

## Continuous variable quantum key distribution based on optical entangled states without signal modulation

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2009 EPL 87 20005

(<http://iopscience.iop.org/0295-5075/87/2/20005>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 218.26.34.78

This content was downloaded on 14/04/2015 at 09:06

Please note that [terms and conditions apply](#).

# Continuous variable quantum key distribution based on optical entangled states without signal modulation

XIAOLONG SU, WENZHE WANG, YU WANG, XIAOJUN JIA, CHANGDE XIE<sup>(a)</sup> and KUNCHI PENG

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

received 3 March 2009; accepted in final form 17 July 2009

published online 18 August 2009

PACS 03.67.Dd – Quantum cryptography and communication security

PACS 42.50.-p – Quantum optics

PACS 03.67.Mn – Entanglement measures, witnesses, and other characterizations

**Abstract** – In this paper, we present the first experimental demonstration on continuous variable quantum key distribution using determinant Einstein-Podolsky-Rosen entangled states of optical field. By means of the instantaneous measurements of the quantum fluctuations of optical modes, respectively, distributed at sender and receiver, the random bits of secret key are obtained without the need for signal modulation. The post-selection boundaries for the presented entanglement-based scheme against both Gaussian collective and individual attacks are theoretically concluded. The final secret key rates of 84 kbits/s and 3 kbits/s are completed under the collective attack for the transmission efficiency of 80% and 40%, respectively.

Copyright © EPLA, 2009

Quantum key distribution (QKD) allows two legitimate parties, Alice and Bob, to establish the secret key only known by themselves. A secret key is usually generated by Alice transmitting the prepared quantum states to Bob, who performs measurements on the received states to distill the information. There are two types of QKD systems in which the discrete or continuous quantum variables are exploited, respectively. For discrete variable (DV) QKD protocols the key information is encoded in discrete quantum variables of single-photon light pulse, such as polarization or phase [1]. In continuous variable (CV) QKD protocols continuous quantum variables of light field, such as amplitude and phase quadratures, are used for transmitting information. Comparing with DV QKD of single-photon schemes CV QKD promises significantly higher secret key rates and eliminates the need for single-photon technology. Recently, coherent state CV QKD protocols have been experimentally demonstrated [2–6]. These successful experiments proved that CV QKD is a hopeful and viable path to develop quantum cryptography for real-world applications. On the other hand, the strictly theoretical proofs on the security of CV QKD protocols using both coherent and non-classical states of light have been achieved [7–10]. CV QKD protocols have recently been shown to be unconditionally

secure, that is, secure against arbitrary attacks [11] and have been proved to be unconditionally secure over long distance [12].

Quantum entanglement is one of the quite essential features in quantum mechanics that has no analogue in classical physics. It has been theoretically demonstrated by Curty *et al.* that the presence of detectable entanglement in a quantum state effectively distributed between sender (Alice) and receiver (Bob) is a necessary precondition for successful key distillation [13]. However, there is no CV QKD experiment directly utilizing optical entangled states to be presented until now, although a variety of theoretical CV QKD protocols based on Einstein-Podolsky-Rosen (EPR) entanglement and squeezing of optical fields have been proposed [14–21]. Not like CV QKD protocols applying coherent states of light [2–6], in which the bits of secret key are constructed classically using amplitude and phase modulation, so-called prepare-and-measure (P&M) scheme [5], in the entanglement-based (EB) schemes proposed by refs. [16] and [17] the bits of the random secret key are constructed by the instantaneous measurements of the correlated quantum fluctuations of the quadratures between two entangled optical modes distributed at Alice and Bob. In the EB CV QKD protocols, the quantum fluctuations of entangled optical beams with the truly quantum randomness are utilized to generate the key. Due to that the

<sup>(a)</sup>E-mail: changde@sxu.edu.cn

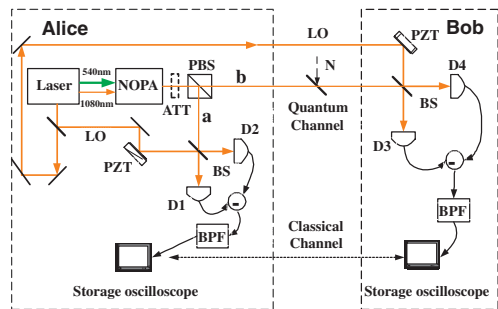


Fig. 1: (Colour on-line) The experimental system of QKD. NOPA: non-degenerate optical parametric amplifier, ATT: attenuator, PBS: polarization beam splitter, LO: local oscillation beam, N: vacuum noise, PZT: piezoelectric transducer, BS: 50/50 beam splitter, D1-D4: photodetector, BPF: band-pass filter.

classical signal modulation is not needed, the bit rates will not be limited by the rates of the electronic modulators and the experimental systems will be simplified.

