Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection

S. Lorenz,[1] J. Rigas,[2] M. Heid,[2] U. L. Andersen,[1] N. Lütkenhaus,[2] and G. Leuchs[1]
[1]*Institute of Optics, Information and Photonics, Universität Erlangen–Nürnberg, Günther-Scharowsky-Straße 1/Bau 24, D-91058 Erlangen, Germany*
[2]*Institute of Theoretical Physics I, Universität Erlangen–Nürnberg, Staudtstraße 7/B2, D-91058 Erlangen, Germany*
(Received 14 March 2006; published 24 October 2006)

We report an experimental demonstration of effective entanglement in a prepare-and-measure type of quantum key distribution protocol. Coherent polarization states and heterodyne measurement to characterize the transmitted quantum states are used, thus enabling us to reconstruct directly their Q function. By evaluating the excess noise of the states, we experimentally demonstrate that they fulfill a nonseparability criterion previously presented by Rigas *et al.* [J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006)]. For a restricted eavesdropping scenario, we predict key rates using postselection of the heterodyne measurement results.

DOI: 10.1103/PhysRevA.74.042326 PACS number(s): 03.67.Mn, 42.50.Lc, 42.25.Ja, 03.67.Dd

I. INTRODUCTION

The process of quantum key distribution (QKD) [1,2] uses quantum-mechanical properties of light fields to establish a secret shared key between two honest parties, named Alice and Bob. This key is then used to ensure secret communication between Alice and Bob by means of a classical cipher such as the one-time-pad [3]. The adversary of Alice and Bob is an eavesdropper Eve, who tries to gain maximum knowledge about the key without being noticed by Alice and Bob. Eve can use any method within the laws of quantum mechanics, and therefore is not restricted by technological imperfections.

The physical implementation of a QKD protocol requires two channels between Alice and Bob. Over the *quantum channel*, Alice and Bob can exchange quantum states. By the laws of quantum mechanics, Alice and Bob are able to detect any interference of Eve with the quantum states. Classical information is exchanged on the *classical channel*. This channel has to be authenticated in order to prevent a man-in-the-middle attack by Eve.

After the quantum states have been exchanged over the quantum channel, they are measured by Bob. Alice and Bob keep the results of the preparation process and the measurement process, thus sharing a set of classical correlated measurement data described by the joint probability distribution $p(A;B)$. This is the first stage of the QKD protocol. In the second stage, Alice and Bob try to generate a key pair from their correlations $p(A;B)$ and correct possible errors. From the disturbance of the correlations they deduce the amount of information Eve might have on the key pair, and reduce Eve's information by privacy amplification. For these tasks, only communication over the classical channel is needed, as all exchanged information is classical. If the QKD is successful, Alice and Bob will share a key and have an upper bound on the information Eve might have about it.

Most practical experimental QKD schemes do not use sources that produce entangled states as such. Instead, they prepare and measure schemes where one sends signals chosen from a set of nonorthogonal signals from Alice to Bob. Clearly, no physical entanglement is present. However, one can introduce entanglement concepts through the back door: Any source preparing nonorthogonal signals can be thought of as employing a specific entangled state internally, so that some measurement on one subsystem produces conditional states of the other subsystem corresponding to the desired nonorthogonal signal states (and the right *a priori* probabilities). This will be explained in more detail for our specific situation in Sec. II. Once the signals have been sent to Bob via the quantum channel, we can therefore think about the situation as if Alice and Bob share effectively a bipartite quantum state. It has been shown by Curty *et al.* [4,5] that there is a necessary precondition for the second stage of QKD, the public discussion stage, to succeed: using the correlations $p(A;B)$ coming from the first stage, one has to be able to verify the entanglement of the effective bipartite state shared between Alice and Bob. Only then will it be possible to generate a secret key from the data set. Again, this "effective entanglement" does not mean that entanglement as a physical resource has to be used in the state preparation step. It is sufficient that Alice and Bob can model their correlations as if they had shared an entangled state. In our approach, we use an entanglement witness to check if the correlations show effective entanglement.

In the absence of full security proofs for a given QKD scheme, the verification of this necessary precondition is an important step to demonstrate that there is a potential to create secret keys. Indeed, had this step been applied to weak-coherent pulse implementations of the BB84 protocol, one would have seen much earlier that some combinations of reported mean photon number and channel transmittivities cannot lead to secure keys at all, even before actual security proofs for some suitable parameter combinations became available. Note that the search for virtual or real entanglement is not only important for QKD, but can also be relevant to demonstrate the presence of quantum effects in setups for other quantum communication tools, such as quantum teleportation.

In this paper, we demonstrate the effective entanglement for a particular prepare-and-measure setup, which uses the

polarization of coherent light pulses to generate nonorthogonal quantum states. The pulses are characterized by a heterodyne measurement [6] on Bob's side, allowing for a reconstruction of their antinormal ordered quasidistribution, or Q function [7]. We show for this particular system that we can prove effective entanglement for the prepared quantum states using a model developed by Rigas *et al.* [8,9]. Thus, clearly it has the potential of generating secret keys. The idea is to combine the advantage of continuous variable detection (here heterodyne measurement) with a small set of signal states, which, in a full security analysis, will simplify the analysis of statistical errors. Following this, we use a reasonable model to predict expected key rates for a classical key generation process with the data obtained in stage 1 of the experiment. It considers postselection [11] with direct or reverse reconciliation [12,34] of the measurement data. This QKD protocol is known to be secure against an adversary Eve who is restricted to beam splitting attacks [13].

The paper is divided into five subsections. In Sec. II, we briefly introduce the theoretical background of the entanglement verification process, as it is described by Rigas *et al.* [8,9]. We also present the QKD quantum state protocol there. In Sec. III, we give a characterization of the experimental apparatus, which implements the quantum stage of the QKD system. Section IV shows how the Q function can be experimentally reconstructed and how the effective entanglement of the QKD setup can be verified. Section V gives achievable key rates for our experiment applying a postselection procedure.

