Quantum Key Distribution with Bright Entangled Beams

Ch. Silberhorn, N. Korolkova, and G. Leuchs

Zentrum für Moderne Optik an der Universität Erlangen-Nürnberg, Staudtstraße 7/B2, D-91058 Erlangen, Germany

(Received 14 November 2001; published 8 April 2002)

We suggest a quantum cryptographic scheme using continuous EPR-like correlations of bright optical beams. For binary key encoding, the continuous information is discretized in a novel way by associating a respective measurement, amplitude, or phase, with a bit value "1" or "0." The secure key distribution is guaranteed by the quantum correlations. No predetermined information is sent through the quantum channel contributing to the security of the system.

DOI: 10.1103/PhysRevLett.88.167902 PACS numbers: 03.67.Dd, 03.65.Ud

Quantum key distribution (QKD) is the most advanced technology in the field of quantum information processing. The conventional arrangements use dichotomic quantum systems to realize the secure information transfer (for a review, see [1]). These discrete systems have the advantage to be in principle loss insensitive in terms of security. However, the generation process for entangled photon pairs needed for QKD based on EPR correlations is spontaneous and therefore probabilistic. This limits the achievable data transmission rates.

A new development employs continuous variable systems [2–5], such as intense light fields, to obtain shorter key distribution times. The security issues of continuous variable quantum cryptography have been addressed [6,7] and it was proven that the secure key distribution can be achieved using continuous EPR-type correlation or quantum squeezed states.

In this Letter we propose a new key distribution scheme based on the quantum EPR-like correlations of conjugate continuous variables. The main novel feature of the protocol [8] is an assignment of a bit value to the type of measurement. The binary bits are encoded by the choice to detect either of two conjugate variables accomplished independently and randomly by both communicating parties. This serves as a discretization of continuous information in the measurement process. The coincidences in the choices of both parties are revealed by testing the EPR-like correlations between the beams and contribute to the key. Thus, in contrast to other continuous variable systems [2–5], the basis value is not predetermined but develops in measurements at receiver and sender stations, resembling the EPR-based Ekert protocol for discrete cryptographic systems. The detection of light statistics performed by both communicating parties plays a decisive role in the proposed scheme. It comprises bit encoding, key sifting, monitoring of the disturbance in the quantum channel, and active control on timing and information flow during the transmission [9].

The basic ingredient of the scheme is quantum correlations between the amplitude $\hat{X}_j = \hat{a}_j^\dagger + \hat{a}_j$ and phase $Y_j = i(\hat{a}_j^\dagger - \hat{a}_j)$ quadratures of bright beams $j = 1, 2$. Because of the high intensity of the optical fields involved, we use the linearization approach throughout this Letter: $\hat{X}_j = \langle X_j \rangle + \delta\hat{X}_j$, $\hat{Y}_j = \langle Y_j \rangle + \delta\hat{Y}_j$. The entangled observables are then the quantum uncertainties in the respective field quadratures. We start with the definition of the relevant measured quantities and of the conditions for appling the two-mode correlations as a quantum resource. It can be done on the basis of the nonseparability criterion for continuous variables [10,11].

The Peres-Horodecki criterion for continuous variables provides a sufficient condition for a Gaussian state to be nonseparable [10,11]. It can be written in terms of sum or difference squeezing variances [12] of amplitude and phase of two beams:

$$V_{\mathrm{sq}}^{\pm}(X) = \frac{V(\delta\hat{X}_1 \pm g\delta\hat{X}_2)}{V(\hat{X}_{1,\mathrm{SN}} + g\hat{X}_{2,\mathrm{SN}})}, \tag{1}$$

$$V_{\mathrm{sq}}^{\mp}(Y) = \frac{V(\delta\hat{Y}_1 \mp g\delta\hat{Y}_2)}{V(\hat{Y}_{1,\mathrm{SN}} + g\hat{Y}_{2,\mathrm{SN}})}, \tag{2}$$

where $V(A)$ is the variance $\langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2$ of an observable $\hat{A}$. The field modes are denoted by the respective subscripts, SN labels the shot noise limit for a corresponding beam, and g is a variable gain to minimize the variance [12]. In the particular case of entirely symmetrical entangled beams the optimal gain is calculated to be $g = 1$ [11]. The nonseparability of the two-mode quantum state requires then $V_{\mathrm{sq}}^{+}(X) + V_{\mathrm{sq}}^{-}(Y) < 2$ [10,11] and the criterion is necessary and sufficient [11]. From here on we use Eqs. (1),(2) with the signs corresponding to amplitude anticorrelations and phase correlations. The two-mode nonseparable state is said to be *squeezed-state entangled* if the following condition is satisfied for the variances of conjugate variables in Eqs. (1),(2) [13]:

$$V_{\mathrm{sq}}^{+}(X) < 1, \qquad V_{\mathrm{sq}}^{-}(Y) < 1. \tag{3}$$

Note that in contrast to the nonseparability criterion, the introduced squeezed-state entanglement requires both variances of conjugate variables to drop below the respective limit. This requirement is crucial for the suggested cryptographic system and ensures both the possibility to build up a binary key string and the security of a transmission.

