Gaussian Entanglement for Quantum Key Distribution from a Single-Mode Squeezing Source

Tobias Eberle[1,2], Vitus Händchen[1], Jörg Duhme[2,3], Torsten Franz[3], Reinhard F Werner[3], Roman Schnabel[1]

[1] Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and Institut für Gravitationsphysik, Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany
[2] Centre for Quantum Engineering and Space-Time Research - QUEST, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany
[3] Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany

E-mail: roman.schnabel@aei.mpg.de

Abstract. We report the realization of an Einstein-Podolsky-Rosen (EPR) entanglement source for gaussian continuous-variable quantum key distribution at 1550 nm. Our source is based on a single continuous-wave squeezed vacuum mode with 11.1 ± 0.1 dB squeezing, combined with vacuum at a balanced beam splitter. The conditional variance product (Reid criterion, *Phys. Rev.* A **40** 913, 1989) of this source is 0.31 ± 0.01, well below the classical threshold 1. The maximal achievable key rate with security against collective attacks is of 0.38 bits/measurement. Although only a single squeezed beam was used, the conditional variance product is comparable to the best reported values using two squeezed beams.

1. Introduction

Quantum key distribution (QKD) enables two remote parties to generate a shared key which is guaranteed to be entirely unknown to any potential eavesdropper. Discrete variable systems implementing, for example, the famous *BB84* protocol [1] are well established [2] and commercial systems even exist. Continuous variable (CV) systems using beams of laser light have also been investigated because they are expected to have characteristic advantages. In CV systems homodyne detection is used to measure the quadratures of the electro-magnetic field. PIN photo diodes, as used in homodyne detectors, are a well developed technology widely used in telecommunication. They offer high bandwidth, low dark noise and high quantum efficiencies. Most CV systems today use prepare-and-measure schemes employing gaussian or discrete modulation [3] - [7]. The less common entanglement-based schemes do not need signal modulation [8], and instead exploit quantum correlations in the field quadratures between the two parties in a bi-partite entangled state. The key resource for key generation then becomes the squeezing of laser beams, which is usually converted to entanglement by interfering two such beams on a beam splitter [9] - [18]. An implementation of a suitable source for a CV entanglement-based scheme was shown in [19] and a demonstration of a fully implemented table-top QKD was done in [20].

In this paper we realize and characterize an EPR entanglement source at the telecommunication wavelength of 1550 nm using only one squeezed mode and a vacuum mode at the two input ports of a balanced beam splitter. The resulting bi-partite two-mode squeezed state is reconstructed using balanced homodyne detection. A comparison of our experimental results with numerical simulations is used to analyze the structure of the noise, including an optical loss of 6.8 % and electronic dark noise, but no detectable phase noise. Various benchmark quantities are determined from the covariance matrix. The maximal extractable secret key rate against collective attacks is about 0.38 bits/measurement. Statistical fluctuations of this quantity due to the finite number of measurements for the reconstruction of the covariance matrix are discussed. Furthermore we calculate the EPR-entanglement, a conditional covariance product introduced by M. Reid [21]. Our source achieves a value of 0.31 ± 0.01, which has to be compared with the classical threshold 1. To the best of our knowledge this is the lowest value published so far [12, 16, 17], even including sources using two squeezed beams.

The paper is organized as follows: In Section 2 we recapitulate the description of gaussian systems in terms of symplectic invariant quantities. In Section 3 we specify our quantum key distribution scheme and show how to express the achievable key rate in terms of local symplectic invariants. Section 4 describes the experimental setup, and Section 5 the main results. Section 6 shows how we can specify the description of the source and the key distribution channel by simulating explicit noise models. Section 7 concludes the paper.

2. Gaussian systems

To fix notation, we summarize some facts about gaussian systems. We consider a bipartite experimental setting, one side labeled Alice, the other Bob. We call the joint state $\rho \in \mathcal{B}(\mathscr{H})$ where $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ is the Alice/Bob system Hilbert space.

2.1. Wigner function

In the following, we describe the state using its Wigner function. As we perform quadrature measurements and our states are gaussian this gives a convenient description. Our setup produces squeezed vacuum states, that is, the first moments are zero. So the gaussian state is completely determined by its covariance matrix Γ, whose elements are given by $\Gamma_{i,j} = \mathrm{tr}\left[\rho\left\{R_i, R_j\right\}_+\right]$, with the quadrature observables $R \in \{X_A, P_A, X_B, P_B\}$. The corresponding Wigner function is given by [22]

$$W(\xi) = (2\pi \det[\Gamma])^{-\dim[\Gamma]} \exp\left[-\frac{1}{2}\xi^T \Gamma^{-1} \xi\right] \ .$$

with the phase space vector ξ and covariance matrix

$$\Gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \ ,$$

where the blocks A and B correspond to the subsystems of Alice and Bob and C to the correlations. Furthermore, a physical gaussian state obeys the positivity criterion

$$\rho \geq 0 \Leftrightarrow \Gamma + i\Omega \geq 0 \ , \quad \text{where} \quad \Omega = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