In the presented paper, we experimentally demonstrated the proof-of-principle CV QKD protocol using a pair of bright EPR entangled beams produced from a non-degenerate optical parametric amplifier (NOPA). We concluded the post-selection boundaries of the presented EB CV QKD scheme against both Gaussian collective and individual attacks. By means of the post-selection, reconciliation and privacy amplification techniques, the final secret key was obtained through distilling the measured data of the correlated quantum fluctuations of quadratures. The generated raw key rate is 2 Mbits/s and the final secret key rates are 84 kbits/s and 3 kbits/s against Gaussian collective attack for the transmission efficiency of 80% and 40%, respectively. We believe that this is the first experimental demonstration of CV QKD protocols directly exploiting the EPR entanglement of amplitude and phase quadratures of optical field. On the physical sense this experiment intuitively shows the close relationship between the security of CV QKD and the quantum entanglement.

The experimental setup of the CV QKD protocol is shown in fig. 1. The laser is a homemade continuous wave intracavity frequency-doubled and frequency stabilized Nd:YAP/KTP ring laser consisting of five mirrors [22]. The second harmonic wave output at 540 nm is used for the pump field of the NOPA and the fundamental wave output at 1080 nm is separated into two parts, one is for the injected signal of the NOPA and the other is used as the local oscillation beams of the homodyne detections for Alice and Bob. The NOPA consists of an  $\alpha$ -cut type-II KTP crystal and a concave mirror. Through a parametric down-conversion process of type-II phase match, a pair of EPR beams with anticorrelated amplitude quadratures and correlated phase quadratures may be produced from the NOPA operating in the state of de-amplification, that is, the pump field and the injected signal are out of

phase [23]. The bandwidth of the NOPA is about 20 MHz, in which the output beams are entangled. If distributing the two beams of EPR pair to Alice (beam  $a$ ) and Bob (beam  $b$ ), the instantaneous measurement outcomes of quadrature quantum fluctuations on their respective modes will be fairly identical due to the quantum correlations of quadratures [24].

In the communication, Alice and Bob randomly measure the amplitude or phase quadrature of the entangled optical beam they hold respectively, with the homodyne detection systems. After the measurement is completed, they compare the measurement basis in the authorized classic channel and only remain the measurement results of the compatible basis. Then they use post-selection technique to select a subset from the measured raw data to make the mutual information of Alice and Bob advantage over Eve's information. To implement the post-selection, Alice publicly announce the absolute values of the measured amplitude or phase quadratures ( $|X_A|$  or  $|Y_A|$ ), but not publicly open their symbols [4]. Alice and Bob also choose a random subset of data to characterize the channel efficiency and excess noise. From these values they select the secure data and discard the insecure data. After post-selection procedure, Alice and Bob interpret the post-selected data into binary data. For the correlated phase quadratures both Alice and Bob may define the positive and negative phase fluctuations as a binary "1" and "0", respectively. However, for the anticorrelated amplitude quadratures if Alice define the positive (negative) amplitude fluctuation as "1" ("0"), Bob should defines negative (positive) amplitude fluctuation as "1" ("0"). Then we apply the reconciliation protocol to correct the errors of the retained data. At last, we apply a privacy amplification procedure to distill the final secret key.

In the security analysis we assume that the quantum channel connecting Alice and Bob is lossy with imperfect transmittivity of  $\eta$  and the Gaussian excess noise  $\delta$  on the quadrature distribution exists in the communication system. The security analyses are restricted to protect against Gaussian attacks only. For the optimal beam splitter attack [25], that is, Eve takes a fraction  $1 - \eta$  of the beam  $b$  at Alice's site and sends the fraction  $\eta$  to Bob through her own lossless line. In this case Eve is totally undetected, and she gets the maximum possible information according to the no-cloning theorem. For collective attack, Eve listens to the communication between Alice and Bob during the key distillation procedure and then applies the optimal collective measurement on the ensemble of stored ancilla. The maximum information Eve may have access to is limited by the Holevo bound  $\chi$  [5]. Under the individual attack, Eve measures the intercepted ensemble before the key distillation stage and Eve's information is summarized by the mutual information between Alice and Eve,  $I_{AE}$ , for direct reconciliation. Generally, the information exchange is secure as long as the mutual information between Alice and Bob ( $I_{AB}$ ) is larger than Eve's information. The condition of  $I_{AB} > I_{AE}$  for extracting