II. PREPARE-AND-MEASURE QUANTUM KEY DISTRIBUTION AND VERIFICATION OF EFFECTIVE ENTANGLEMENT

The existing QKD systems fall into two categories: entanglement-based systems and prepare-and-measure systems. For a review on both, see, e.g., [14]. In entanglement-based systems, a bipartite entangled state is produced by a source that might even be under Eve's control. One part of the entangled state is then sent to Alice while the other is sent to Bob. Here Alice and Bob can directly verify the entanglement of the state, thus bounding any interaction of Eve [15]. Then privacy amplification can be understood as an entanglement distillation (see, e.g., Shor and Preskill [16]).

In a prepare-and-measure system Alice prepares a quantum state and sends it through the quantum channel to Bob [2,17]. He characterizes the quantum state, and from Alice's preparation and Bob's measurement results they estimate Eve's action and information on the quantum state. As sources of entangled states are hard to implement and suffer from technical disadvantages, we use the latter approach in our experiment, which ensures stable, deterministic state preparation with minimum resources.

In our protocol, Alice encodes her bit values into two nonorthogonal states as in the B92 protocol [17]. In particular, she prepares coherent states with the amplitudes $-\alpha$ or $+\alpha$. A general coherent state can be described in a Fock state basis by

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{1}$$

where n is the photon number and $|n\rangle$ is a photon number eigenstate. The set of coherent states constitutes an overcomplete basis, and the overlap between any two coherent states with amplitudes α and β is given by

$$\langle \beta | \alpha \rangle = e^{-(1/2)|\beta - \alpha|^2}. \tag{2}$$

Thus it is impossible to discriminate between the coherent states $|-\alpha\rangle$ and $|+\alpha\rangle$ with certainty [18–21]. The coherent states emitted by Alice are transmitted through the quantum channel, which is under the control of the eavesdropper Eve. She can manipulate the states and adjust the channel properties to get an advantageous position in the key generation process. As the states enter Bob's measurement station, he performs a heterodyne measurement [6], in contrast with the original B92 setup, where a photon counter is used to discriminate between the different states. The heterodyne measurement splits the optical mode on a 50/50 beam splitter and measures the two conjugate field quadratures on its outputs with two homodyne detectors. This measurement of two conjugate observables (see, e.g., [22,23]) corresponds to a projection on coherent states. The quadrature operators are derived from the creation and annihilation operators $a^\dagger$ and a by

$$\mathbf{X} = \frac{1}{2}(a^\dagger + a), \quad \mathbf{Y} = \frac{i}{2}(a^\dagger - a). \tag{3}$$

Bob records the results of the heterodyne measurement in a two-dimensional histogram, which represents the Q function [7,24–28],

$$Q(\mathrm{Re}\ \beta; \mathrm{Im}\ \beta) = \frac{1}{\pi} \langle \beta | \rho | \beta \rangle. \tag{4}$$

Here, the general state ρ is projected onto the coherent state $|\beta\rangle$.

To model the prepare-and-measure setup with effective entangled states, we follow Bennett *et al.* [29] and assume that Alice possesses a source of bipartite quantum states given by

$$|\Psi\rangle_{\mathrm{Alice}\to\mathrm{Bob}} = \frac{1}{\sqrt{2}} |\Psi_0\rangle_{AB} + \frac{1}{\sqrt{2}} |\Psi_1\rangle_{AB}, \tag{5}$$

whereas the states $|\Psi_{0,1}\rangle_{AB}$ are given by

$$|\Psi_0\rangle_{AB} = |0\rangle_{\mathrm{Alice}} \otimes |-\alpha\rangle_{\mathrm{to\ Bob}},$$

$$|\Psi_1\rangle_{AB} = |1\rangle_{\mathrm{Alice}} \otimes |+\alpha\rangle_{\mathrm{to\ Bob}}. \tag{6}$$

The model setup is shown in Fig. 1. Alice keeps the first part of the state, which consists of a qubit, and sends the other part of the state over the quantum channel to Bob. By detecting her qubit, Alice effectively prepares a coherent state of amplitude $-\alpha$ or $+\alpha$ as a signal. Thus, conditioned on her qubit measurement result, Alice produces a certain coherent state. As her measurement result, 0 or 1, is occurring completely randomly, but also completely correlated with the

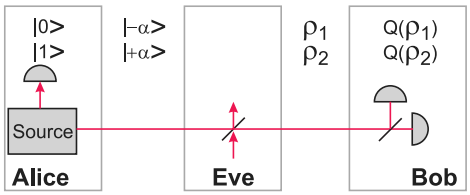

FIG. 1. (Color online) Simplified theoretical setup.

generated coherent state, the entanglement source resembles the random production of coherent states with amplitudes $-\alpha$ or $+\alpha$. In reality, such a random production of coherent states can be enabled without the use of an entanglement source, but in the theoretical description there is no difference between these two physical systems.

The coherent states travel over the quantum channel, where Eve can interact with them. Also channel losses are attributed to Eve, as she can always replace a lossy channel with a lossless one and tap off the surplus intensity. When Eve has interacted, the pure coherent states might have changed to more general mixed states described by the density matrices ρ_1 and ρ_2. From the results of the heterodyne measurement, Bob can reconstruct the Q-function, and deduce the quadrature variances $\Delta^2\mathbf{X}=\langle\mathbf{X}^2\rangle-\langle\mathbf{X}\rangle^2$ and $\Delta^2\mathbf{Y}=\langle\mathbf{Y}^2\rangle-\langle\mathbf{Y}\rangle^2$ and all other elements of the covariance matrix.