is the symplectic form. The covariance matrix is always given with respect to a local choice of basis states. Many interesting properties, such as entanglement and the optimal extractable key rate, do not depend on these choices. One can therefore choose a basis bringing the covariance matrix into a simplified form, the so-called Simon normal form [23]

$$\Gamma = \begin{pmatrix} \lambda_a & 0 & c_x & 0 \\ 0 & \lambda_a & 0 & -c_p \\ c_x & 0 & \lambda_b & 0 \\ 0 & -c_p & 0 & \lambda_b \end{pmatrix}$$

with $\lambda_i \geq c_x \geq |c_p|$. Here c_x and c_p describe the correlations between Alice's and Bob's outcomes of the amplitude and phase measurements. These quantities characterize the state independent of any local basis transformations. However, their dependence on the original (e.g., measured) matrix Γ involves the diagonalization-like process of bringing Γ into this form by suitable local symplectic transformations. It is therefore often easier to use local symplectic invariants with a direct expression in terms of Γ. We use the set [23]

$$\begin{aligned} I_1 &= \det[A] = \lambda_a^2 \\ I_2 &= \det[B] = \lambda_b^2 \\ I_3 &= \det[C] = -c_x c_p \\ I_4 &= \det[\Gamma] = \left(c_x^2 - \lambda_a\lambda_b\right)\left(c_p^2 - \lambda_a\lambda_b\right) \ . \end{aligned}$$

2.2. EPR-Correlations

Different criteria have been used to quantify the (non-)classicality of quantum systems. The most basic distinction is whether a given state is separable, i.e. whether it can be written as a mixture of product states. States that are not separable are called

entangled, yet there are also entangled states which can be described with a local classical model [24]. The existence of such a model is equivalent to the full hierarchy of Bell inequalities. Sometimes (e.g., in [24]) one can get by with models in which on one side, say Bob's, quantum mechanics is taken for granted, so that the hidden variable is a random quantum state, from which the response of all measurement devices is computed by the quantum formalism. States allowing models with this property on *both* sides are exactly the separable ones. The one-sided condition is also called steering [25] after a remark by Schrödinger [26]. Thus, steering states (those which do not allow a half-quantum classical model) are more demanding to make than just non-separable ones, but such states might still be unfit for violating any Bell inequality [25].

In the gaussian setting violations of Bell inequalities are generally hard to get and require the measurement of some observables which are not functions of a single quadrature and hence not accessible by homodyne measurements. Indeed, if Alice and Bob are restricted to such measurements, the Wigner function provides an exact classical model for all correlations. However, the gaussian analogue of the steering condition makes sense, and has been shown [25, 27] to be equivalent to a criterion introduced by Margaret Reid [21], who called it "EPR-entanglement". It reads

$$\mathrm{Var}_{A|B}(X_A, X_B) \cdot \mathrm{Var}_{A|B}(P_A, P_B) < 1 \ , \tag{1}$$

where $\mathrm{Var}_{A|B}$ denotes the conditional variance of Alice's measurement given Bob's result and 1 is the critical value below which a state is called to be EPR entangled. Interchanging the roles of Alice and Bob gives a second, inequivalent criterion. Separable states are never EPR-entangled, while states violating a Bell inequality always do. On the converse, a state that fulfils the EPR criterion may not be separable, but may allow a description with a one-sided classical model.

In terms of the symplectic invariants the conditional variance product (1), optimized over the choice of local quadratures, is equal to I_4/I_1 (resp. I_4/I_2 if we exchange the roles of Alice and Bob). Hence Reid's EPR-entanglement is equivalent to

$$\frac{I_4}{I_1} < 1.$$

3. Quantum key distribution with gaussian states

In the following we summarize the classification of attacks on quantum cryptography systems. We determine the secure key rate for gaussian states described by their covariance matrix, assuming collective attacks and also consider effects due to experimental imperfections of the reconstruction of the covariance matrix.

3.1. Attacks

Possible attacks on QKD-schemes can be summed up in different classes whereby Eve has in all cases unlimited computational power. The classes are different in the way how Eve performs her measurement on the quantum channel. In ascending order of Eve's power they are:

Individual attacks	Eve does not posses a quantum memory and measures each signal individually.
Collective attacks	Eve has a quantum memory but attacks all signals in the same way, i.e., her attacks are permutation invariant.
Coherent attacks	Eve has a quantum memory and all attacks are allowed.
Device independent	Eve has produced Alice and Bobs devices and may exploit knowledge about the inner workings of the devices.

3.2. Secure key rate for collective attacks

Here we consider collective attacks in the limit of asymptotic key length. The extractable secret key rate is given by the Devetak-Winter bound [28] which has been adapted by Lodewyck et al. [4], to the gaussian regime:

$$k_{sec} = I_{A,B} - \chi_{E,X}$$

with $X \in \{A, B\}$. Here $I_{A,B}$ is the mutual information between Alice's and Bob's measurement outcomes, in other words, the information Alice has on Bob's outcome and vice versa. The Holevo rate $\chi_{E|X}$ represents the information Eve has on the measurement outcome of X. Eve always has the choice to eavesdrop Alice's or Bob's quantum channel or both. Because it is unknown where Eve performs her collective attack, X must be chosen such that

$$k_{sec} = \min\left[I_{A,B} - \chi_{E,X} | X \in \{A, B\}\right]$$

and all loss is thus considered to stem from attacks on the secrecy of the quantum channel. For example, if the state held by Alice and Bob is pure it follows that $\chi_{E,X} = 0$. Hence, due to the security analysis, loss always decreases the secrecy of our QKD scheme.