secure key directly results in the restriction of the maximum transmission losses less than 3 dB which will limit the possible transmission distances [25]. Fortunately, the 3 dB loss limit for CV QKD protocols can be beaten by implementing a reverse reconciliation scheme [2] or applying an appropriate post-selection [3,4,26]. It has been shown that there must be a lower limit of  $\eta$  ( $2\eta > \delta$ ) for the secure key distillation if the excess noise exists [27]. The security of EB scheme against collective attack with reverse reconciliation has been proved [28]. Here, we analyze the post-selection boundary for the EB scheme against Gaussian collective attack and Gaussian individual attack.

For the EPR beams with anticorrelated amplitude quadratures and correlated phase quadratures, we have the following relations [28]:

$$\langle X_{a(b)}^2 \rangle = \langle Y_{a(b)}^2 \rangle = VN_0 = (e^{2r} + e^{-2r})N_0/2, \quad (1)$$

$$\langle (X_a + X_b)^2 \rangle = \langle (Y_a - Y_b)^2 \rangle = 2e^{-2r}N_0, \quad (2)$$

$$\langle X_a X_b \rangle = -\sqrt{V^2 - 1}N_0, \quad (3)$$

$$\langle Y_a Y_b \rangle = \sqrt{V^2 - 1}N_0, \quad (4)$$

where  $r$  is the correlation parameter,  $N_0 = 1/4$  is the shot-noise-limited variance. These beam are entangled, and the measurement of a quadrature of beam  $a$  (e.g.  $Y_a$ ) gives Alice information on the same quadrature of the other beam ( $Y_b$ ). By measuring the amplitude quadrature  $X_a$  (phase quadrature  $Y_a$ ) on her beam  $a$ , Alice learns  $X_A$  ( $Y_A$ ), and projects the Bob's beam  $b$  onto a  $X$ -squeezed ( $Y$ -squeezed) state of squeezing parameter  $s = 1/V$  centered on  $(X_A, 0)$  [ $(0, Y_A)$ ] [28]. The best estimate Alice can have on  $Y_b$  knowing  $Y_a$  is of the form  $Y_A = \alpha Y_a$  with  $\alpha = \frac{\langle Y_b Y_a \rangle}{\langle Y_a^2 \rangle}$ , the value of  $\alpha$  being found by minimizing the variance of the error operator  $\delta Y_A = Y_b - Y_A$ . The conditional variance  $V_{Y_b|Y_A}$  of  $Y_b$  knowing  $Y_A$  quantifies the remaining uncertainty on  $Y_b$  after the measurement of  $Y_a$  giving the estimate  $Y_A$  of  $Y_b$ , and we have

$$V_{Y_b|Y_A} = \langle \delta Y_A^2 \rangle = \langle Y_b^2 \rangle - \frac{|\langle Y_a Y_b \rangle|^2}{\langle Y_a^2 \rangle} = \frac{N_0}{V}. \quad (5)$$

Since by measuring  $Y_a$  Alice deduces  $Y_A$ , and since  $Y_b = Y_A + \delta Y_A$ , the beam  $b$  is projected onto a  $Y$ -squeezed state with squeezing variance  $V_s = V_{Y_b|Y_A} = N_0/V$  centered on  $(0, Y_A)$ . Alternatively, by measuring  $X_a$ , Alice learns  $X_A$  and projects the other beam onto a  $X$ -squeezed state centered on  $(X_A, 0)$  with the same squeezing variance  $V_s = N_0/V$ . The variances of quadratures measured by Alice and Bob are  $V_A = \alpha^2 V N_0 = (V - 1/V)N_0$  and  $V_B = (\eta V_A + \eta V_s + 1 - \eta + \delta)N_0$ , respectively.

