

EUROPHYSICS LETTERS

OFFPRINT

Vol. 61 • Number 5 • pp. 579–585

**Quantum key distribution for continuous variable
by means of phase-sensitive nondegenerate
optical parametric amplifier**

* * *

J. ZHANG, C. D. XIE and K. C. PENG



Published under the scientific responsibility of the
EUROPEAN PHYSICAL SOCIETY
Incorporating
JOURNAL DE PHYSIQUE LETTRES • LETTERE AL NUOVO CIMENTO



EUROPHYSICS LETTERS

Editor-in-Chief

Prof. H. Müller-Krumbhaar
IFF Theorie 3 - Forschungszentrum Jülich
D-52425 Jülich - Germany
h.mueller-krumbhaar@fz-juelich.de

Taking full advantage of the service on Internet,
please choose the fastest connection:

<http://www.edpsciences.org>
<http://edpsciences.nao.ac.jp>
<http://edpsciences-usa.org>
<http://www.epletters.ch>

Staff Editor: Edith Thomas

Europhysics Letters, 27 chemin de la Vendée, P.O. Box 69, CH-1213 Petit-Lancy 2, Switzerland

Editorial Director: Angela Oleandri

Director of publication: Jean-Marc Quilbé

Publishers: EDP Sciences S.A., France - Società Italiana di Fisica, Italy

Europhysics Letter was launched more than fifteen years ago by the European Physical Society, the Société Française de Physique, the Società Italiana di Fisica and the Institute of Physics (UK) and owned now by 17 National Physical Societies/Institutes.

Europhysics Letters aims to publish short papers containing non-trivial new results, ideas, concepts, experimental methods, theoretical treatments, etc. which are of broad interest and importance to one or several sections of the physics community.

Europhysics letters provides a platform for scientists from all over the world to offer their results to an international readership.

Subscription 2003

24 issues - Vol. 61-64 (6 issues per vol.)

ISSN: 0295-5075 - ISSN electronic: 1286-4854

- France & EU (VAT included) 1 568 €
- Rest of the World (without VAT) 1 568 €

Payment:

- Check enclosed payable to EDP Sciences
- Please send me a proforma invoice
- Credit card:
- Visa Eurocard American Express

Valid until:

Card No:

- Please send me a **free** sample copy

Institution/Library:

.....

Name:

Position:

Address:

.....

.....

ZIP-Code:

City:

Country:

E-mail:

Signature :

Order through your subscription agency or directly to EDP Sciences:

17 av. du Hoggar • B.P. 112 • 91944 Les Ulis Cedex A • France
Tel. 33 (0)1 69 18 75 75 • Fax 33 (0)1 69 86 06 78 • subscribers@edpsciences.org

Quantum key distribution for continuous variable by means of phase-sensitive nondegenerate optical parametric amplifier

J. ZHANG(*), C. D. XIE and K. C. PENG

*The State Key Laboratory of Quantum Optics and Quantum Optics Devices
Institute of Opto-Electronics, Shanxi University - Taiyuan 030006, PRC*

(received 6 May 2002; accepted in final form 12 December 2002)

PACS. 03.67.Hk – Quantum communication.

PACS. 03.65.Ta – Foundations of quantum mechanics; measurement theory.

Abstract. – A new protocol realizing quantum key distribution for continuous variables is proposed, in which the bright entangled EPR beams are produced from a phase-sensitive nondegenerate optical parametric amplifier. Based on randomly changing the operating states of NOPA at the sending station and randomly choosing the phase difference between two modes of EPR beams at the receiving station, the secret key string is established. The application of direct detection system of photocurrents makes the proposed scheme relatively easier to be experimentally demonstrated.