A key point for the QKD protocol is sum (difference) measurement (1),(2) testing for the correlation in the

amplitude and phase quadratures. It is used to determine a bit value and it ensures an undisturbed transmission. Suppose Alice and Bob both record the amplitude quadratures of their respective EPR beam. In this case the detected quantum uncertainties $\delta\hat{X}_1$ and $\delta\hat{X}_2$ are anticorrelated [14]. Bob tests for anticorrelations by recording the variance of the sum (1) of photo currents of his and Alice's measurement. Note, however, that the time interval used to experimentally determine the photo current statistics plays a crucial role for the security of the protocol because it may allow for an undetectable eavesdropping (see below). At this stage we explain the protocol in terms of squeezing variances for the sake of clarity in the presentation of main ideas. If there is a nonlocal anticorrelation between δX_1 and δX_2, the sum photo current will drop below the quantum limit, $V_{\mathrm{sq}}^{+}(X) < 1$, to the extent dependent on the quality of the EPR source. Analogously, if there is nonlocal correlation between δY_1 and δY_2 the difference photo current will drop below the quantum limit $V_{\mathrm{sq}}^{-}(Y) < 1$ (2). The quality of the source is limited by the finite degree of continuous quantum correlations $V_{\mathrm{sq}}(X)$, $V_{\mathrm{sq}}(Y)$ (1),(2), perfect correlation requiring infinite energy resources. For the efficiency of transmission, noise and losses in the quantum channel play a significant role. The net quality of both the source and the channel has an impact on the distance, on which the quantum correlations are still reliably observable, on the sensitivity to the disturbance by an eavesdropper, and on possible achievable bit rates.

The obtained constraint $V_{\mathrm{sq}}(X) \ll 1$ and $V_{\mathrm{sq}}(Y) \ll 1$ serve Bob as a criterion for the generation of the sifted key and as a test for eavesdropping. A measured normalized noise power of $V_{\mathrm{sq}}(X) \ll 1$ at Bob's station delivers a bit value "1" and $V_{\mathrm{sq}}(Y) \ll 1$ a bit value "0." The observation of $V_{\mathrm{sq}}(X)$, $V_{\mathrm{sq}}(Y) > 1$ means that both parties have measured different quadratures. These events are discarded. However, Alice and Bob should keep controlling that the overall rate of the event "no correlation" is statistically close to 50% as is inherent to the protocol (X or Y quadrature). $V_{\mathrm{sq}}(X)$, $V_{\mathrm{sq}}(Y) < 1$ to an extent less than expected or no correlations in more than 50% measurements reveals an unexpected disturbance in the line. Note that there is no need to communicate the obtained constraints $V_{\mathrm{sq}} \ll 1$ to Alice.

The quantum key distribution protocol for squeezed-state entangled bright beams based on the measurement of the EPR-like correlations works as follows. The EPR source is at Alice's station (Fig. 1). Alice generates and distributes the entangled beams keeping beam 1 at her station and sending beam 2 to Bob. The relevant measured quantities are the quadrature quantum uncertainties which *a priori* carry no information. To establish the right timing of their recordings Alice and Bob have to synchronize their clocks and agree upon a set of time intervals Δt_k in which they subdivide their measurements. Alice and Bob proceed with a series of measurements.

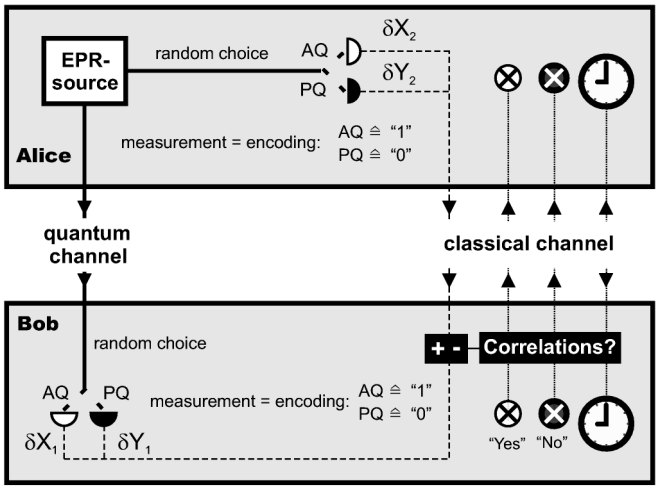

FIG. 1. QKD with bright EPR-entangled beams (see text).