The probability that Bob obtains the measurement outcome  $Y_B$  is given by

$$P_B(Y|\Psi) = \frac{1}{\sqrt{2\pi V_B^N}} \exp \left[ -\frac{(Y_B - \sqrt{\eta} Y_A)^2}{2V_B^N} \right], \quad (6)$$

where  $|\Psi\rangle$  represents the transmitted quantum state, the noise variance  $V_B^N = (\eta V_s + 1 - \eta + \delta)N_0$  of which depends on the squeezed variance  $\eta V_s N_0$ , the ‘vacuum noise’ component due to the line losses  $(1 - \eta)N_0$ , and the ‘excess noise’ component  $\delta N_0$ . The corresponding Bob's error rate is given by

$$p = \frac{P_B(Y|\Psi)}{P_B(Y|\Psi) + P_B(Y|-\Psi)} = \frac{1}{1 + \exp \left( \frac{4\sqrt{\eta} Y_A |Y_B|}{2V_B^N} \right)}. \quad (7)$$

Based on eq. (7) we calculated the mutual information between Alice and Bob

$$I_{AB} = 1 + p \log_2 p + (1 - p) \log_2 (1 - p). \quad (8)$$

For collective attack, Eve's knowledge of the data can be quantified by the Holevo bound  $\chi$ , which equals to [29]

$$\chi = S(\bar{\rho}) - \sum_{i=0}^1 p_i S(\rho_i), \quad \rho = \sum_{i=0}^1 p_i \rho_i, \quad (9)$$

where  $S(\rho) = -\text{tr} \rho \log_2 \rho$  is the von Neumann entropy of a quantum state  $\rho$ . The  $\chi$  includes that Eve being allowed to measure out her ancillas collectively. After Alice and Bob have corrected their bit strings, Eve can use the information transmitted over the public channel to optimize her measurements on her ancilla systems. The quantum states in Eve's hand, conditioned on Alice's data, are given by  $|\Psi_i\rangle_E = |\pm \sqrt{1 - \eta} \Psi\rangle$ , where  $i = 0, 1$  denote the encoded binary state. These states are pure, so that we have  $\chi = S(\bar{\rho})$ . What remains to be calculated are the eigenvalues of  $\bar{\rho} = \frac{1}{2}(|\Psi_0\rangle_E \langle \Psi_0| + |\Psi_1\rangle_E \langle \Psi_1|)$ . The symmetry allows us to write the states  $|\Psi_i\rangle_E$  as

$$\begin{aligned} |\Psi_0\rangle_E &= c_0 |\Phi_0\rangle + c_1 |\Phi_1\rangle \\ |\Psi_1\rangle_E &= c_0 |\Phi_0\rangle - c_1 |\Phi_1\rangle \end{aligned} \quad (10)$$

where the  $|\Phi_i\rangle$  are orthonormal states. A short calculation shows that is already diagonal in this basis with eigenvalues  $|c_i|^2$ , so that the Holevo quantity is given by

$$\chi = S(\bar{\rho}) = -\sum_{i=0}^1 |c_i|^2 \log_2 |c_i|^2. \quad (11)$$

The normalization of  $\rho$ ,  $|c_0|^2 + |c_1|^2 = 1$ , and the overlap  $|c_0|^2 - |c_1|^2 = {}_E \langle \Psi_0 | \Psi_1 \rangle_E$  give the expressions for the coefficients,

$$\begin{aligned} |c_0|^2 &= \frac{1}{2}(1 + {}_E \langle \Psi_0 | \Psi_1 \rangle_E), \\ |c_1|^2 &= \frac{1}{2}(1 - {}_E \langle \Psi_0 | \Psi_1 \rangle_E). \end{aligned} \quad (12)$$

The overlap of the two states can be calculated by  ${}_E \langle \Psi_0 | \Psi_1 \rangle_E = \pi \int W(X, -Y) W(X, Y) dX dY$  if  $Y$ -quadrature is measured, where  $W(X, Y)$  is the Wigner function of the projected squeezed states centered on

$(X_0, Y_0)$ . If  $Y$ -quadrature is measured by Alice, the correlation matrix of the projected  $Y$ -squeezed state can be written as

$$\mathbf{V}_c = \frac{1}{4} \begin{bmatrix} V & 0 \\ 0 & 1/V \end{bmatrix}. \quad (13)$$

Using the expression of Wigner function for Gaussian states with one-dimensional vector [30]

$$W(X, Y) = \frac{1}{2\pi\sqrt{\det \mathbf{V}_c}} \exp \left\{ -\frac{1}{2} (X, Y) [\mathbf{V}_c]^{-1} (X, Y)^T \right\}, \quad (14)$$

we can write out the corresponding Wigner function of the projected  $Y$ -squeezed state

$$W(X, Y) = \frac{2}{\pi} \exp \left[ -\frac{4(X - X_0)^2}{e^{2r} + e^{-2r}} - (e^{2r} + e^{-2r})(Y - Y_0)^2 \right]. \quad (15)$$

If  $Y$ -quadrature are measured, then Eve's state is displaced to  $Y_0 = \sqrt{1 - \eta} Y_A$ , so the overlap between the two states  $W(X, Y)$  and  $W(X, -Y)$  is

$$f = {}_E \langle \Psi_0 | \Psi_1 \rangle_E = \exp \left[ -\frac{(1 - \eta) Y_A^2}{2V_s} \right]. \quad (16)$$

So, the Holevo quantity can be directly calculated. From eqs. (8) and (11), we can obtain the secret key rates  $K = I_{AB} - \chi$  against collective attack.