For completeness, we give now the secret key rate in terms of symplectic invariants (compare with [4]). First, we can express the mutual information as:

$$I_{A,B} = 1 - \frac{1}{2}\log_2\left(1 - \frac{1}{2}\left(\frac{I_4'}{I_1 I_2} + \sqrt{\frac{I_4'^2}{I_1^2 I_2^2} - \frac{4I_3^2}{I_1 I_2}}\right)\right)$$

with $I_4' = I_1 I_2 + I_3^2 - I_4$. Defining

$$\begin{aligned}
f(x) &= \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right) \\
d_{\pm} &= \sqrt{1/2\left((I_1 + I_2 + 2I_3) \pm \sqrt{(I_1 + I_2 + 2I_3)^2 - 4I_4}\right)} \\
d_A &= \sqrt{\sqrt{\frac{I_2}{I_1}}\left(\sqrt{I_1 I_2} - 1/2\left(\frac{I_4'}{\sqrt{I_1 I_2}} + \sqrt{\frac{I_4'^2}{I_1 I_2} - 4I_3}\right)\right)} \\
d_B &= \sqrt{\sqrt{\frac{I_1}{I_2}}\left(\sqrt{I_1 I_2} - 1/2\left(\frac{I_4'}{\sqrt{I_1 I_2}} + \sqrt{\frac{I_4'^2}{I_1 I_2} - 4I_3}\right)\right)}
\end{aligned}$$

we can express the Holevo rate as

$$\chi_{E,X} = f(d_+) + f(d_-) - f(d_X) \ ,$$

with $X \in \{A, B\}$. It should be noted, that asymmetries between Alice's and Bob's part of the state are only reflected in the $d_{A,B}$ quantity. This form lets us efficiently determine the secret key rate for any covariance matrix. Note again, that our security analysis mathematically only holds in the limit of asymptotic key length, thus finite size effects are not considered.

3.3. Effects of a finite number of measurements on the reconstruction of the covariance matrix

In our experiment we reconstruct the covariance matrix by homodyne measurements with finitely many samples. Hence, the reconstruction of the state is not perfect as infinite measurements would be needed. To account for this effect, we determine the state with the lowest extractable key that is compatible with the observed data. We find the physical state Γ' in a region around the measured state defined through gaussian abberation that minimizes the key rate in order to regain the security of our QKD. This approach comprises the standard gaussian error propagation of the key rate too. We optimize over the individual entries of the covariance matrix

$$k_{sec}\left(\Gamma'\right) = \min\left[k_{sec}\left(\widetilde{\Gamma}\right) | \forall i,j \ : \widetilde{\Gamma}_{i,j} \in \left[\Gamma_{i,j} - \frac{1}{\sqrt{N}}\Gamma_{i,j}, \Gamma_{i,j} + \frac{1}{\sqrt{N}}\Gamma_{i,j}\right]\right] \ , \tag{2}$$

where N is the number of measurements used for the reconstruction of the entry. This Ansatz is motivated by the fact that the abberation of the secure key rate itself, as numerically computed from the experimental data, scales with $1/Sqrt[N]$. We found that for practical inputs the minimizing matrix was of the form

$$\Gamma' = \Gamma + \frac{1}{\sqrt{N}} \begin{pmatrix} \lambda_a & 0 & -c_x & 0 \\ 0 & \lambda_a & 0 & c_p \\ -c_x & 0 & \lambda_b & 0 \\ 0 & c_p & 0 & \lambda_b \end{pmatrix} \ ,$$

although it should be noted that this is not necessarily unique. This gaussian abberation automatically considers the uncertainty of the reconstructed covariance matrix with respect to finite statistical effects.

4. Experiment

A schematic of the experiment is shown in Fig. 1. The EPR entanglement source was driven by a commercial 1 W 1550 nm fiber laser. Most of its power was frequency doubled in a quasi phase-matched periodically poled potassium titanyl phosphate (PPKTP) crystal [29] and served as a pump for the squeezed-light source. The squeezed-light source consisted of a $1 \times 2 \times 9.3\,\mathrm{mm}^3$ PPKTP crystal. One of its end-surfaces was curved with a radius of curvature of 12 mm and coated with a high-reflective coating for both the pump and the fundamental beam at 775 nm and 1550 nm, respectively. The other end-surface was flat and anti-reflective coated for both wavelengths. Together with a coupling mirror with a radius of curvature of 25 mm a hemilithic cavity was formed. The coupling mirror had a reflectivity of 90 % for 1550 nm and a reflectivity of 20 % for 775 nm. With an 23 mm air gap between the crystal and the coupling mirror the cavity had a finesse of 60 at 1550 nm, a