Quantum cryptography —or, more precisely, quantum key distribution (QKD)— is a technique according to which the distribution of random number keys in two remote parties for cryptographic purposes can be made secure by using the fundamental properties of quantum mechanics to ensure that any interception of the key information can be detected [1–3]. It was firstly discussed in protocols of discrete variable systems and then was experimentally carried out using single photons as fundamental quantum systems. Although the quantum cryptography with discrete variables has the advantage of insensitivity to transmission losses, some disadvantages mainly associated with the lack of efficient single-photon sources and the poor efficiency of photon-counting detectors limit its practical applications. Recently, new development on quantum cryptography using nonclassical light fields as the carriers of information has significantly increased the interests in the continuous variable systems [4–9]. The keys may be extracted from binary modulated EPR beam [4, 6] or from correlated measurement sequences [7, 8]. Hillery proposed a QKD scheme based on binary modulated squeezed light [10]. Cerf *et al.* showed that Hillery’s scheme may be improved if using Gaussian modulation [11, 12] instead of binary one and then proposed a reconciliation protocol [12] to implement this improved protocol. The continuous variable QKD based on error-correcting codes and coherent state has been suggested by Gottesmann *et al.* [13] and Grosshans *et al.* based on [14] recently. The EPR quantum correlated light fields have been experimentally produced with optical

(*) E-mail: jzhang74@yahoo.com

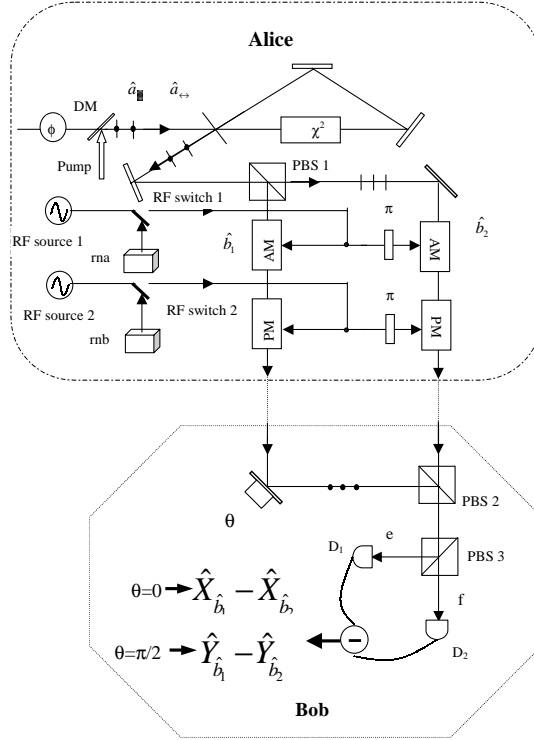


Fig. 1 – The schematic for quantum key distribution. DM, dichroic mirror. rna and rnb are independent random number sources. PBSs are polarizing beam splitter.

parametric amplifiers (OPAs) and applied successfully in the experimental investigations of the quantum teleportation and the dense coding for continuous variables [15–18]. In this paper a new QKD scheme based on bright EPR beam generated from a phase-sensitive NOPA exchangeably operated in the states of amplification and deamplification. The binary key string is modulated directly on EPR beams. Security is provided by the uncertainty principle of quantum mechanics which protects from simultaneously measuring both noncommuting quadrature phase amplitude with an arbitrary accuracy. In this proposed system, the quadrature phase amplitude of light fields is directly detected, thus local oscillators for the balanced homodyne detection are not needed. This feature simplifies the measurement systems and may improve the detection efficiency significantly.

The schematic diagram of the QKD system is shown in fig. 1. A ring NOPA including a type-II nonlinear crystal (χ^2) serves as the EPR source. Two coherent input signals a_{\uparrow} and a_{\leftrightarrow} with same frequency ω_0 and orthogonal polarizations are injected into the NOPA. For simplification and without losing generality, we assume that the polarizations of the injected signal and idler fields are oriented along the vertical and horizontal directions, and their intensities and original phases before NOPA are considered to be identical. The amplifier is pumped with the second harmonic wave of $\omega_p = 2\omega_0$ and the amplitude $a_p \gg a_{\uparrow}, a_{\leftrightarrow}$; in this case the pump field may be considered as a classical field without depletion during the amplification process. The output signal and idler fields polarized along the vertical and horizontal directions are denoted with b_{\uparrow} and b_{\leftrightarrow} . The input-output Heisenberg evolutions

of the field modes of the NOPA are given by [19]