As the full joint density matrix of Alice and Bob is not accessible by heterodyne measurements and dichotomic preparation, we revert to the *bipartite expectation value matrix* defined in [9] to describe the state shared by Alice and Bob. It consists of a part A describing Alice's state preparation, and a part **B** describing Bob's heterodyne measurement,

$$\chi=\begin{bmatrix}\langle|0\rangle\langle 0|_A\otimes\mathbf{B}\rangle & \langle|1\rangle\langle 0|_A\otimes\mathbf{B}\rangle\\ \langle|0\rangle\langle 1|_A\otimes\mathbf{B}\rangle & \langle|1\rangle\langle 1|_A\otimes\mathbf{B}\rangle\end{bmatrix}, \tag{7}$$

with the matrix **B** composed of the quadrature operators directly accessible to Bob,

$$\mathbf{B}=\begin{bmatrix}1 & X & Y\\ X & X^2 & \frac{1}{2}(XY+YX)\\ Y & \frac{1}{2}(XY+YX) & Y^2\end{bmatrix}. \tag{8}$$

It has been shown that some classes of observed expectation value matrices can be explained only by underlying entangled states. The derivation of the corresponding criteria [9] is based on the partial transposition criteria [10]. The criteria give already useful information given only the knowledge of the overlap of the signal states and the expectation values corresponding to the matrix **B** of the two conditional signal states arriving at Bob's receiver. By proving effective entanglement from the experimental data, we fulfill the first precondition in order to be able to generate a secret key from Alice's and Bob's correlations [4,5]. The separability condition can be evaluated by semidefinite programming [30], giving an upper bound on the tolerable noise $\Delta^2\mathbf{X},\Delta^2\mathbf{Y}$ below which the effective entanglement can be verified. This bound depends on the input state overlap $\langle-\alpha|+\alpha\rangle$ and the

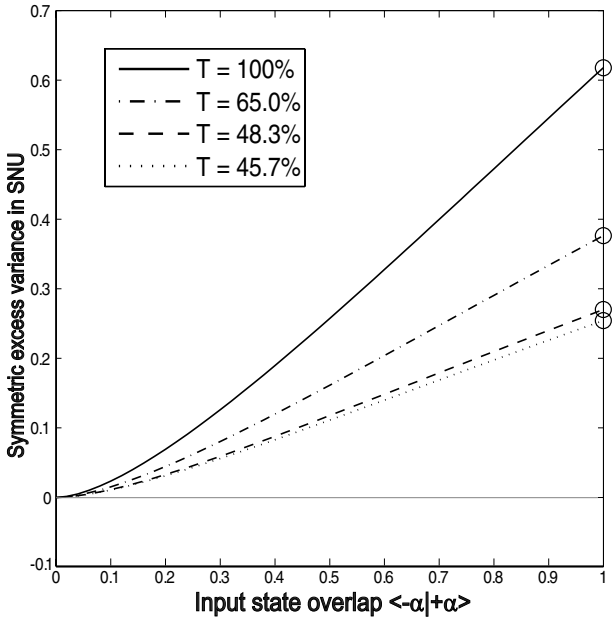

FIG. 2. Graphical representation of the entanglement criterion. For excess variances E [in shot noise units (SNU)] below the curves, the correlated data $p(A;B)$ cannot be explained by separable states. Zero excess variance corresponds to the detection of a pure coherent state. Different curves belong to different quantum channel transmissions T. The input state overlap depends only on Alice's choice of the coherent state amplitude α, and not on the channel transmission.

quantum channel loss. We define the excess noise or excess variance E of an observable **X** for a signal state by comparing its variance to the variance of a coherent vacuum state (shot noise) as

$$E(\mathbf{X})=\frac{\Delta^2\mathbf{X}(\text{signal})}{\Delta^2\mathbf{X}(\text{vacuum})}-1. \tag{9}$$

Figure 2 shows the numerically calculated bounds to the excess variance for different quantum channel transmissions. All experimental excess variances that are below their corresponding bounds fulfill the nonseparability condition and thus the scheme exhibits effective entanglement.

III. EXPERIMENTAL APPARATUS

The experimental setup deviates from the theoretical description in the previous section in one aspect. To determine the quadratures **X** and **Y**, Bob has to use a phase reference as a local oscillator for the homodyne measurements [6,31]. This phase reference is sent along with the signal state in our experiment, as it is done in most continuous-variable quantum cryptography experiments [32–36,38].

The reported theoretical analysis of quantum correlations does not apply to this experimental setup as such, as it would mean that Eve cannot manipulate the reference pulse. However, one can think about a setup that either reloads the phase of the reference phase via classical phase estimation into a local oscillator (as used in [39]), or one that directly uses

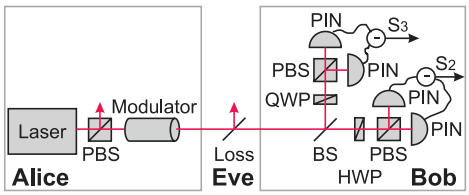

FIG. 3. (Color online) Simplified experimental setup. Alice prepares coherent polarization states with a cw laser diode and a Faraday modulator. Bob characterizes the incoming light by a heterodyne measurement consisting of two polarization sensitive homodyne setups. Eve is simulated by changing the loss of the quantum channel.

classical synchronization of the local oscillators. Both methods are not as practical as desired. Moreover, one does not expect that Eve indeed obtains a noticeable advantage in the actual experiment. Therefore, we now *assume* that the local oscillator is not manipulated by Eve in any way.