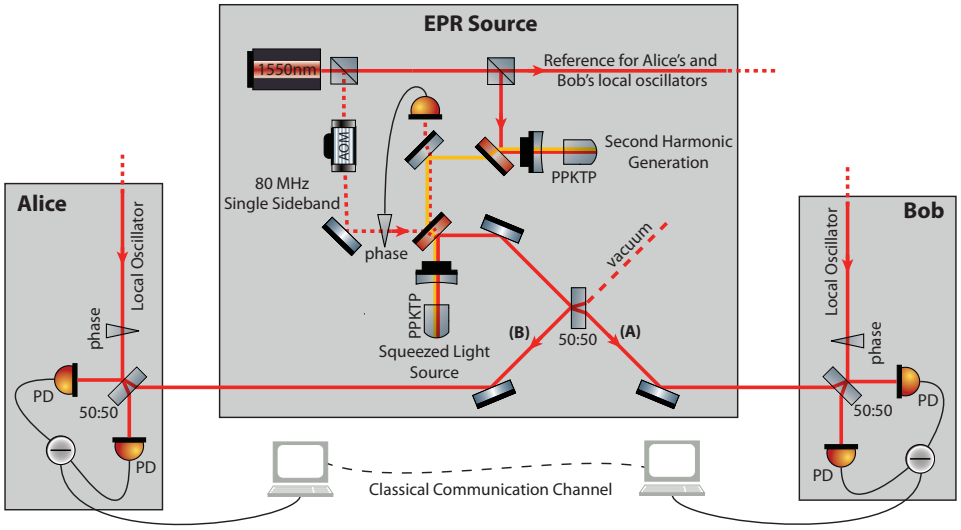

Figure 1. Schematic of the experiment: The beam of a 1550 nm fiber laser (red) was frequency doubled (yellow) and used as a pump for the squeezed-light source. The squeezed beam was overlapped with a vacuum mode at a 50 : 50 beam splitter to produce a pair of EPR entangled beams. The field quadratures of both beams were measured by balanced homodyne detection to characterize the EPR source and to provide data points that can be used to extract a secret quantum key from simultaneous measurements of the amplitude or phase quadrature. AOM: acousto-optical modulator, PD: photo diode.

free spectral range of 3.8 GHz and a full width half maximum linewidth of 63 MHz. The temperature of the PPKTP crystal was tuned to about 50° C to achieve quasi phase-matching. A sub-milliwatt control beam which was coupled into the cavity through the high-reflective mirror, was used to lock either the length of the cavity and the phase of the pump. The output of the squeezed-light source was split from the pump by means of a dichroic beam splitter and overlapped with a vacuum mode at a balanced beam splitter to produce a pair of EPR entangled beams. The field quadratures of these beams were measured by homodyne detection. Therefore each beam was overlapped with a strong local oscillator of about 10 mW at a balanced beam splitter with a visibility of about 99.5 % and detected by a pair of custom-made PIN photo diodes with high quantum efficiency ($> 99\,\%$). By changing the relative phase between the local oscillator and the quantum field the measured field quadrature could be chosen. In order to lock both homodyne detectors to a certain quadrature a single sideband technique was used. Therefore an 80 MHz frequency shifted beam, produced by an acousto-optical modulator, was coupled into the squeezing path from behind the dichroic beam splitter and phase locked to it. The single sideband was detected by the homodyne detectors and demodulated at 80 MHz. By choosing the phase of the electronic oscillator used for the demodulation appropriately the homodyne detector could be set to measure a certain field quadrature.

The outputs of both homodyne detectors were recorded simultaneously by means of a data acquisition system. Therefore they were demodulated with a double-balanced mixer at 8.3 MHz and lowpass filtered with an anti-aliasing filter having a passband of 40 kHz. The data was sampled with 14 bit resolution at a sampling rate of 500 kHz.