$$\begin{aligned}\widehat{b}_{0\uparrow} &= \mu\widehat{a}_{0\uparrow} + \nu\widehat{a}_{0\leftarrow}^\dagger, & \widehat{b}_{0\leftarrow} &= \mu\widehat{a}_{0\leftarrow} + \nu\widehat{a}_{0\uparrow}^\dagger, \\ \widehat{b}_{+\uparrow} &= \mu\widehat{a}_{+\uparrow} + \nu\widehat{a}_{+\leftarrow}^\dagger, & \widehat{b}_{+\leftarrow} &= \mu\widehat{a}_{+\leftarrow} + \nu\widehat{a}_{+\uparrow}^\dagger, \\ \widehat{b}_{-\uparrow} &= \mu\widehat{a}_{-\uparrow} + \nu\widehat{a}_{-\leftarrow}^\dagger, & \widehat{b}_{-\leftarrow} &= \mu\widehat{a}_{-\leftarrow} + \nu\widehat{a}_{-\uparrow}^\dagger,\end{aligned}\quad (1)$$

where \widehat{a} , \widehat{a}^\dagger and \widehat{b} , \widehat{b}^\dagger denote the annihilation and creation operators of the input and the output modes. The subindex 0 and \pm stand for the central mode at frequency ω_0 and the sidebands at frequency $\omega_0 \pm \Omega$, respectively. The parameters $\mu = \cosh r$ and $\nu = e^{i\theta_p} \sinh r$ are functions of the squeezing factor r ($r \propto L\chi^2|a_p|$, L is the nonlinear crystal length, χ^2 is the effective second-order susceptibility of the nonlinear crystal in NOPA, a_p is the amplitude of the pump field) and the phase θ_p of the pump field. In the following calculation the phase θ_p is set to zero as the reference of relative phases of all other light fields. For bright optical field, the quadratures of the output orthogonal polarization modes at a certain rotated phase θ are expressed by

$$\begin{aligned}\widehat{X}_{\widehat{b}_{\uparrow}}(\theta) &= \frac{b_{0\uparrow}^* \widehat{b}_{+\uparrow} e^{-i\theta} + b_{0\uparrow} \widehat{b}_{-\uparrow}^\dagger e^{i\theta}}{|b_{0\uparrow}|} \\ &= \widehat{b}_{+\uparrow} e^{-i(\theta+\varphi)} + \widehat{b}_{-\uparrow}^\dagger e^{i(\theta+\varphi)}, \\ \widehat{X}_{\widehat{b}_{\leftarrow}}(\theta) &= \widehat{b}_{+\leftarrow} e^{-i(\theta+\varphi)} + \widehat{b}_{-\leftarrow}^\dagger e^{i(\theta+\varphi)},\end{aligned}\quad (2)$$

where $\varphi = \arg(b_{0\uparrow}) = \arg(b_{0\leftarrow}) = \arg(e^{i\Phi} + e^{-i\Phi} \tanh r)$ is the phase of the modes $\widehat{b}_{0\uparrow}$, $\widehat{b}_{0\leftarrow}$ relative to θ_p and Φ is the phase of the modes $\widehat{a}_{0\uparrow}$, $\widehat{a}_{0\leftarrow}$ relative to θ_p . Taking $\theta = 0$ and $\theta = \pi/2$ in eq. (2), the amplitude and phase quadrature of the output field are obtained:

$$\begin{aligned}\widehat{X}_{\widehat{b}_{\uparrow}} &= \widehat{X}_{\widehat{b}_{\uparrow}}(0) = \widehat{b}_{+\uparrow} e^{-i\varphi} + \widehat{b}_{-\uparrow}^\dagger e^{i\varphi}, \\ \widehat{X}_{\widehat{b}_{\leftarrow}} &= \widehat{X}_{\widehat{b}_{\leftarrow}}(0) = \widehat{b}_{+\leftarrow} e^{-i\varphi} + \widehat{b}_{-\leftarrow}^\dagger e^{i\varphi}, \\ \widehat{Y}_{\widehat{b}_{\uparrow}} &= \widehat{X}_{\widehat{b}_{\uparrow}}\left(\frac{\pi}{2}\right) = -i\left(\widehat{b}_{+\uparrow} e^{-i\varphi} - \widehat{b}_{-\uparrow}^\dagger e^{i\varphi}\right), \\ \widehat{Y}_{\widehat{b}_{\leftarrow}} &= \widehat{X}_{\widehat{b}_{\leftarrow}}\left(\frac{\pi}{2}\right) = -i\left(\widehat{b}_{+\leftarrow} e^{-i\varphi} - \widehat{b}_{-\leftarrow}^\dagger e^{i\varphi}\right).\end{aligned}\quad (3)$$