Consequently, our experimental realization of the quantum channel has to transmit two light modes: the signal field mode **a** contains the weak coherent pulses in which the quantum information is encoded. The local oscillator mode **b** is needed in the heterodyne measurement of the signal mode as a phase reference. We have a free-space implementation in mind, and therefore, instead of using two spatially separated channels to transmit the two modes, we use two orthogonal polarization modes as representing the two fields in one spatial mode. This facilitates the generation of the signal states as well as providing high-quality interference of the two modes at the heterodyne detector. If one aims at fiber-optics implementations, however, this polarization encoding is not a good choice; instead, one would encode the two modes into two time separated modes in the fiber. The amplitude and relative phase of our two orthogonal polarization modes can be described by the Stokes parameters [40] or by the Stokes operators [41–43] in quantum theory. In our notation, they read

$$\mathbf{S}_0 = a^\dagger a + b^\dagger b, \tag{10}$$

$$\mathbf{S}_1 = a^\dagger a - b^\dagger b, \tag{11}$$

$$\mathbf{S}_2 = a^\dagger b + b^\dagger a, \tag{12}$$

$$\mathbf{S}_3 = -i(a^\dagger b - b^\dagger a). \tag{13}$$

The intensity in the local oscillator mode **b** is always much larger than the intensity in the signal mode **a**, thus we have $\langle S_0\rangle \simeq -\langle S_1\rangle \gg 1$, $\langle S_2\rangle \approx 0$, $\langle S_3\rangle \approx 0$. The relative phases and amplitudes of the polarization modes can be manipulated with birefringent optical elements and polarizing beam splitters.

A schematic drawing of our setup is shown in Fig. 3. An external cavity laser diode emits continuous wave light at 810 nm, and by a polarizing beam splitter acting as a polarization filter, a coherent bright state is created in the local oscillator mode **b** whereas the signal mode **a** is in the vacuum state. The light passes through a magneto-optical modulator that utilizes the Faraday effect to alter the polarization state [44]. Depending on the externally applied magnetic field, the modulator rotates a linearly polarized input field and shifts the phase of circular polarized fields. The light polarization can be varied continuously from $\mathbf{S_1}$-polarized to $\mathbf{S_2}$-polarized, which corresponds to equal optical power in the **a** and the **b** modes. In our case, we only induce a very tiny modulation, such that for the optical powers P_a, P_b in the two modes $P_b \gg P_a$ is always satisfied. The modulation is applied in pulses of 5 μs duration, either with parallel or antiparallel magnetic-field orientation, such that either the state $|+\alpha\rangle$ or the state $|-\alpha\rangle$ is produced in the **a** mode. The state overlap $\langle +\alpha|-\alpha\rangle = e^{-2|\alpha|^2}$ is in the range from 0.2 to 0.8. When encoding the signal, the intensity in the local oscillator mode is reduced only by a negligible amount (intensity variations are smaller than 10^{-9} in our experiment). Therefore, a local oscillator of constant power can be assumed. As the signal field is derived from the local oscillator field through modulation, the relative phase of both fields is constant, even though the laser phase might suffer from fluctuations.

The beam is then directed to Bob, traveling through Eve's domain over a free space link of approximately 20 cm. Various quantum channel transmissions can be simulated by using neutral density filters to equally attenuate both modes **a** and **b**.

In Bob's receiver, the incoming beam undergoes a heterodyne measurement. It is split on a polarization independent 50/50 beam splitter, and both parts are directed to individual homodyne measurement setups, which record the $\mathbf{S_2}$-polarization and $\mathbf{S_3}$-polarization, respectively. This is done by interfering the signal and the local oscillator modes on a beam-splitter and subsequently recording the intensity difference at the beamsplitter output ports [31,45,46]. As long as the local oscillator mode is much brighter than the signal mode, the difference photocurrent I corresponds to

$$I \propto \sqrt{P_b}\sqrt{P_a}\cos\phi \tag{14}$$

with P_b being the local oscillator optical power and P_a the signal optical power, and ϕ the relative phase between signal and local oscillator. The relative phase of signal and local oscillator in our setup is controlled by the appropriate choice and setting of half-wave plates (HWP, $\mathbf{S_2}$ measurement) and quarter-wave plates (QWP, $\mathbf{S_3}$ measurement). The two modes interfere at polarizing beam splitters. As both the signal and the local oscillator are in the same spatial mode, a very high interference contrast can be achieved. We record a polarization contrast larger than 10^4, corresponding to an interference visibility larger than 99.9%. Both homodyne detector voltages are sampled with a fast A/D converter. Figure 4 shows 10 superimposed test pulses with high amplitude in the **a** mode. Each point corresponds to one sample. It can be seen that one polarization pulse is much longer than one sample period. The variance of the sampled data is an indicator for the shot noise of the signal light mode. For the experiments, a sample rate of 20×10^2 samples/s and a pulse duration of 5 μs was chosen. Consequently, an integration over 100 samples defines our pulse amplitude. The electronic and dark noise of the detectors is more than 14 dB below the signal

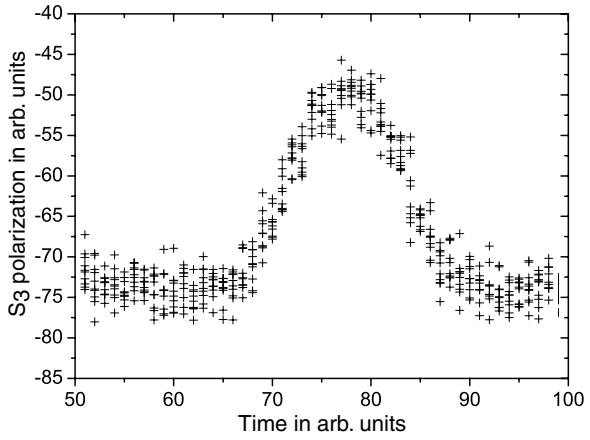

FIG. 4. Demonstration of a detected signal in the time domain. Ten identical measurements were superimposed to show the variations in detector voltage due to quantum noise. The pulse duration was set to 50 μs at a sample rate of 1×10^2 samples/s to better visualize the pulse shape and the discrete nature of the sampled data. In the further experiments, a pulse duration of 5 μs was used.

noise in a frequency window from 100 Hz to 2 MHz with a local oscillator power of P_b=1.2 mW. Dark noise at higher frequency is filtered by a 2 MHz low pass filter. From the pulse amplitudes, the quadratures and polarizations are calculated by measuring the local oscillator power and the detector transimpedance (approximately 110 kΩ) as well as the diode quantum efficiencies (91% ±3.5%).