For the individual attack, the mutual information between Alice and Eve is expressed by [26]

$$I_{AE} = \frac{1}{2} (1 + \sqrt{1 - f^2}) \log_2 (1 + \sqrt{1 - f^2}) + \frac{1}{2} (1 - \sqrt{1 - f^2}) \log_2 (1 - \sqrt{1 - f^2}). \quad (17)$$

The secret key rate against individual attack is  $\Delta I = I_{AB} - I_{AE}$ . Of course, the security boundary can also be directly applied to the anti-correlated amplitude quadrature  $X$ , for that we only need to change the signs of the measured amplitude values.

In the communication, at first Alice separates the EPR entangled beams generated by the NOPA with a polarized beam splitter (PBS) and then sends one of them (beam  $b$ ) to Bob while keeps the other one (beam  $a$ ) within her own station. The beam  $b$  is transmitted in air about 2 meter. We simulated the QKD communication in two cases respectively with the transmission efficiency of 80% and 40%, which were completed by inserting an appropriate attenuator into the optical path. For making the balance attenuation of two optical and implementing simultaneous measurements of the correlated quantum fluctuations, we insert an attenuator (ATT) with transmission efficiency 89% or 45% into the optical path of the EPR beams before they are separated. In addition to the detection efficiency of 90%, the total transmission efficiency between Alice and Bob is 80% (89%  $\times$  90%)

or 40% (45%  $\times$  90%), respectively. During the communication, Alice and Bob randomly and instantaneously measure the amplitude or phase quadratures of their own beam with a homodyne detection system, which is completed by randomly switching the phase difference between the local oscillation and the EPR beam from 0 for the amplitude quadratures to  $\pi/2$  for the phase quadratures. The time interval  $\Delta t$  in which Alice and Bob switch the quadrature measurement is 5 ms in our experiment. The long interval of 5 ms for switching the measurement bases was limited by the phase locking technology of the homodyne detection systems we held in the proof-of-principle experiment. Indeed, to ensure the security the time interval  $\Delta t$  should be as short as possible which should be only confined by the storage time of photons in the NOPA. (It equals the reciprocal of the optical cavity bandwidth. For our NOPA the minimal  $\Delta t_{min}$  may reach  $\sim 5 \times 10^{-8}$  s in principle.) Of course, we also can enhance the security by lengthening the communication period to be much longer than  $\Delta t$  [31]. We choose the sideband frequency of  $\Omega = 2$  MHz as the centre frequency for Alice's and Bob's measurements because the highest entanglement is obtained at this frequency with our system. The measured initial correlation variances of the amplitude sum and phase difference between the signal and idler beams from the NOPA were 3.08 dB and 3.01 dB below the corresponding shot-noise-level (SNL) at 2 MHz, which corresponding to the correlation parameter  $r = 0.355$  and  $r = 0.347$  for amplitude and phase quadratures, respectively. The output photocurrent from the negative power combiner (-) passes through a low-noise amplifier of 30 dB and a band-pass filter (BPF) with the central frequency of 2 MHz and the bandwidth of 600 kHz, then it is recorded by a storage oscilloscope (Agilent 54830B) at Alice and Bob, respectively. The recorded data are transferred to a computer for the further data processing. Before the communication, Alice and Bob should synchronize their clocks and agree on the time interval  $\Delta t$  and the instantaneous measurement time  $\Delta T$  in which a data point is taken. Only when the instantaneous measurement time  $\Delta T$  is longer than the storage time of the NOPA, the measured correlations between the quadratures of signal and idler beams have a stable value [32]. The sample rate of 10 MHz was chosen in the experiment. Since a band-pass filter is placed before the storage oscilloscope in order to extract the highly correlated quantum fluctuations, the real communication bandwidth is reduced. Thus, in the data processing we digitally re-sample the recorded data at 2 MHz (which corresponds to  $\Delta T = 5 \times 10^{-7}$  s).