When the injected subharmonic signal and harmonic pump field are in phase ($\Phi = \varphi = 0$), the maximum parametric amplification is achieved [17]. The difference of the amplitude quadratures and the sum of the phase quadratures between two orthogonal polarization modes are

$$\begin{aligned}\widehat{X}_{\widehat{b}_{\uparrow}} - \widehat{X}_{\widehat{b}_{\leftarrow}} &= e^{-r} \widehat{X}_{\widehat{a}_{\uparrow}} - e^{-r} \widehat{X}_{\widehat{a}_{\leftarrow}}, \\ \widehat{Y}_{\widehat{b}_{\uparrow}} + \widehat{Y}_{\widehat{b}_{\leftarrow}} &= e^{-r} \widehat{Y}_{\widehat{a}_{\uparrow}} + e^{-r} \widehat{Y}_{\widehat{a}_{\leftarrow}}.\end{aligned}\quad (4)$$

Under the limit $r \rightarrow \infty$, the output orthogonal polarization modes are the perfect EPR beams with quadrature amplitude correlation and quadrature phase anticorrelation [17]. When the injected subharmonic signal and harmonic pump fields are out of phase, *i.e.* $\Phi = \varphi = \pi/2$, NOPA operates at parametric deamplification [18,20]. Therefore, the sum of the amplitude

TABLE I – Generation of the secret key string.

| Time | State of NOPA | T_1 | T_2 | T_3 | T_5 | T_6 |
|-------------|---------------|----------|-------|----------|-------|----------|
| | | Dam | Am | Am | Dam | Am |
| Alice | rna | 1 | 0 | 0 | 0 | 1 |
| | rnb | 0 | 1 | 1 | 0 | 0 |
| Bob | | AQ | AQ | PQ | PQ | PQ |
| Correlation | | Yes | No | Yes | No | Yes |
| Key | | 1 | – | 1 | – | 0 |

quadratures and the difference of the phase quadratures of the orthogonal polarization modes are as follows:

$$\begin{aligned}\widehat{X}_{\widehat{b}_1} + \widehat{X}_{\widehat{b}_{\leftarrow}} &= e^{-r}\widehat{Y}_{\widehat{a}_1} + e^{-r}\widehat{Y}_{\widehat{a}_{\leftarrow}}, \\ \widehat{Y}_{\widehat{b}_1} - \widehat{Y}_{\widehat{b}_{\leftarrow}} &= e^{-r}\widehat{X}_{\widehat{a}_1} - e^{-r}\widehat{X}_{\widehat{a}_{\leftarrow}}.\end{aligned}\quad (5)$$

Obviously, the EPR beams with the quadrature amplitude anticorrelation and quadrature phase correlation are obtained for $r > 0$.

For implementing the QKD with the bright EPR beams, the EPR source is placed in Alice's station (sender). Controlling the relative phase between the pump and the injected signal fields of the NOPA to $\Phi = 0$ or $\Phi = \pi/2$, the two types of EPR beams specified by eqs. (4) and (5) are produced. In this proposed scheme, we require the two types of EPR beams having the same intensity which may be realized by simultaneously adjusting the power of the pump field when the relative phase is changed in experiments. The random exchanging between the two types of EPR correlations is controlled by Alice; therefore, an eavesdropper cannot determine which type of correlation the bright EPR beams process. Alice splits two orthogonal polarization modes which are two quantum-correlated halves of the EPR beams, to two space-separated modes \widehat{b}_1 and \widehat{b}_2 with the polarizer (PBS1). Alice generates two independent random strings of binary numbers and encodes random strings on the bright EPR beams with the help of switches which are gated on and off to control radio frequency (RF) sources. The RF signals of one random string are modulated on the amplitude quadrature of \widehat{b}_1 and \widehat{b}_2 simultaneously with reverse signs by amplitude modulators (AM) and the ones of the other random string on phase quadrature by phase modulators (PM). Alternatively, the operating state of NOPA between amplification and deamplification and modulating signals on \widehat{b}_1 and \widehat{b}_2 have to be synchronized. From eqs. (3) we know that the amplitude and phase quadratures $\langle \delta(\widehat{X}_{\widehat{b}_1})^2 \rangle = \langle \delta(\widehat{X}_{\widehat{b}_2})^2 \rangle = \langle \delta(\widehat{Y}_{\widehat{b}_1})^2 \rangle = \langle \delta(\widehat{Y}_{\widehat{b}_2})^2 \rangle$ of EPR beams have a large noise when the squeezing factor r is large. We make the modulated signals be completely submerged in the large noise background. Alice now decides at random whether to send EPR beams with $\langle \delta(\widehat{X}_{\widehat{b}_1} + \widehat{X}_{\widehat{b}_2})^2 \rangle / 2 < 1$ and $\langle \delta(\widehat{Y}_{\widehat{b}_1} - \widehat{Y}_{\widehat{b}_2})^2 \rangle / 2 < 1$ or with $\langle \delta(\widehat{X}_{\widehat{b}_1} - \widehat{X}_{\widehat{b}_2})^2 \rangle / 2 < 1$ and $\langle \delta(\widehat{Y}_{\widehat{b}_1} + \widehat{Y}_{\widehat{b}_2})^2 \rangle / 2 < 1$, and Bob decides, also at random, which quadratures are to be measured.