With the pulse separation of 10 μs, a clock rate of 100 $\times10^3$ pulses/s is feasible. As we characterized five vacuum noise time slots for each bright signal pulse, the effective clock rate for signal pulses was reduced to 16.7 $\times10^3$ pulses/s for the Q function and effective entanglement measurements. In the real QKD system, the vacuum characterization is only needed for an initial calibration, and the full clock rate can be used for pulse transmission subsequently.

A whole measurement sequence consists of 250 000 signal pulses. A histogram of recorded pulse amplitudes in the $\mathbf{S_2}$ polarization (corresponding to a 0 or π phase shift between signal mode **a** and local oscillator mode **b**) is shown in Fig. 5. The shot noise reference in this demonstration is produced with no modulation current (vacuum mode) and is shown in black (dotted) [53]. The gray histogram is derived from the signal pulses with amplitudes $-\alpha$ and $+\alpha$. The overlap of the two resulting Gaussian distributions is too high to distinguish between them in this histogram, the only visible effect being a decrease in peak height and an increase in variance.

The variances of the polarization (or quadrature of the **a** mode) measurement can be used to calculate the appropriate entries of the χ matrix [cf. Eq. (7)]. We reconstructed the Q function of the state entering Bob's measurement apparatus by building a histogram of the $\mathbf{S_2}$ and $\mathbf{S_3}$ values and renormalizing the volume of the resulting two-dimensional function. As this apparatus is not lossless due to experimental imperfections, as in all tomography experiments, our recorded functions are rather convolutions of the Q function with a Gaussian function defined by the detection loss. This loss consists of optical losses and nonunit quantum efficiency of the detector, and sums up to 13.6%. Thus, also the peak height of our Q functions does not reach π^{-1} as it would after Eq. (4), but a somewhat lower value even for pure states. It is assumed, however, that these losses cannot be actively used by Eve, as they appear in Bob's domain and can be monitored by him. For the entanglement criterion, the excess noise variance [cf. Eq. (9)] is used, which compares the signal variance with the vacuum variance. As the vacuum variance is determined with the same setup, the detection losses are not regarded in further analysis.

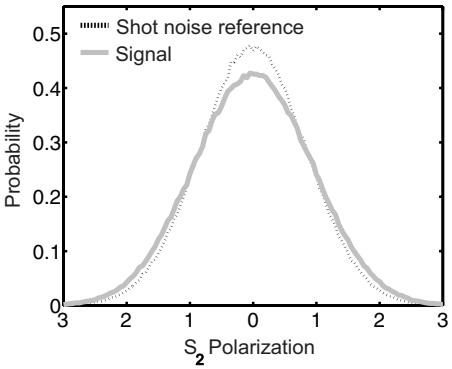

FIG. 5. Marginal distribution of the measured dimensionless polarization values. The dotted black curve represents the shot noise reference, recorded with vacuum in the signal mode a_S. The solid gray curve is Bob's measurement value histogram for two alternating states, corresponding to Fig. 9 and the highlighted line in Table I.

IV. RESULTS

The restrictions for the quadrature variances given by the entanglement criterion of Rigas *et al.* [9] are shown in Fig. 6 for the relevant parameter range. The curve shows the maximum measured excess variance E compared to the coherent

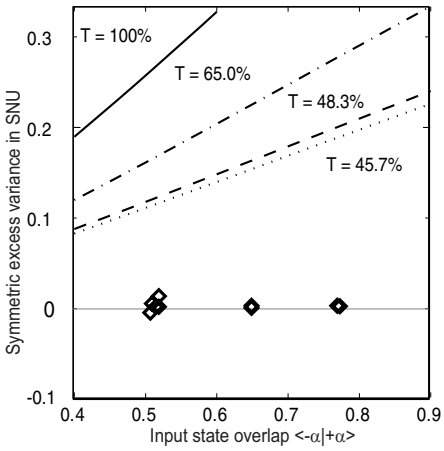

FIG. 6. Graphical representation of the entanglement criterion. For excess variances below the curves, the correlated data $p(A;B)$ cannot be satisfied by separable states. Different curves correspond to different quantum channel losses. The open diamonds show measured averages of $E(\mathbf{S_2})$ and $E(\mathbf{S_3})$; their numerical values can be seen in Table I.

TABLE I. Excess variances E for the coherent state measurement, depending on state overlap and quantum channel transmission. The statistical error is ±0.5 for $E(\mathbf{S_2})$ and ±0.3 for $E(\mathbf{S_3})$. The last column gives the excess variance with the electronic noise subtracted only from the shot noise reference, which refers to a worst case scenario. The highlighted line shows the data set that produced the Q function in Fig. 9 and the marginal distribution in Fig. 5.