5. Experimental results

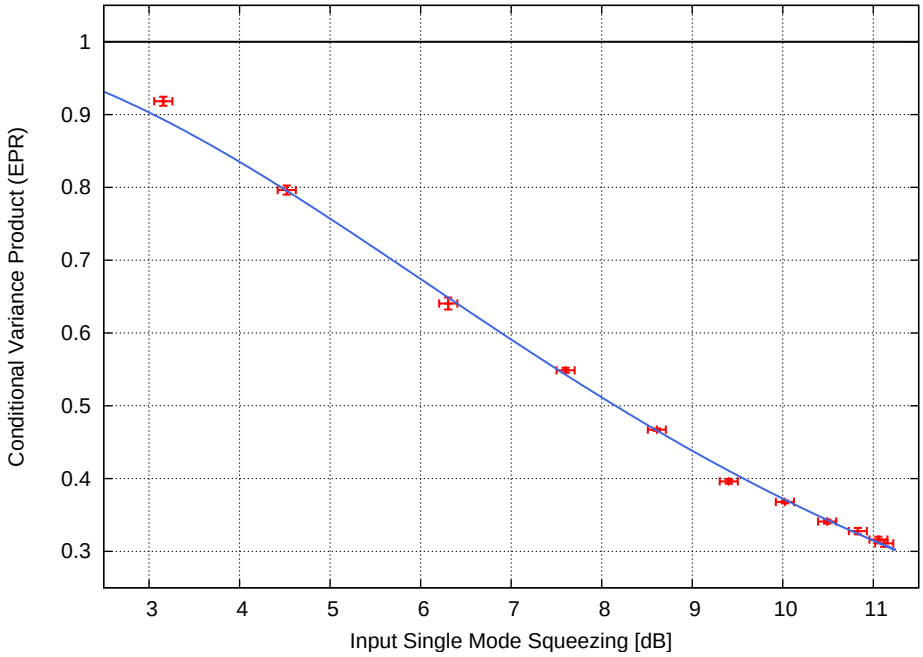

Figure 2. Characterization of the EPR source: The conditional variance product (EPR) is plotted versus the detected squeezing, measured before the balanced entanglement beam splitter. All measurements are done at a sideband frequency of 8.3 MHz. The blue line describes a theoretical model. The model fitted best with a total optical loss of 6.8 % and no phase noise.

Figure 2 shows a characterization of our EPR source. The conditional variance product from Eq. (1) is plotted versus the single mode input squeezing used to produce the entanglement. The conditional variance product was measured by both homodyne detectors taking either amplitude or phase quadrature data simultaneously. The variance of the squeezed state was determined by one of the homodyne detectors and a removed 50 : 50 beam splitter in the optical path. For this measurement the same optical pump power for the nonlinear process was used as for the entanglement measurement. For an input squeezing of 11.1 ± 0.1 dB (with corresponding anti-squeezing of 16.6 ± 0.1 dB) the Einstein-Podolsky-Rosen covariance product was as low as 0.31 ± 0.01. This is to the best of our knowledge the strongest Einstein-Podolsky-Rosen entanglement published so far. As all other schemes either use two squeezed beams to produce the entanglement or type II parametric down-conversion which is equivalent to the previous one, this result is quite remarkable. The blue solid line in the figure shows a theoretical model using

$$\mathrm{Var}_{A|B}(X_A, X_B) \cdot \mathrm{Var}_{A|B}(P_A, P_B) = \frac{1 + (\nu - \nu^2)\sinh^2 r}{1 + \frac{1}{4}(1-\nu^2)\sinh^2 r} \ ,$$

where ν denotes the overall optical loss and

$$r = -\frac{1}{2}\ln\left(\frac{10^{\mathrm{Var}_{sqz}/10} - \epsilon}{1-\epsilon}\right)$$

with Var_{sqz} being the variance of the squeezed input state in decibel. The parameter ϵ is the optical loss we obtained from the measurement of the input squeezing i.e. without 50:50 beam splitter. We determined ϵ to 5.9 %. The optical loss ν for the entanglement measurement was expected to be larger since further components were involved in the setup. We assumed it to be symmetric since both detectors are separated from the entanglement source by comparable optical paths. The model fits best with no phase noise and an overall optical loss of $\nu = 6.8\,\%$, which is indeed slightly higher than the total optical loss of the input squeezing measurement.

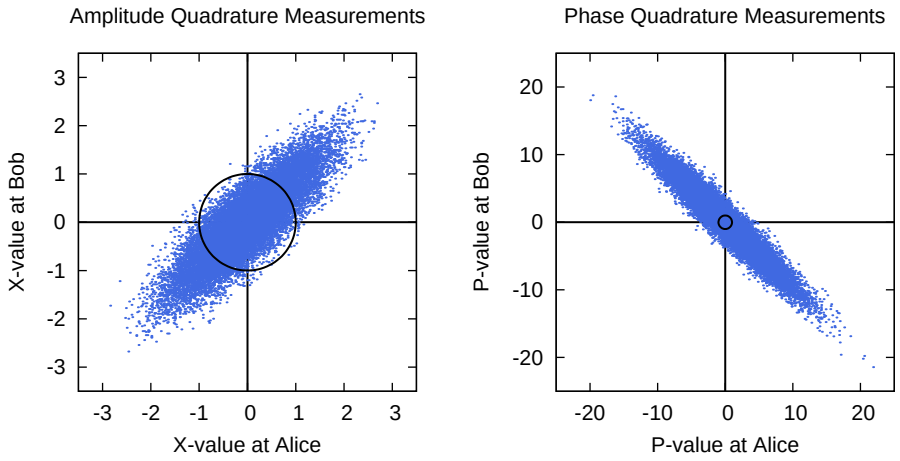

Figure 3. Data points from simultaneous measurements of the amplitude (left) and phase quadrature (right): In both quadratures the measurements are significantly correlated and anticorrelated, respectively.

Figure 3 shows the correlations between Alice and Bob at an input squeezing of 11.1 dB. The figure on the left hand side shows data points from simultaneous measurements of the amplitude quadrature at both detectors. Each point refers to the outcome of Alice's measurement on the abscissa and Bob's corresponding measurement outcome on the ordinate, where both values are normalized to the standard deviation of the vacuum (black circle in the figure). On the right hand side the same for the phase quadrature is shown. The amplitude quadrature measurements are significantly correlated, whereas the phase quadrature measurements are anti-correlated due to the phase flip at the entanglement beam splitter. Furthermore, the measurement values for the phase quadrature have a considerably higher variance at each detector since this quadrature is anti-squeezed.