After having recorded a string of data which include many data sets (each set is measured within a phase switching time interval of 5 ms), Alice and Bob communicate through an authenticated public channel to discard the sets measured on the incompatible bases and to remain the compatible measured sets corresponding to the same bases. The measured normalized variances of Alice's and Bob's amplitude quadratures are

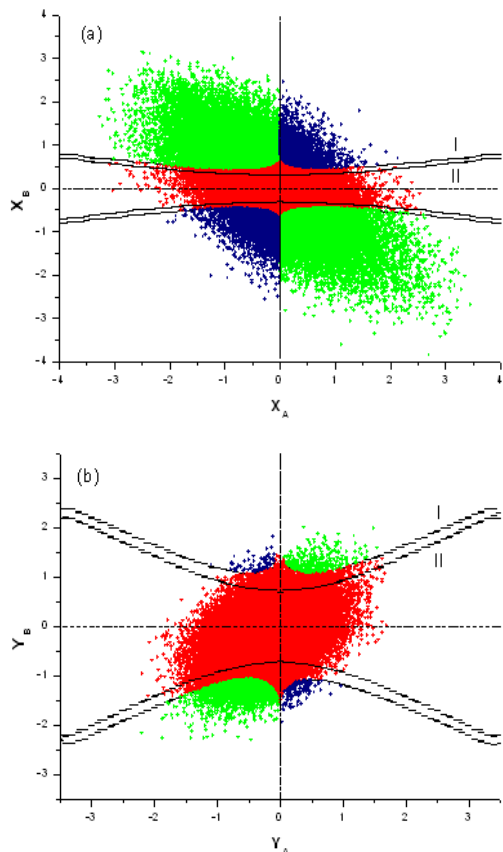


Fig. 2: (Colour on-line) The “global” perspective of Alice’s and Bob’s data. (a) Amplitude quadrature for 80% transmission efficiency. (b) Phase quadrature for 40% transmission efficiency. I: post-selection boundary for collective attack. II: post-selection boundary for individual attack. Green data points: data that is error-free. Blue data points: data that has bit-flip errors. Red data points: data that has a negative net information rate.

$6.78N_0$  and  $7.02N_0$  for 80% transmission efficiency, respectively. Considering the influence of transmission efficiency, the variance measured by Alice is  $V_{A'} = (\eta V_A + 1 - \eta)N_0 = 6.78N_0$  for the transmission efficiency 80%, so we have  $V_A = 8.23N_0$ . Since  $V_A = (V - 1/V)N_0$  and  $V_s = N_0/V$ , we obtained  $V = 8.35N_0$  and  $V_s = 0.12N_0$ . From  $V_B = (\eta V_A + \eta V_s + 1 - \eta + \delta)N_0$  and Bob’s variance value we obtained the corresponding excess noise of  $\delta_1 = 0.14N_0$  for 80% transmission efficiency. In the same way, from the normalized variances of Alice’s and Bob’s phase quadratures  $3.89N_0$  and  $4.05N_0$  for 40% transmission efficiency, we calculated the excess noise of  $\delta_2 = 0.11N_0$ . Figure 2 shows the “global” perspective of Alice’s and Bob’s results measured on compatible bases, fig. 2(a) shows the function of the amplitude quadratures ( $X_B$  vs.  $X_A$ ) for 80% transmission efficiency and fig. 2(b) shows that of the phase quadratures ( $Y_B$  vs.  $Y_A$ ) corresponding to 40% transmission efficiency. The anti-correlation of the amplitude quadratures ( $\pm X_a \sim \mp X_b$ ) and the correlation of the phase quadratures ( $\pm Y_a \sim \pm Y_b$ ) are clearly exhibited in the perspective. The quadrature

measurements are normalized to the SNL of the measured beam. Each one of fig. 2(a) and (b) contains 50000 data points.

For extracting the secure data of  $I_{AB} > \chi(I_{AB} > I_{AE})$  from the measured raw data in the CV QKD, we used a post-selection technique, that is, to select a subset from the measured raw data points to make the mutual information of Alice and Bob advantage over Eve’s information. According to the way described before, Alice and Bob select the secure data and discard the insecure data. The dashed hyperbolas I and II in fig. 2 correspond to the secure boundaries for collective attack and individual attack, respectively. The regions at the outside of the hyperbolas I (II) are secure  $K > 0$  ( $\Delta I > 0$ ) for the collective (individual) attack, while the regions between the hyperbolas are insecure (red points), the data in which should be discarded. The green data points correspond to error-free bits, whilst the blue data points correspond to that with bit-flip errors.