State overlap $\langle -\alpha \vert +\alpha\rangle$	Quantum channel transmission T	Excess variance $E(\mathbf{S_2})$	Excess variance $E(\mathbf{S_3})$	$E(\mathbf{S_2})$ with electronic noise subtracted
0.51	100%	0.8%	0.1%	4.5%
0.50	**45.7%**	**0.2%**	**–0.3%**	**8.3%**
0.78	100%	–0.2%	–0.2%	3.5%
0.77	45.7%	0.3%	0.1%	8.3%
0.52	100%	1.6%	0.1%	5.3%
0.52	48.3%	0.2%	0.3%	7.7%
0.51	65.0%	0.2%	0.0%	5.8%
0.65	100%	0.6%	-0.5%	4.2%
0.65	48.3%	0.1%	0.0%	7.5%

vacuum state, which is tolerable without having a separable state. As it can be seen, all measurement results (diamonds) lie below this threshold. Therefore, the joint probability distribution can only be explained by effective entanglement in the whole shared state between Alice and Bob. Numerical values are compiled in Table I. For each measurement, a separate evaluation of the vacuum variance (shot noise level) was calculated from the vacuum pulses transmitted during the measurement. The state overlap prepared by Alice is shown in the first column. The second column gives the quantum channel transmission, where losses in Bob's detection unit are not taken into account. The third column gives the excess variance $E(\mathbf{S_2})$ of Bob's polarization measurements compared to the vacuum variance. The fourth column gives the excess variance $E(\mathbf{S_3})$ of the $\mathbf{S_3}$ polarization. Apart from one value, all excess variances fall well below 1%, whereas more than 10% are enough to prove effective entanglement with the given quantum channel transmissions. Note that negative excess variances are no sign of nonclassical states but represent the statistical variations due to the finite sample size. The average excess variance is given by $E(\mathbf{S_2})=0.4\pm0.5\%$ and $E(\mathbf{S_3})=0.0\pm0.3\%$. Additionally, to give a conservative estimate on the impact of electronic noise on our measurement results, we subtracted the variance of the electronic noise *only* from the shot noise reference. The excess variances that are compared to this corrected vacuum state are given in column five. They are all still below 9%. Even with this conservative correction, we witness the presence of effective entanglement.

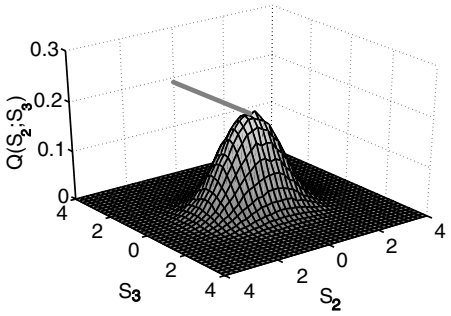

FIG. 8. Mixed Q function of the two signal states ρ_1 and ρ_2 after leaving Alice's preparation.

Figure 7 shows the reconstructed Q function of the vacuum state. This function is a direct histogram, and has not been smoothed or fitted. In Fig. 8, we depict the Q function of the mixed state $\rho=\frac{1}{2}|+\alpha\rangle\langle+\alpha|+\frac{1}{2}|-\alpha\rangle\langle-\alpha|$ with an overlap $\langle-\alpha|+\alpha\rangle=0.51$ measured with no channel loss. From the figure, it can be seen that the height of the Q function is an indicator of mixedness of the depicted state. Here the mixture of ρ_1 and ρ_2 states with no additional quantum channel loss gives a Q function with a peak height that is distinctively less than that of the pure vacuum state. After a loss of 54.3%, the mixedness of the state is decreased (cf. Fig. 9). This Q function corresponds to the highlighted line in Table I and the gray histogram in Fig. 5.

If Alice reveals to Bob which pulse belonged to the state $|\Psi_0\rangle_{AB}$ and which to the state $|\Psi_1\rangle_{AB}$, Bob can produce two histograms. They are both shown in Fig. 10. The two Gaussian distributions represent the states Bob receives of $|\Psi_0\rangle_{AB}$ ($\rho_1=|-\alpha\rangle\langle-\alpha|$ ideally) and of $|\Psi_0\rangle_{AB}$ ($\rho_2=|+\alpha\rangle\langle+\alpha|$ ideally). The overlap increases as losses are introduced. Figure 11 shows the two states' Q functions after 54.3% losses. The

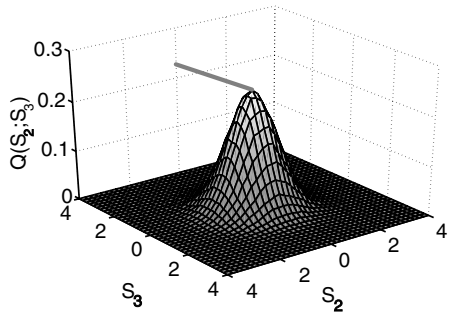

FIG. 7. Vacuum noise Q function. $\mathbf{S_2}$ and $\mathbf{S_3}$ are proportional to the $\mathbf{X}$ and $\mathbf{Y}$ quadrature of the signal mode a. The peak height is indicated by the gray line. Note that all displayed quantities are dimensionless.

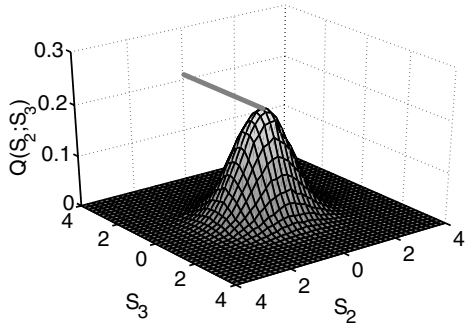

FIG. 9. Mixed Q function of the two signal states ρ_1 and ρ_2 in balanced mixture after experiencing 54.3% of channel loss. This Q function corresponds to the highlighted line in Table I.