We consider that two optical modes \widehat{b}_1 and \widehat{b}_2 have the boson commutation relations

$$\left[\widehat{b}_k, \widehat{b}_{k'} \right] = \left[\widehat{b}_k^\dagger, \widehat{b}_{k'}^\dagger \right] = 0, \quad \left[\widehat{b}_k, \widehat{b}_{k'}^\dagger \right] = \delta_{kk'} \quad k, k' = 1, 2. \quad (6)$$

The quadrature phase amplitudes of the two optical modes are given by

$$\widehat{X}_{\widehat{b}_k} = \widehat{b}_k + \widehat{b}_k^\dagger, \quad \widehat{Y}_{\widehat{b}_k} = -i(\widehat{b}_k - \widehat{b}_k^\dagger). \quad (7)$$

The quadrature phase amplitudes obey the commutation relations

$$\left[\widehat{X}_{\widehat{b}_k}, \widehat{X}_{\widehat{b}_{k'}} \right] = \left[\widehat{Y}_{\widehat{b}_k}, \widehat{Y}_{\widehat{b}_{k'}} \right] = 0, \quad \left[\widehat{X}_{\widehat{b}_k}, \widehat{Y}_{\widehat{b}_{k'}} \right] = 2i\delta_{kk'}, \quad k, k' = 1, 2. \quad (8)$$

Performing the unitary transformation on the modes \widehat{b}_1 and \widehat{b}_2 , we have

$$\widehat{c}_1 = \frac{1}{\sqrt{2}}(\widehat{b}_1 - \widehat{b}_2), \quad \widehat{c}_2 = \frac{1}{\sqrt{2}}(\widehat{b}_1 + \widehat{b}_2). \quad (9)$$

Thus the operators \widehat{c}_1 and \widehat{c}_2 satisfy the commutation relations just like modes \widehat{b}_1 and \widehat{b}_2 (eq. (6)). The quadrature phase amplitudes of the operators \widehat{c}_1 and \widehat{c}_2 can be written as

$$\begin{aligned} \widehat{X}_{\widehat{c}_1} &= \frac{1}{\sqrt{2}}(\widehat{X}_{\widehat{b}_1} - \widehat{X}_{\widehat{b}_2}), & \widehat{Y}_{\widehat{c}_1} &= \frac{1}{\sqrt{2}}(\widehat{Y}_{\widehat{b}_1} - \widehat{Y}_{\widehat{b}_2}), \\ \widehat{X}_{\widehat{c}_2} &= \frac{1}{\sqrt{2}}(\widehat{X}_{\widehat{b}_1} + \widehat{X}_{\widehat{b}_2}), & \widehat{Y}_{\widehat{c}_2} &= \frac{1}{\sqrt{2}}(\widehat{Y}_{\widehat{b}_1} + \widehat{Y}_{\widehat{b}_2}). \end{aligned} \quad (10)$$

The quadrature phase amplitudes of the operators \widehat{c}_1 and \widehat{c}_2 also obey the commutation relations (8). According to the commutation relations, the corresponding uncertainty principles of the quadrature phase amplitudes of the operators \widehat{c}_1 and \widehat{c}_2 are

$$\langle \delta \widehat{X}_{\widehat{c}_1}^2 \rangle \langle \delta \widehat{Y}_{\widehat{c}_1}^2 \rangle \geq 1, \quad \langle \delta \widehat{X}_{\widehat{c}_2}^2 \rangle \langle \delta \widehat{Y}_{\widehat{c}_2}^2 \rangle \geq 1. \quad (11)$$