The expected quality of quantum correlations $V_{\mathrm{sq}}(X)$, $V_{\mathrm{sq}}(Y) < 1$ is determined experimentally as described above. Alice and Bob start a key transmission by performing randomly and independently measurements of either amplitude quadrature (AQ) or phase quadrature (PQ) each. Hereby they keep recording (1) their photo currents $(\delta\hat{X}_j, \delta\hat{Y}_j)$, (2) the respective time slots (t_k), and (3) the type of measurement performed (AQ or PQ).

Bob and Alice use two classical communication channels to evaluate the transmission results. Alice permanently keeps sending the results of her measurements, the photo current containing δX_2^k or δY_2^k in the time slots t_k, to Bob via a classical channel I. Bob performs the selection of "good" bits and the security test. To generate the sifted key, he checks correlations between the results of his measurements and the results received from Alice by recording the variance $V_{\mathrm{sq}}^{+}(X)$ (1) of the sum of the relevant photo currents for his choice of AQ or the difference variance $V_{\mathrm{sq}}^{-}(Y)$ (2) for PQ.

After evaluating his correlation measurements (Fig. 1), Bob publicly communicates to Alice via the classical channel II the time points $t_1, t_3, \ldots, t_k$ when he detected correlations (3). The choice of the AQ/PQ measurement is not disclosed. At this stage Alice and Bob can generate the common secret key. They pick up the measurement type (AQ/PQ) from their recordings at the time points $t_1, t_3, \ldots, t_k$ and build the secret key string by association: AQ = bit value 1 and PQ = bit value 0. They discard the rest of the data. The presence of Eve will be revealed by distortion of the correlations or by events "no correlations" occurring statistically more frequent than 50%. This protocol is summarized in Table I.

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. The complete security analysis for the case of continuous variables is nontrivial and lies beyond the scope of the present Letter. It will be

TABLE I. Generation of the common secret key string.

Time	t_1	t_2	t_3	t_4	$\cdots$	t_k
Alice	AQ	PQ	PQ	AQ	$\cdots$	PQ
Bob	AQ	AQ	PQ	PQ	$\cdots$	PQ
Correlation	Yes	No	Yes	No	$\cdots$	Yes
Key	1	$\cdots$	0	$\cdots$	$\cdots$	0

considered elsewhere in terms of mutual information and disturbance of transmission [15] and using noise characteristics like signal-to-noise ratio [9,16]. Here we restrict ourselves to the optical tap attack of an eavesdropper Eve and for an idealized case of lossless quantum channel to illustrate the main security mechanisms. The tapping beam splitter has a transmissivity η.

An eavesdropper Eve will attempt to figure out which quadrature was measured by Alice by tapping the quantum channel and by trying to relate these measurements to the photo currents traveling from Alice to Bob through the classical channel. If Eve has decided to detect the amplitude quadrature by tapping, she has at her disposal the minus and plus channels:

$$V_{\mathrm{sq}}^{\mp}(X_{\mathrm{E}};Z_{\mathrm{A}}) = \frac{V(\delta\hat{X}_{\mathrm{E}} \mp g_{\mathrm{E}}\delta\hat{Z}_{\mathrm{A}})}{V(\hat{X}_{\mathrm{E,SN}} + \hat{Z}_{\mathrm{A,SN}})}, \qquad \hat{Z}_{\mathrm{A}} = \hat{X}_{\mathrm{A}}, \hat{Y}_{\mathrm{A}}. \tag{4}$$

Subscripts E, A denote the quantum uncertainties, measured, respectively, by Eve and by Alice, the upper (lower) sign refers to the minus (plus) channel, and g_{E} is a variable gain used by Eve. To construct the secret key, Eve must be able to distinguish between two possible events: $\delta\hat{Z}_{\mathrm{A}} = \delta\hat{X}_{\mathrm{A}}$ or $\delta\hat{Z}_{\mathrm{A}} = \delta\hat{Y}_{\mathrm{A}}$. An effective strategy for Eve is to check the difference between her plus and minus channels $\Delta = V_{\mathrm{sq}}^{-}(X_{\mathrm{E}};Z_{\mathrm{A}}) - V_{\mathrm{sq}}^{+}(X_{\mathrm{E}};Z_{\mathrm{A}})$. No difference between recordings in these two channels reveals to Eve that she and Alice have measured different quadratures. If Eve records a significant difference Δ, she knows that she and Alice have measured the same quadrature:

$$\begin{aligned}\Delta &= V_{\mathrm{sq}}^{-}(X_{\mathrm{E}};X_{\mathrm{A}}) - V_{\mathrm{sq}}^{+}(X_{\mathrm{E}};X_{\mathrm{A}}) \\ &= g_{\mathrm{E}}\sqrt{(1-\eta)}\,[V_{\mathrm{sq}}^{+}(X) + V_{\mathrm{sq}}^{-}(X)].\end{aligned} \tag{5}$$