Assuming collective attacks, the achievable secure key rate dependent on the input squeezing is shown in Fig. 4. According to our model, with an optical loss of 6.8 % and no phase noise, we observed a positive key rate for more than 5 dB input squeezing reaching about 0.38 bits/measurement for 10.5 dB. The secure key rate was calculated with Eq. (2) from the reconstructed covariance matrices. Hence, no error bars are given as the shown secure key rate refers to its lower bound.

To reconstruct the covariance matrix of our bi-partite state the partial tomographic protocol described in [19] was used, where for the first time the complete covariance matrix of a gaussian state was measured. For example the covariance

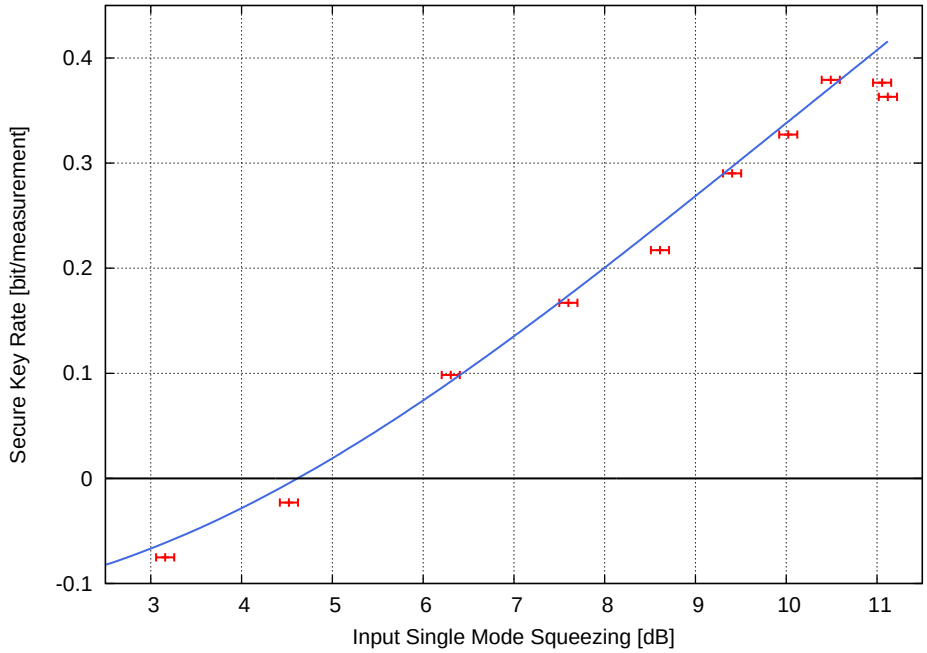

Figure 4. Achieved key rate, secure against collective attacks, as a function of detected squeezing, which was measured before the 50 : 50 entanglement beam splitter. The blue line is a simulated model, which fitted best with an optical loss of 6.8 %, no phase noise and an electronic dark noise level 18.3 dB below the vacuum noise.

matrix for the generated state with an input squeezing of 11.1 dB is given as follows,

$$\Gamma = \left(\begin{array}{cc|cc} 0.55 & -0.09 & 0.45 & -0.14 \\ -0.09 & 24.7 & -0.07 & -23.2 \\ \hline 0.45 & -0.07 & 0.55 & 0.01 \\ -0.14 & -23.2 & 0.01 & 23.7 \end{array}\right) .$$

One can directly see certain properties of the state from the entries in the matrix. The values on the principal diagonal are the variances for the amplitude and phase quadrature measurements at Alice's and Bob's detector. The diagonal entries of the two blocks in the upper right and lower left give the strengths of the correlations in the amplitude quadrature and the anticorrelations in the phase quadrature, respectively, between both detectors. In a perfect orthogonal measurement the remaining entries should turn out to be zero since they give the covariance between amplitude and phase quadratures. The small deviation from zero show that the measurements were not perfectly orthogonal. The influence of this effect on the secure key rate is discussed in Section 6.

The solid line in Fig. 4 describes the theoretical behavior of the secure key rate. The theoretical model was calculated by simulating all biasing experimental effects on the key rate. A description of these effects and their influences as well as the fit parameters are given in Section 6. The deviation of the experimental data from the theoretical model at high input squeezing stems probably from the locks of the

squeezed-light source and the homodyne detectors which might be unsufficient as disturbances on small time scales have large impact for such high squeezing levels.

6. Determination of system parameters

In order to give a precise description of our source, we have modeled different types of noise that could influence the state, respectively, the data acquisition. We used numerical simulations to determine which type of noise is present in the experiment and discuss influences on the secure key rate. It should be emphasized here, that we are performing our investigations under the assumption of collective attacks and in the limit of infinite repetition.

6.1. Sources

The generation of squeezed light has been modeled in [30] as

$$\mathrm{Var}_{\mathrm{sqz,asqz}} = 1 \pm \eta \frac{4\sqrt{P/P_{\mathrm{th}}}}{(1 \mp \sqrt{P/P_{\mathrm{th}}})^2 + 4K^2} \ ,$$

where η is the overall efficiency, P the pump power for the nonlinear process, P_{th} the threshold power and K a constant depending on the implementation. The corresponding parameters were determined directly at the source, i.e. without $50:50$ beam splitter, to $\eta = 0.941$, $P_{\mathrm{th}} = 268\,\mathrm{mW}$ and $K = 0.136$. One should note, that the generated state is mixed for all pump powers.