Equations (8) and (11) imply that quadrature amplitude difference $\widehat{X}_{\widehat{c}_1}$ and quadrature phase difference $\widehat{Y}_{\widehat{c}_1}$ cannot be measured simultaneously with arbitrarily high accuracy. However, the differences of the amplitude or phase quadratures of modes \widehat{b}_1 and \widehat{b}_2 , $\widehat{X}_{\widehat{c}_1}$ or $\widehat{Y}_{\widehat{c}_1}$ and the sums, $\widehat{X}_{\widehat{c}_2}$ or $\widehat{Y}_{\widehat{c}_2}$, are commutated and may be simultaneously measured with high accuracy. In our protocol the binary modulated signals on two halves of EPR beams are out of phase, therefore the quadrature amplitude sum $\widehat{X}_{\widehat{c}_2}$ or the quadrature phase sum $\widehat{Y}_{\widehat{c}_2}$ do not carry any binary modulated signal and are not used for the communication. At Bob's station the two bright modes \widehat{b}_1 and \widehat{b}_2 are combined into a same direction with a polarizing beamsplitter (PBS2), then are split into two modes \widehat{e} and \widehat{f} by PBS3. The modes \widehat{e} and \widehat{f} are written as

$$\widehat{e} = \widehat{b}_1 \cos \frac{\theta}{2} + i\widehat{b}_2 \sin \frac{\theta}{2}, \quad \widehat{f} = \widehat{b}_2 \cos \frac{\theta}{2} + i\widehat{b}_1 \sin \frac{\theta}{2}, \quad (12)$$

where θ is the relative phase between the modes \widehat{b}_2 and \widehat{b}_1 which is controlled by a variable delay. The bright output beams \widehat{e} and \widehat{f} are directly detected by D_1 and D_2 , then the detected photocurrents are subtracted with a negative power combiner (-). Bob randomly chooses either $\theta = 0$ or $\theta = \pi/2$. When $\theta = 0$ the normalized output spectrum of the photocurrent difference is given by

$$\widehat{i}_-^0(\Omega) = \frac{1}{\sqrt{2}} \left[\widehat{X}_{\widehat{b}_1}(\Omega) - \widehat{X}_{\widehat{b}_2}(\Omega) \right] + X_{s,rna}, \quad (13)$$

where $X_{s,rna}$ stands for the signals of the random string a (rna) modulated on amplitude quadrature. In this case, the amplitude quadrature difference measurement between two modes \widehat{b}_1 and \widehat{b}_2 can be achieved by means of the direct detection of photocurrent. If the EPR beams with the correlated amplitude quadrature are received, Bob obtains the data string rna imposed on the sub-QNL noise floor and serves it as key and if deamplification

occurs, Bob is not able to extract the signal submerged in the large noise background [9,18]. For $\theta = \pi/2$, the normalized output spectrum of photocurrent difference is given by [16]

$$\hat{i}_-^{\pi/2}(\Omega) = \frac{1}{\sqrt{2}} \left[\hat{Y}_{\hat{b}_1}(\Omega) - \hat{Y}_{\hat{b}_2}(\Omega) \right] + Y_{s,\text{rnb}}, \quad (14)$$

where $Y_{s,\text{rnb}}$ stands for the signals of the random string b (rnb) modulated on phase quadrature. The phase quadrature difference measurement between two modes \hat{b}_1 and \hat{b}_2 can be achieved by the direct detection system of photocurrents without the help of LO beam. If the received EPR beams are phase-correlated, Bob obtains the data string rna modulated on the phase quadrature of EPR beams. Of course, if they are anticorrelated, Bob obtains nothing. What mentioned above and eqs. (4), (5) show that only when Alice operates NOPA at amplification and Bob chooses $\theta = 0$, the signals modulated on amplitude quadrature can be obtained by Bob, as well as only when Alice operates NOPA at the deamplification and Bob chooses $\theta = \pi/2$, the signals modulated on phase quadrature can be extracted by Bob. After a communication of a key string is accomplished, Bob tells Alice on a public line which quadrature he detected at given time points, but he does not tell the signals he obtained. Statistically, the probability that Bob obtains the signals is 50%. At this stage, Alice and Bob generate the common secret key. This protocol is summarized in table I. The presence of Eve will be revealed by increased noise floor of signals or by events “no key” occurring statistically more than 50%. Because of the transmission errors (and possibly the actions of Eve) Alice and Bob will not share the same data string. However, techniques exist for data reconciliation and privacy amplification which allow Alice and Bob to select with high probability a subset of their data which is error free [12,21]. In the proposed protocol, the security of transmission against eavesdropping is guaranteed by the sensitivity of the existing correlations to losses and by the impossibility to measure both conjugate variables simultaneously due to the limitation of the uncertainty principle. The complete security analysis for the case of continuous variables is non-trivial and lies beyond the scope of the present paper. The general proof of the optimum eavesdropper strategies for continuous variable scheme has been discussed in refs. [5, 13, 14].