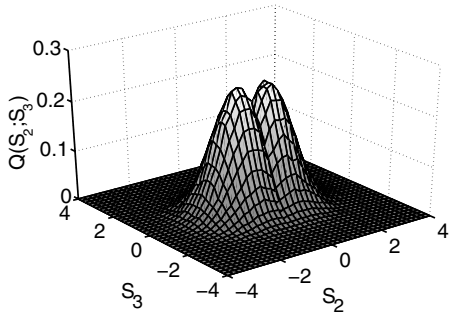

FIG. 10. Both Q functions of the ρ_1 and the ρ_2 state, measured directly after preparation. This figure corresponds to Fig. 8.

two Gaussians moved closer together and the overlap has increased. In the ultimate limit of 100% loss, a pure vacuum state (cf. Fig. 7) would be registered by Bob.

V. APPLICATION TO A CONTINUOUS VARIABLE QKD SCHEME

We now use our prepare-and-measure system for a specific quantum key distribution protocol. Alice prepares either the coherent state $|+\alpha\rangle$ or $|-\alpha\rangle$ as a signal. As shown in the previous sections, Alice and Bob can verify the entanglement in their virtually shared state by simultaneously measuring both quadratures (or polarizations) and thereby recording the Q function of the received states. In this section, we want to demonstrate a key generation system, which is based on postselection of Bob's measurement results. The idea of postselection of continuous variable data was introduced by Hirano *et al.* [32] and Silberhorn *et al.* [11]. The implementation with a discrete set of states was demonstrated in [32,47]. The idea for the simultaneous measurement setup was already demonstrated in [35] and further elaborated in [36].

To estimate the efficiency of our experiment of generating key pairs, we make three assumptions. The first concerns the excess noise produced by the quantum channel. We have shown in the previous section that this excess noise is always less than 0.02 shot noise units and that we are clearly within the regime of quantum correlations. We expect that the influence on the key rate is small for these values of the channel

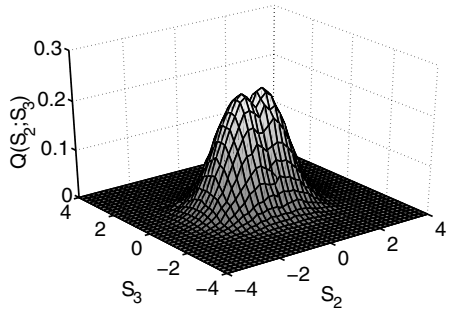

FIG. 11. Both Q functions of the ρ_1 and the ρ_2 state, measured after propagation with 54.3% losses. This figure corresponds to Fig. 9.

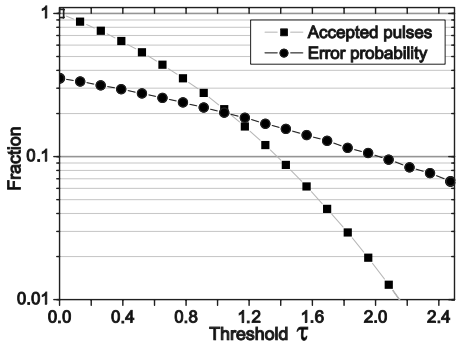

FIG. 12. Experimental analysis of relative acceptance and average error rate depending on the postselection threshold. Open squares: Fraction of accepted states after applying a postselection threshold of τ. Black circles: remaining average error rate in the postselected pulses. This measurement was produced with a channel loss of 51.7% (cf. Table I, last line).

excess noise. Therefore, we neglect this excess noise in a first approximation and assume a noiseless quantum channel. A full security analysis, however, will have to take noisy quantum channels into account.

The second assumption concerns the local oscillator. As already mentioned in Sec. III, we transmit the local oscillator mode and the signal mode through the quantum channel, and manipulate both by polarization optics. We assume also in this section that the classical local oscillator mode is not manipulated by Eve.

Our third assumption is that Eve performs a collective attack, which consists of an individual interaction of Eve's ancilla states with the signals and a coherent measurement onto those states. Eve is allowed to delay her measurement after the classical postprocessing step in the protocol is completed to optimize her attack. In this scenario, a lower bound on the secret key rate G is then given by Devetak and Winter [48],

$$G \geqslant I_{A:B} - \chi_{\text{Holevo}}, \tag{15}$$

whereas $I_{A:B}$ denotes the mutual information between Alice and Bob. The Holevo quantity χ_{Holevo} is a function of the states that Eve holds and quantifies her knowledge about the data [37].

With these assumptions, we estimate the secret key rate while using either direct or reverse reconciliation combined with postselection. The estimation of the key rates is based on the derivation given in [13]. In a reverse reconciliation scheme, the key is built from Bob's measured data to improve the key rate [34]. This can be achieved by using suitable one-way protocols in the classical postprocessing phase of the protocol.

The characteristic effect of postselection on the data rate can be seen from Fig. 12. The experimental measurement data from the last line in Table I are used to demonstrate the general effect of postselection on a joint probability distribution $p(A;B)$ derived from our experiment. After the postselection step, Alice and Bob share correlated data from which they deduce a binary raw key by assigning a "0" bit value to negative measurement results, and a "1" bit value to positive

measurement results. The x axis of Fig. 12 shows the postselection threshold τ; only data points with $|\mathbf{S_2}| > \tau$ are used to generate the raw key pair. The open squares show the fraction of the data points that are postselected. The black circles show the average error rate of the raw key after postselection. It can be seen that the postselected fraction depends on the threshold τ as expected, but also that the average error rate decreases with increasing threshold, as data points with higher absolute value are less ambiguous than data points with low absolute value (cf. also [32]). In this sense, the plotted error rate is averaged over all accepted data points, whether they originate from low absolute values with high error probability or from high absolute values with low error probability.

A refined version of the postselection procedure uses an analysis that defines effective binary information channels between Alice and Bob to estimate the mutual information $I_{A:B}$ between Alice and Bob and the Holevo quantity χ_{Holevo}. It is described in [13] and can be used to determine the secret key rate G for direct reconciliation using postselection and reverse reconciliation [12,34]. By using these information channels, one can determine the mutual information and Eve's knowledge about the data separately for each channel. The secret key rate can be optimized over Alice's input signal strength. Furthermore, it is possible to include the fact that any implementation of an error correction scheme cannot reach the theoretical performance limit given by Shannon [49,50].