6.2. Optical loss

Optical loss stems from absorption, scattering, the non-ideal quantum efficiency of the balanced homodyne detector and from non-perfect mode-matching reducing the visibility. It can be modeled as a convex combination of the original state ρ with the vacuum state ρ_{vac} as $\rho' = (1-\nu)\rho + \nu\rho_{vac}$, which translates to the covariance matrix as

$$\Gamma' = (1-\nu)\,\Gamma + \nu\mathbb{1} \ ,$$

where $\nu \in [0,1]$ is the optical loss parameter.

6.3. Phase noise

We subsume all imperfections of the measurement basis choice under the topic phase noise. While the ideal measurement would always measure only the phase or amplitude quadrature, phase noise imprinted on the local oscillator would introduce deviations from the perfect choice of the quadrature. We describe phase noise as random rotation in phase space, given by a distribution F. The state ρ transforms as

$$\rho^{\text{phase noise}} = \int F\left(\Delta\sigma, \Delta\alpha_t\right) U\left(\Delta\alpha_t\right)^{\dagger} \rho U\left(\Delta\alpha_t\right) d\alpha_t \ .$$

Thereby $U\left(\alpha_t\right)$ describes the rotation while $F\left(\Delta\sigma, \Delta\alpha_t\right)$ is chosen as gaussian distribution with mean α and variance σ.

Phase noise is not a gaussian process, i.e. the resulting state will not be fully described by its second moments [31, 32]. On the other hand, the effect of phase noise would significantly reduce the gaussian character of the state.

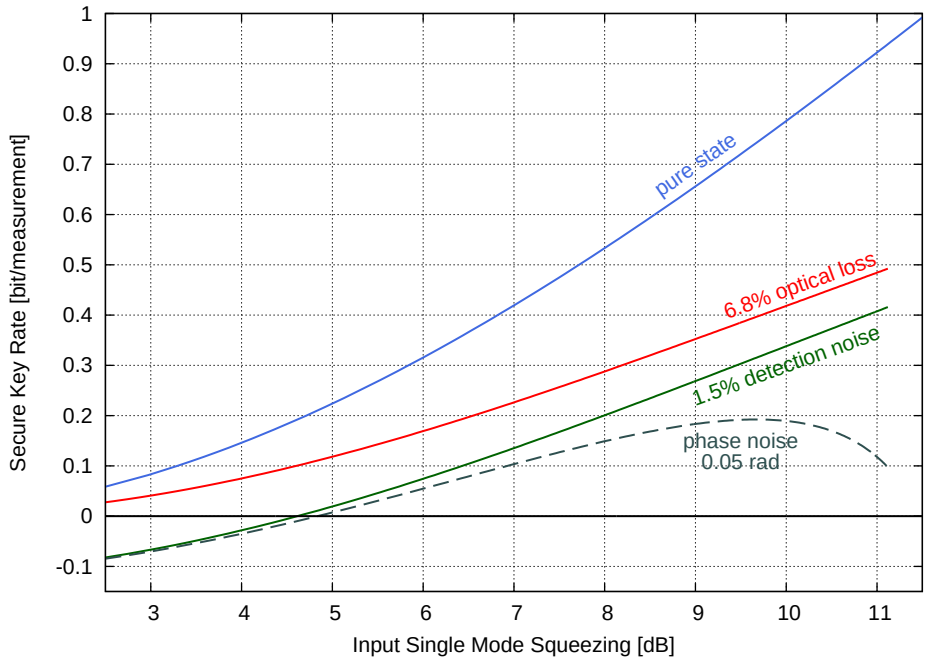

Figure 5. Simulation of the secure key rate vs. the input single mode squeezing: The blue curve shows the secure key rate expected from a pure state. For the red one an optical loss of 6.8 %, as present in our experiment, was taken into account. Therefore an optical loss of 5.9 % was assumed for the squeezing, i.e. before the beam splitter, yielding the input single mode squeezing on the abscissa. For the green curve 1.5 % detection noise was added in addition to the optical loss. This curve corresponds to the one in Fig. 4. In the presence of additional 0.05 rad phase noise the secure key rate would drop to the grey dashed curve.

6.4. Detection noise

In our setup, detection noise is mainly given by electronic dark noise of the balanced homodyne detector. Other sources of detection noise could be residual technical noise of the local oscillator beam in combination with a non-perfect common mode rejection. Shot noise and technical noise of the control beams accompanying the entangled fields could also result in increased noise in the balanced homodyne detector.

6.5. Discussion

We have found that the behavior of the state in terms of its covariance matrix can be described quite well with the types of noise discussed above. For the theoretical model in Fig. 4 we found a total optical loss of $\nu = 6.8\,\%$ and zero phase noise. Our simulation revealed a detection noise of 1.5 % in respect to the balanced homodyne detectors' vacuum noise. This is in excellent agreement with their independently measured dark noise variance of 18.3 dB below the vacuum noise. Hence, our control beams did not contribute to the detection noise. It should be noted, that every source of noise has a characteristic impact on the key rate, which can be seen in Fig. 5.