After post-selection procedure, Alice and Bob interpret the post-selected data into binary data according to the way described above. Then we apply the “Cascade” reconciliation protocol [33] to correct the errors of the retained data. At the stage of the error correction, the data are arranged into many random subsets and the error data are corrected. The efficiency of reconciliation is about 80%. At last, we apply a privacy amplification procedure based on universal hashing functions to distill the final secret key [34,35]. First, Alice and Bob calculate a conservative upper bound for Eve’s knowledge about their key, then Alice and Bob compute the parities of random subsets of the error-corrected key bits. The obtained parity bits are kept as the final secret key. The results for different stages of the QKD protocol used to distill the secret key are shown in table 1. The cost of these secret key distillation processes is a reduction in the size of the secret key. With the existence of the Gaussian collective attack, after the privacy amplification procedure the final secret key rates of 84 kbits/s and 3 kbits/s are obtained for the transmission efficiencies of 80% and 40%, respectively. To the Gaussian individual attack only, the final secret key rates of 109 kbits/s and 10 kbits/s are obtained for the transmission efficiencies of 80% and 40%, respectively.

In conclusion, we accomplished the first experimental demonstration of CV QKD protocol using the bright EPR entangled optical beams. The quantum entanglement between two beams and the random quantum fluctuations of amplitude and phase quadratures of respective optical mode provide the physical mechanism for the CV QKD protocol without the signal modulation. The security of the EB CV QKD protocol against Gaussian collective and individual attack using post-selection technique is analyzed. Although, as an example, the binary coding scheme is utilized for simplification, Alice and Bob can agree on a higher-dimensional coding by dividing their results into intervals corresponding to more than two bits values, in principle. The presented CV QKD experiment

Table 1: Experimental results for the different stages of the QKD protocol used to distill the final secret key. Each step shows Alice's and Bob's mutual information ( $I_{AB}$  bits/symbol), Eve's information ( $\chi$  bits/symbol for collective attack and  $I_{AE}$  bits/symbol for individual attack), the corresponding net information rate ( $K$  bits/symbol and  $\Delta I$  bits/symbol) and the secret key rate (kbits/second) for 80% and 40% transmission efficiency, respectively.

|                       | 80% Transmission efficiency |          |          |      |                   |          |            |      |
|-----------------------|-----------------------------|----------|----------|------|-------------------|----------|------------|------|
|                       | Collective attack           |          |          |      | Individual attack |          |            |      |
|                       | $I_{AB}$                    | $\chi$   | $K$      | Rate | $I_{AB}$          | $I_{AE}$ | $\Delta I$ | Rate |
| Raw data              | 0.36                        | 0.35     | 0.01     | 2000 | 0.38              | 0.23     | 0.15       | 2000 |
| Post-selection        | 0.64                        | 0.44     | 0.20     | 508  | 0.52              | 0.26     | 0.26       | 679  |
| Reconciliation        | $\sim 1$                    | 0.68     | 0.32     | 346  | $\sim 1$          | 0.51     | 0.49       | 436  |
| Privacy amplification | $\sim 1$                    | $\sim 0$ | $\sim 1$ | 84   | $\sim 1$          | $\sim 0$ | $\sim 1$   | 109  |
|                       | 40% Transmission efficiency |          |          |      |                   |          |            |      |
|                       | Collective attack           |          |          |      | Individual attack |          |            |      |
|                       | $I_{AB}$                    | $\chi$   | $K$      | Rate | $I_{AB}$          | $I_{AE}$ | $\Delta I$ | Rate |
| Raw data              | 0.18                        | 0.44     | -0.26    | 2000 | 0.18              | 0.33     | -0.15      | 2000 |
| Post-selection        | 0.69                        | 0.63     | 0.06     | 46   | 0.44              | 0.35     | 0.09       | 180  |
| Reconciliation        | $\sim 1$                    | 0.89     | 0.11     | 34   | $\sim 1$          | 0.80     | 0.20       | 115  |
| Privacy amplification | $\sim 1$                    | $\sim 0$ | $\sim 1$ | 3    | $\sim 1$          | $\sim 0$ | $\sim 1$   | 10   |

intuitively and directly demonstrated the importance of the quantum entanglement for the secure communication. It is possible to develop the more complicated CV QKD networks by using the multipartite CV optical entangled states based on this demonstrated scheme.

\*\*\*

This research was supported by the NSFC (Grants No. 60736040, 10674088, 10804065 and 60608012), NSFC Project for Excellent Research Team (Grant No. 60821004), National Basic Research Program of China (Grant No. 2006CB921101) and Shanxi Province Science Foundation for Youths (Grant No. 2008021002).