In conclusion, we propose a protocol of the quantum key distribution which may be experimentally realized by using a NOPA as the EPR source and controlling the operating states of NOPA. By means of the random choices to the operating states of amplification and deamplification at Alice and the measured quadratures (quadrature amplitude difference $\hat{X}_{\hat{c}_1}$ or quadrature phase difference $\hat{Y}_{\hat{c}_1}$) at Bob, the secret key is established. The uncertainty relations of quantum mechanics provide the security of the communication. Due to exploiting the bright EPR beams generated from NOPA and the directly measuring technique, the troubles due to the local oscillator and the high sensitivity to mode-mismatching which are met in usual homodyne detection are eliminated.

* * *

This research was supported by the National Fundamental Research Program (No. 2001CB309304), the National Natural Science Foundation of China (Approval No. 60178012, 60238010) and the Shanxi Province Young Science Foundation (No. 20021014).

REFERENCES

- [1] BENNETT C. H. and BRASSARD G., *Public-key distribution and coin tossing*, in *Proceedings of the IEEE International Conference Computers, Systems and Signal Processing, Bangalore*, Vol. **175** (IEEE) 1984, pp. 175-179.

- [2] BENNETT C. H., *Phys. Rev. Lett.*, **68** (1992) 3121.
- [3] EKER A. K., *Phys. Rev. Lett.*, **67** (1991) 661.
- [4] RALPH T. C., *Phys. Rev. A*, **61** (2000) 010303(R).
- [5] RALPH T. C., *Phys. Rev. A*, **62** (2000) 062306.
- [6] REID M. D., *Phys. Rev. A*, **62** (2000) 062308.
- [7] SILBERHORN CH. *et al.*, *Phys. Rev. Lett.*, **88** (2002) 167902.
- [8] NAVEZ P., GATTI A. and LUGIATO L. A., e-print quant-ph/0101113 (2001).
- [9] PEREIRA S. F., OU Z. Y. and KIMBLE H. J., *Phys. Rev. A*, **62** (2000) 042311.
- [10] HILLERY M., *Phys. Rev. A*, **61** (2000) 022309.
- [11] CERF N. J., LEVY M. and ASSCHE G. V., *Phys. Rev. A*, **63** (2000) 052311.
- [12] CERF N. J., IBLISDIR S. and ASSCHE G. V., e-print quant-ph/0107077 (2001).
- [13] GOTTESMANN D. and PRESKILL J., *Phys. Rev. A*, **63** (2001) 022309.
- [14] GROSSHANS F. and GRANGIER P., *Phys. Rev. Lett.*, **88** (2002) 057902.
- [15] FURUSAWA A. *et al.*, *Science*, **282** (1998) 706.
- [16] ZHANG J. and PENG K. C., *Phys. Rev. A*, **62** (2000) 064302; ZHANG J. *et al.*, *Phys. Rev. A*, **66** (2002) 032318; 042319.
- [17] ZHANG Y. *et al.*, *Phys. Rev. A*, **62** (2000) 023813.
- [18] LI X. Y. *et al.*, *Phys. Rev. Lett.*, **88** (2002) 047904.
- [19] ZHANG J., XIE C. D. and PENG K. C., *Phys. Lett. A*, **287** (2001) 7.
- [20] SCHNEIDER K. *et al.*, *Opt. Lett.*, **21** (1996) 1396.
- [21] RALPH T. C., arXiv:quant-ph/0109096.