulated beam while this is sent back to Bob. Then, she observes intensity fluctuation around Ω and tries to reveal the modulation. Assuming a delta correlated vacuum field $\langle v(t)v^\dagger(t') \rangle = \delta(t-t')$ at the second port of the BS, the fluctuation spectra for the transmitted (C) and the reflected (D) beams are affected by an additional shot noise contribution. Applying BS input–output relations one obtains:

$$\begin{aligned} S_{IC}(\omega) &= t^4 S_{IA}(\omega) + (rt)^2 \langle I_A \rangle, \\ S_{ID}(\omega) &= r^4 S_{IA}(\omega) + (rt)^2 \langle I_A \rangle, \end{aligned} \quad (4)$$

where $t(r)$ ($t^2 + r^2 = 1$) is the transmission (reflection) coefficient of the BS, A is the signal mode and $\langle \dots \rangle$ indicates the mean value. Eve measures the following fluctuation spectrum (see Eq. (2))

$$\begin{aligned} S_{IE}(\omega) &= S_{IA}(\omega) C_0^2 r^4 + r^4 C_1^2 \cdot S_{IA}(\omega - \Omega) \\ &\quad + (tr)^2 (C_0 + C_1) \langle I_A \rangle + \mathcal{L}(\omega - \Omega) C_1^2 r^4, \end{aligned} \quad (5)$$

while, because of Eve's action, Bob observes the difference spectrum

$$\begin{aligned} S'_{dB}(\omega) &= S_{dB}(\omega) + t^4 C_1^2 S_{IA}(\omega - \Omega) \\ &\quad + (tr)^2 (C_0 + C_1) \langle I_A \rangle + \mathcal{L}(\omega - \Omega) \cdot t^4 C_1^2, \end{aligned} \quad (6)$$

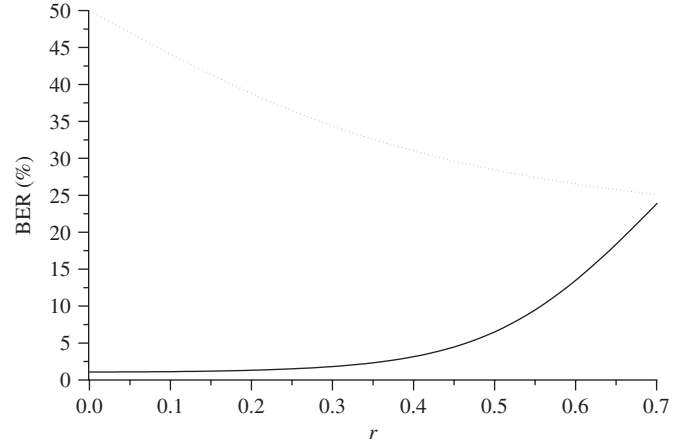


Fig. 3. Bit error rate of Bob (lower curve) and Eve (upper dotted curve) versus BS reflectivity r for interception attacks. Up to $r = 0.4$, corresponding to an interception of 16% of the beam power, Bob's BER increases very slowly while Eve obtains a BER of $\approx 31\%$. For higher r , BER on Eve side decreases while Bob would be able to detect Eve attack because of the increasing of the BER on his data.

where S_{dB} takes into account the losses due to Eve's intrusion and the subsequent reduction in the intensity correlation.

In Fig. 3, the BER for both Bob and Eve is plotted versus BS reflection coefficients r . Eve reveals herself by increasing the BER on Bob side as a consequence of the signal decrease and the increase of the effective noise around Ω . The lower limit for Eve's BER is obtained when the whole beam is caught; it corresponds to the single beam BER given above (22.5% for $m = 0.52$). For $r \leq 0.4$ (i.e. 16% of power reflection) Bob's BER increases to 3% and therefore it is not immediate for him to reveal Eve's attack. However, at the same time, Eve's BER reaches 31%, thus making the attack unsuccessful. For higher r , correlation critically deteriorates and Bob's BER rapidly increases, making easy to detect any eavesdropping action. In summary, for any value of the splitting ratio, Eve's single attack strategy is either useless or easily detected.

For an eavesdropper with unlimited resources an additional scenario should be considered, namely the possibility that Eve can perform a beamsplitting insertion whose splitting ratio is tuned for matching the channel loss. Then, she could replace the (lossy) line by an ideal channel, thus hiding her attack. In this case, it is very difficult for Alice and Bob to reveal eavesdropping, while security of the transmission is still assured, thanks to the high Eve's BER and to the polarization encoding, which, in this case, plays a major role.

Since the bits are encoded by applying or not a modulation to one of the beams, it is important to discuss Eve's catch-and-resend strategy [2]. This consists of the possibility for Eve to catch the whole beam and, after a suitably informative measurement, to resend the information she gets on a different optimal carrier. In such a case our scheme is secure because of its asymmetry. In fact, Eve

has at her disposal only one single party of the entangled twin-beam, and therefore, thanks to the quantum correlation, any measurement performed by Eve will affect the state of the whole system. In turn, this implies that any action by Eve reduces the correlations between the beams [25,26] so increasing the probability of being detected.

4. Conclusions

In conclusion, a quantum communication scheme based on non-classical correlations between intensity and polarization of CW twin-beams generated in a type-II OPO has been presented.