## REFERENCES

- [1] Gisin N., Ribordy G., Tittel W. and Zbinden H., *Rev. Mod. Phys.*, **74** (2002) 145.
- [2] Grosshans F. *et al.*, *Nature*, **421** (2003) 238.
- [3] Lorenz S., Korolkova N. and Leuchs G., *Appl. Phys. B*, **79** (2004) 273.
- [4] Lance A. M. *et al.*, *Phys. Rev. Lett.*, **95** (2005) 180503.
- [5] Lodewyck J. *et al.*, *Phys. Rev. A*, **76** (2007) 042305.
- [6] Qi B., Huang L. L., Qian L. and Lo H. K., *Phys. Rev. A*, **76** (2007) 052323.
- [7] Gottesman D. and Preskill J., *Phys. Rev. A*, **63** (2001) 022309.
- [8] Iblisdir S., Van Assche G. and Cerf N. J., *Phys. Rev. Lett.*, **93** (2004) 170502.
- [9] Grosshans F., *Phys. Rev. Lett.*, **94** (2005) 020504.
- [10] Navascués M. and Acín A., *Phys. Rev. Lett.*, **94** (2005) 020505.
- [11] Renner R. and Cirac J. I., *Phys. Rev. Lett.*, **102** (2009) 110504.
- [12] Leverrier A. and Grangier P., *Phys. Rev. Lett.*, **102** (2009) 180504.
- [13] Curty M., Lewenstein M. and Lütkenhaus N., *Phys. Rev. Lett.*, **92** (2004) 217903.
- [14] Ralph T. C., *Phys. Rev. A*, **61** (1999) 010303(R).
- [15] Hillery M., *Phys. Rev. A*, **61** (2000) 022309.
- [16] Cerf N. J., Levy M. and Van Assche G., *Phys. Rev. A*, **63** (2000) 052311.
- [17] Reid M. D., *Phys. Rev. A*, **62** (2000) 062308.
- [18] Bencheikh K., Symul Th., Jankovic A. and Levenson J. A., *J. Mod. Opt.*, **48** (2001) 1903.
- [19] Silberhorn Ch., Korolkova N. and Leuchs G., *Phys. Rev. Lett.*, **88** (2002) 167902.
- [20] Su X. L., Jing J. T., Pan Q. and Xie C. D., *Phys. Rev. A*, **74** (2006) 062305.
- [21] Pirandola S., Mancini S., Lloyd S. and Braunstein S. L., *Nat. Phys.*, **4** (2008) 726.
- [22] Jia X. J., Su X. L., Pan Q., Gao J. R., Xie C. D. and Peng K. C., *Phys. Rev. Lett.*, **93** (2004) 250503.
- [23] Li X. Y., Pan Q., Jing J. T., Zhang J., Xie C. D. and Peng K. C., *Phys. Rev. Lett.*, **88** (2002) 047904.
- [24] Takei N. *et al.*, *Phys. Rev. A*, **74** (2006) 060101(R).
- [25] Grosshans F. and Grangier P., *Phys. Rev. Lett.*, **88** (2002) 057902.
- [26] Silberhorn Ch., Ralph T. C., Lütkenhaus N. and Leuchs G., *Phys. Rev. Lett.*, **89** (2002) 167901.
- [27] Namiki R. and Hirano T., *Phys. Rev. Lett.*, **92** (2004) 117901.
- [28] Grosshans F. *et al.*, *Quantum. Inf. Comput.*, **3** (2003) 535.
- [29] Heid M. and Lütkenhaus N., *Phys. Rev. A*, **73** (2006) 052316.
- [30] Van Loock P., *Fortschr. Phys.*, **50** (2002) 1177.
- [31] Lamoureaux L. P. *et al.*, *Phys. Rev. A*, **73** (2006) 032304.
- [32] Reynaud S., Fabre C. and Giacobino E., *J. Opt. Soc. Am. B*, **4** (1987) 1520.
- [33] Brassard G. and Salvail L., *Advances in Cryptology-Eurocrypt'93*, edited by Helleseht T., Vol. **765** (Springer-Verlag, Berlin) 1994, pp. 410-423.
- [34] Bennett C. H., Brassard G., Crépeau C. and Maurer U. M., *IEEE Trans. Inf. Theory*, **41** (1995) 1915.
- [35] Cachin C. and Maurer U. M., *J. Cryptol.*, **10** (1997) 97.