Following the calculations in [13], we can predict the key rates for a realistic error correction protocol that is assumed to perform as efficiently as the widely used error correction protocol CASCADE [51]. The pulse rate for the experiment was 100 kPulse/s; the signal rate was 16.7 kPulse/s due to calibration. For the experiments of Table I, the key rates are shown in Table II. With the setup used, clock rates up to 2 MPulse/s are feasible, with no need for calibration (vacuum pulses) in the case of key generation, thus much higher secret key rates will be achieved in future experiments.

TABLE II. Relative key rates for the experimental data, assuming realistic error correction and no channel excess noise. DR stands for direct reconciliation, RR for reverse reconciliation.

State overlap $\langle -\alpha \vert + \alpha \rangle$	Quantum channel transmission T	Key rate DR and postselection	Key rate RR and postselection
0.50	45.7%	0.0027	0.0168
0.77	45.7%	0.0004	0.0025
0.52	48.3%	0.0038	0.0194
0.65	48.3%	0.0021	0.0106
0.51	65.0%	0.0244	0.0562

VI. CONCLUSIONS

We presented an experiment to verify the entanglement intrinsically present in Alice's and Bob's preparation and measurement data in a prepare-and-measure quantum key distribution experiment. Under the assumption that the local oscillator cannot be used by Eve to gain any information, we built a coherent state measurement setup with high quantum efficiency and low added noise. For two overlapping coherent states prepared by Alice, we show that the joint probability distribution $p(A;B)$ can only be explained by effective entanglement between Alice and Bob. This is the precondition for establishing a secret shared key [4,5,52]. In addition, by our special measurement setup we reconstruct Husimi's Q function for the states received by Bob, which is useful in detecting manipulations in the quantum channel. We show that the excess noise of our coherent states is within the measurement accuracy, and less than 2% of the variance of the shot noise. With this low noise, many attacks by Eve can be ruled out for a large range of transmission losses, allowing longer distance key distribution without compromising the security. By applying postselection to our measurement data, we showed that a secure key can be generated when Eve is restricted to using the beam splitting attack.

ACKNOWLEDGMENTS

This work was supported by the German engineers society (VDI) and the German science ministry (BMBF) under FKZ:13N8016, by the network of competence QIP of the state of Bavaria (A8), the EU-IST network SECOQC, and the German Research Council (DFG) under the Emmy-Noether program. The authors would like to thank N. Korolkova and D. Elser for valuable discussions.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. Bennett and G. Brassard, in *International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984).
[3] G. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).
[4] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[5] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
[6] J. H. Shapiro and S. S. Wagner, IEEE J. Quantum Electron. **20**, 803 (1984).
[7] N. Walker, J. Mod. Opt. **34**, 15 (1987).
[8] J. Rigas, Diplomarbeit, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2005.
[9] J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006).
[10] A. Peres, Phys. Rev. Lett. **77**, 1413 (2005).
[11] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[12] F. Grosshans and P. Grangier, e-print quant-ph/0204127.

[13] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2005).
[14] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[15] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[17] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[18] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[19] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[20] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[21] C. Fuchs, in *Quantum Communication, Computing, and Measurement 2*, edited by P. Kumar (Kluwer Academic/Plenum Publishers, New York, 2000), pp. 11–16.
[22] E. Arthurs and J. L. Kelly, Bell Syst. Tech. J. **44**, 725 (1965).
[23] S. Stenholm, Ann. Phys. (N.Y.) **218**, 233 (1992).
[24] K. Husimi, Proc. Phys. Math. Soc. Jpn. **22**, 264 (1940).
[25] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).
[26] Y. Lai and H. A. Haus, Quantum Opt. **1**, 99 (1989).
[27] U. Leonhardt and H. Paul, Phys. Rev. A **47**, R2460 (1993).
[28] U. Leonhardt and H. Paul, Phys. Rev. A **48**, 4598 (1993).
[29] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[30] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
[31] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inf. Theory **26**, 78 (1980).
[32] T. Hirano, T. Konishi, and R. Namiki, e-print quant-ph/0008037 (2000); T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).
[33] E. Corndorf, G. Barbosa, C. Liang, H. P. Yuen, and P. Kumar, Opt. Lett. **28**, 2040 (2003).
[34] F. Grosshans, G. Van Assche, R. M. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[35] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B: Lasers Opt. **79**, 273 (2004).
[36] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[37] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[38] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[39] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[40] G. Stokes, Trans. Cambridge Philos. Soc. **9**, 399 (1852).
[41] U. Fano, J. Opt. Soc. Am. **39**, 859 (1949).
[42] E. Collett, Am. J. Phys. **38**, 563 (1970).
[43] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and C. Silberhorn, Phys. Rev. A **65**, 052306 (2002).
[44] A. Yariv, *Optical Electronics in Modern Communications*, 5th ed. (Oxford University Press, New York, 1997).
[45] A. Forrester, J. Opt. Soc. Am. **51**, 253 (1961).
[46] L. Mandel, J. Opt. Soc. Am. **56**, 1200 (1966).
[47] R. Namiki and T. Hirano, Phys. Rev. A **67**, 022308 (2003).
[48] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[49] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[50] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[51] G. Brassard and L. Salvail, in *Advances in Cryptology—EUROCRYPT '93*, Lecture Notes in Computer Science Vol. 765, edited by T. Helleseth (Springer, Berlin, 1994), pp. 410–423.
[52] A. Acin and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[53] In an actual QKD implementation, one would need to make sure that the vacuum state is prepared locally in the receiver to avoid manipulation of the eavesdropper.