Here $V_{\mathrm{sq}}^{+}(X)$ is the normalized sum photo current noise for the amplitude quadratures measured by Alice and Bob during the undisturbed transmission. It is given by the squeezing variance [Eq. (1)] with the optimal gain $g = g_{\mathrm{sq}} = 1$. $V_{\mathrm{sq}}^{-}(X)$ [Eq. (1)] is the difference photo current noise which is recorded in Bob's minus channel for an amplitude measurement. If the beams of Alice and Bob are anticorrelated in the amplitude quadrature, the variance $V_{\mathrm{sq}}^{+}(X)$ is well below unity. Because of the quantum penalty the complimentary variance $V_{\mathrm{sq}}^{-}(X)$ exhibits then substantial excess noise. Equation (5) thus shows that though Eve can split off a small fraction of the signal and process arbitrarily her measurement results which are classical photo currents, she will be limited by inherent noise present in the signal. Eve can amplify her signal using the electronic gain g_{E}, but it will not improve the signal-to-noise ratio of the detected light field.

We discuss now which means Alice and Bob have at their disposal to reveal the malicious disturbance caused by Eve in the quantum channel. First, we review another criterion for quantum EPR-like correlations introduced by Reid and Drummond [12]. For the discussions about this EPR condition and about the nonseparability criterion, see [13,17] and references therein. The EPR criterion refers to the demonstration of the EPR paradox for continuous variables and specifies the ability to infer "at a distance" either of the two noncommuting signal observables with a precision below the vacuum noise level of the signal beam [12]. The relevant inference errors [12] at the optimal gain are the conditional variances:

$$V_{\mathrm{cond}}^{\pm}(X_1\,|\,X_2) = \frac{V(\delta\hat{X}_1 \pm g\,\delta\hat{X}_2)}{V(\hat{X}_{1,\mathrm{SN}})}, \tag{6}$$

$$V_{\mathrm{cond}}^{\mp}(Y_1\,|\,Y_2) = \frac{V(\delta\hat{Y}_1 \mp g\,\delta\hat{Y}_2)}{V(\hat{Y}_{1,\mathrm{SN}})}. \tag{7}$$

The demonstration of the EPR paradox for continuous variables [12,14,18] corresponds to

$$V_{\mathrm{cond}}^{+}(X_1\,|\,X_2)V_{\mathrm{cond}}^{-}(Y_1\,|\,Y_2) < 1. \tag{8}$$

An interesting tool to control the quantum channel is the variable gain g in definition of these conditional variances $V_{\mathrm{cond}}^{\pm}(X_1\,|\,X_2)$ [Eqs. (1),(6)].

Let us consider first the undisturbed transmission with an example of the amplitude measurement performed by Bob. Even for symmetrical squeezed-state entangled beams the optimal gain to minimize the conditional variance $V_{\mathrm{cond}}^{+}(X_1\,|\,X_2)$ [Eq. (6)] differs from unity. It can be expressed as

$$g_{\mathrm{cond}} = \frac{V_{\mathrm{sq}}^{-}(X) - V_{\mathrm{sq}}^{+}(X)}{V_{\mathrm{sq}}^{-}(X) + V_{\mathrm{sq}}^{+}(X)}. \tag{9}$$

With $V_{\mathrm{sq}}^{+}(X) \to 0$, the noise variance in the minus channel $V_{\mathrm{sq}}^{-}(X) \to \infty$ and the optimal gain for $V_{\mathrm{cond}}^{+}(X_1\,|\,X_2)$ is also approaching unity $g_{\mathrm{cond}} \to 1$, like the optimal gain for the squeezing variances [Eqs. (1),(6)].