The transmission is ruled by the receiver (Bob) who retains one of the beams and sends the other to Alice. The bits are encoded by amplitude modulation with a very small depth, so that the modulation sidebands remain hidden in the quantum noise of the beam. The security of the system and the possibility of revealing an eavesdropping interception have been discussed by evaluating the BER of the receiver and of an eavesdropper with unlimited resources. The asymmetry of the scheme guarantees that the catch-and-resend strategy is ineffective. The scheme has been discussed as the base for a possible QKD protocol. In such a case a random variable, namely the beam polarization, can be introduced to increase the channel security.

Acknowledgment

MGAP is research fellow at *Collegio Alessandro Volta*. Shortly after this paper was submitted a new paper appeared on a preprint archiv [27] where a single-photon QKD protocol based on random rotations of the photon polarization is discussed.

References

- [1] Phoenix SJD, Townsend PD. Quantum cryptography: how to beat the code breakers using quantum mechanics. *Cont Phys* 1995;36:165–95.
- [2] See for example: Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Rev Mod Phys* 2002;74:145–95, and reference therein.
- [3] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of IEEE international conference on computers systems and signal processing*, Bangalore, India, December 1984. New York: IEEE; 1984. p. 175–9.
- [4] Ralph TC. Continuous variable quantum cryptography. *Phys Rev A* 1999;61:010303/1–4.
- [5] Ralph TC. Security of continuous variable quantum cryptography. *Phys Rev A* 2000;62:062306/1–7.
- [6] Curty M, Lewenstein M, Lütkenhaus N. Entanglement as a precondition for secure quantum key distribution. *Phys Rev Lett* 2004;92:217903/1–4.
- [7] Pereira SF, Ou ZY, Kimble HJ. Quantum communication with correlated nonclassical states. *Phys Rev A* 2000;62:042311/1–8.
- [8] Jing J, Pan Q, Xie C, Peng K. Quantum cryptography using Einstein–Podolsky–Rosen correlations of continuous variables. *arXiv* 2002; quant-ph/0204111.
- [9] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. *Phys Rev Lett* 2002;88:057902/1–4.
- [10] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. *Nature* 2003;421:238–41.
- [11] Weedbrock C, Lance AM, Bowen WP, Symul T, Ralph TC, Lam PK. Quantum cryptography without switching. *Phys Rev Lett* 2004;93:170504/1–4.
- [12] Silberhorn C, Korolkova N, Leuchs G. Quantum key distribution with bright entangled beams. *Phys Rev Lett* 2002;88:167902/1–4.
- [13] Zhang J, Xie CD, Peng KC. Quantum key distribution for continuous variable by means of phase-sensitive nondegenerate optical parametric amplifier. *Europhys Lett* 2003;61:579–85.
- [14] Funk AC, Raymer MG. Quantum key distribution using nonclassical photon-number correlations in macroscopic light pulses. *Phys Rev A* 2002;65:042307/1–5.
- [15] Li X, Pan Q, Jing J, Zhang J, Xie C, Peng K. Quantum dense coding exploiting a bright Einstein–Podolsky–Rosen beam. *Phys Rev Lett* 2002;88:047904/1–4.
- [16] Zhang Y, Kasai K, Hayasaka K. Quantum channel using photon number correlated twin beams. *Opt Expr* 2003;11:3592–7.
- [17] Heidmann A, Horowicz RJ, Reynaud S, Giacobino E, Fabre C, Camy G. Observation of quantum noise reduction on twin laser beams. *Phys Rev Lett* 1987;59:2555–7.
- [18] Teja J, Wong NC. Twin-beam generation in a triply resonant dual-cavity optical parametric oscillator. *Opt Expr* 1998;2:65–71.
- [19] Porzio A, Sciarrino F, Chiummo A, Fiorentino M, Solimeno S. Twin beams correlation and single beam noise for triply resonant KTP OPOs. *Opt Commun* 2001;194:373–9.
- [20] Porzio A, Chiummo A, Sciarrino F, Solimeno S. A theoretical and experimental study of fluctuations of the optical parametric oscillator. *Opt Lasers Eng* 2002;37:585–99.
- [21] Bennett CH, Brassard G, Crepeau C, Maurer UM. Generalized privacy amplification. *IEEE Trans Inform Theory* 1995;41:1915–23.
- [22] Yariv A. *Optical electronics in modern communications*, 5th ed. Oxford: Oxford University Press; 1997.
- [23] Fabre C, Giacobino E, Heidmann A, Reynaud S. Noise characteristics of a nondegenerate optical parametric oscillator-application to quantum noise reduction. *J Phys France* 1989;50:1209–25.
- [24] Porzio A, Altucci C, Aniello P, De Lisio C, Solimeno S. Resonances and spectral properties of detuned OPOs pumped by fluctuating sources. *Appl Phys B* 2002;75:655–65.
- [25] Laurat J, Coudreau T, Treps N, Maître A, Fabre C. Conditional preparation of a quantum state in the continuous variable regime: generation of a sub-Poissonian state from twin beams. *Phys Rev Lett* 2003;91:213601/1–4.
- [26] Paris MGA, Cola M, Bonifacio R. Quantum-state engineering assisted by entanglement. *Phys Rev A* 2003;67:042104/1–10.
- [27] Kye W-H, Kim C-M, Kim MS, Park Y-J. Quantum key distribution with blind polarization bases. *arXiv* 2005; quant-ph/0501014.