Consider now how the invasion of an eavesdropper is reflected in the measurements at Bob's station. The sum photo current measured by Bob, $V_{\mathrm{sq}}^{+}(X;\eta)$, becomes more noisy in the presence of Eve:

$$V_{\mathrm{sq}}^{+}(X;\eta) = \frac{(1+\sqrt{\eta})^2}{4}V_{\mathrm{sq}}^{+}(X) + \frac{(1-\sqrt{\eta})^2}{4}V_{\mathrm{sq}}^{-}(X) + \frac{1-\eta}{2} \tag{10}$$

containing $V_{\mathrm{sq}}^{-}(X) \gg 1$. Analogously, the signal in Bob's minus channel, i.e., the variance $V_{\mathrm{sq}}^{-}(X;\eta)$, will also be changed, both plus and minus channels approaching the same limit. Note that Eve should be cautious enough to keep the classical amplitude of Bob's signal unchanged. Bob uses, therefore, the unchanged value of the shot noise

level to which the measured noise variances are normalized to obtain V_{sq} corresponding to $g_{\mathrm{sq}} = 1$.

The modified noise variances in the plus and minus channel $V_{\mathrm{sq}}^{\pm}(X;\eta)$ will be reflected in the optimal gain to minimize the conditional variance g_{cond} (9):

$$g_{\mathrm{cond}}(\eta) = \frac{V_{\mathrm{sq}}^{-}(X) - V_{\mathrm{sq}}^{+}(X)}{V_{\mathrm{sq}}^{-}(X) + V_{\mathrm{sq}}^{+}(X)}\sqrt{\eta}\,. \tag{11}$$

This gain also minimizes the observed unnormalized noise variance $V(\delta\hat{X}_1 \pm g\delta\hat{X}_2)$. If Bob monitors $g_{\mathrm{cond}}(\eta)$ (11) in his measurements, he can easily infer $\eta \neq 1$ in the quantum channel.

An important issue is the finite time for the confident experimental determination of the squeezing variance. To gain some partial information, when decoding V_{sq} Eve might go for less time than both legitimate communicating parties, accepting less confidence in determining the variance. She will tap the signal for a fraction of Bob's measurement time and hence will introduce less disturbance as expected for a given beam splitting ratio. The losses in the channel reduce the correlations and enhance the time needed for the determination of the variance with sufficient precision. If Eve is tapping close to Alice, where the impact of losses is still negligible, she can additionally profit from less time needed for her measurement compared to that of Bob with a given confidence level. The optimum strategy for Alice and Bob seems to be to operate with as short a measurement time as possible, ultimately with single measurements. The above statistical analysis in terms of variances should therefore be extended to cope with single shot measurements. This, however, is beyond the scope of discussion presented here and will be considered in detail elsewhere.

To summarize, the scheme presented here possesses several novel features and shows the strong sides of continuous variable cryptography. The effect of losses on the maximum possible transmission distance will have to be studied further. The bit value is encoded by the type of measurement, i.e., by the choice of measured observable amplitude or phase. The information on the key is thus emerging only *a posteriori,* at sender and receiver stations. One of the advantages of the presented scheme is the high value of the achievable effective bit rates. For example, for the pulsed EPR source the principal theoretical limit is given by half of the repetition rate R_{rep}, the factor $\frac{1}{2}$ being inherent to the protocol and realistic values of R_{rep} reaching up to 100 GHz. The implementation of the scheme with bright EPR-entangled beams [14] is experimentally simple and robust and well suited for both fiber-integrated or free-space transmission.

This work was supported by the Deutsche Forschungsgemeinschaft and by the EU grant under QIPC, Project No. IST-1999-13071 (QUICOV). The authors gratefully acknowledge fruitful discussions with T. C. Ralph, N. Lütkenhaus, Ph. Grangier, R. Loudon, and S. Lorenz.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098.
[2] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[3] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[4] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
[5] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[6] T. C. Ralph, Phys. Rev. A **62**, 062306 (2000).
[7] D. Gottesman *et al.,* Phys. Rev. A **63**, 022309 (2001).
[8] Ch. Silberhorn, N. Korolkova, and G. Leuchs, in *Proceedings of the 2000 International Quantum Electronics Conference: Conference Digest, Nice, France, 2000* (IEEE, Piscataway, NJ, 2000), p. 8.
[9] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs (to be published).
[10] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[11] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[12] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); M. D. Reid, Phys. Rev. A **40**, 913 (1989); J. Mod. Opt. **46**, 1927 (1999).
[13] G. Leuchs, Ch. Silberhorn, F. König, A. Sizmann, and N. Korolkova, in Quantum Information Theory with Continuous Variables, edited by S. L. Braunstein and A. K. Pati (Kluwer Academic Publishers, Dordrecht, to be published).
[14] Ch. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001).
[15] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996); D. Bruß and N. Lütkenhaus, quant-ph/9901061.
[16] T. C. Ralph, in Quantum Information Theory with Continuous Variables (Ref. [13]).
[17] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001); S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, quant-ph/0012001.
[18] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).