One effect, not part of the current investigation, are correlations between

successive measurements. These correlations have been observed in the experiment and would reduce the key rate. A possible source for these correlations has been identified in the anti-aliasing lowpass filter which is used for the data acquisition [33]. A future enhancement of the experiment is expected to show much less correlations.

7. Conclusion

We have presented a gaussian entanglement source involving a squeezed mode and a vacuum mode which revealed a positive secure key rate when taking collective attacks into account. We have shown that a single squeezed input mode is a resource sufficient for entanglement based quantum key distribution. The modelling of our EPR entanglement is in very good agreement with our experimental data.

In the present experiment the entanglement has been distributed on an optical table. Coupling one part of the bi-partite state into an standard optical telecommunication fiber and building Bob's detector remotely would allow for quantum key distribution in local area networks. Our simulation revealed that even with an additional optical loss of up to about 20 % in one arm the secure key rate would still be positive, assuming no phase noise is induced by the fiber. A previous experiment showed that a high coupling efficiency to optical fibers can be achieved [34]. Hence, secure keys can be distributed between two parties who are about 1 to 2 km apart. Although the restriction to a single squeezed input mode, as presented here, is of fundamental interest, a full scheme with two squeezed fields overlapped at a balanced beam splitter will achieve higher key rates. Assuming again no phase noise we expect the secure key rate for a 1 km fiber to be around 1 bit/measurement. Since a squeezing bandwidth of more than 100 MHz was already demonstrated [35] such a kilometer-scale quantum key distribution could achieve significant overall key rates.

Acknowledgments

This research was supported by the EU FP 7 project Q-ESSENCE (Grant agreement number 248095). TE and VH thank the IMPRS on Gravitational Wave Astronomy for support. VH acknowledges support from HALOSTAR. TF acknowledges support from DFG under grant WE-1240/12-1 and from BMBF project QUOREP. RFW acknowledges support by the EU FP 7 project COQUIT (Grant agreement number 233747).

References

[1] Bennett C H and Brassard G 1984, *Proc. of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore: India) p 175–9
[2] Gisin N, Ribordy G, Tittel W, and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[3] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **85** 057902
[4] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, and Grangier P 2007 *Phys. Rev.* A **76** 042305
[5] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New. J. Phys.* **11** 045023
[6] Lance A M, T Symul T, Sharma V, Weedbrook C, Ralph T C, and Lam P K 2005 *Phys. Rev. Lett.* **95** 180503
[7] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[8] Rodo C, Romero-Isart O, Eckert K, Sanpera A 2007 *Open Syst. Inf. Dyn.* **14** 69–80
[9] Ou Z Y, Pereira S F, Kimble H J, Peng K C 1992 *Phys. Rev. Lett.* **68** 3663–6

[10] Zhang Y, Wang H, Li X, Jing J, Xie C, Peng K 2000 *Phys. Rev.* A **62** 023813
[11] Schori C, Sorensen J L, Polzik E S 2002 *Phys. Rev.* A **66** 033802
[12] Laurat J, Coudreau T, Keller G, Treps N, Fabre C 2005 *Phys. Rev.* A **71** 022313
[13] Keller G, D'Auria V, Treps N, Coudreau T, Laurat J, Fabre C 2008 *Opt. Express* **16** 9351–6
[14] Bowen W P, Schnabel R, Lam P K, Ralph T C 2003 *Phys. Rev. Lett.* **90** 043601
[15] Takei N, Lee N, Moriyama D, Neergaard-Nielsen J S, Furusawa A 2006 *Phys. Rev.* A **74** 060101(R)
[16] Hage B, Janousek J, Armstrong S, Symul T, Bernu J, Chrzanowski H M, Lam P K, Bachor H A *Eur. Phys. J.* D **63** 457–61
[17] Eberle T, Händchen V, Duhme J, Franz T, Werner R F, and Schnabel R 2011 *Phys. Rev.* A **83** 052329
[18] Silberhorn C, Lam P K, Weiß O, König F, Korolkova N, Leuchs G 2001 *Phys. Rev. Lett.* **86**, 4267–70
[19] DiGuglielmo J, Hage B, Franzen A, Fiurasek J, and Schnabel R 2007 *Phys. Rev.* A **76** 012323
[20] Su X, Wang W, Wang Y, Jia X, Xie C and Peng K 2009 *EPL* **87** 20005
[21] Reid M D 1989 *Phys. Rev.* A **40** 913–23
[22] Wigner E 1932 *Phys. Rev.* **40** 749
[23] Simon R 2000 *Phys. Rev. Lett.* **84** 2726–2729
[24] Werner R F 1989 *Phys. Rev.* A **40** 4277–4281
[25] Wiseman H M, Jones S J and Doherty A C 2007 *Phys. Rev. Lett* **98** 140402
[26] Schrödinger E 1935 *Proc. Camb. Phil. Soc.* **31** 553
[27] Cavalcanti E G, Jones S J, Wiseman H M, and Reid M D 2009 *Phys. Rev.* A **80** 032112
[28] Devetak I, and Winter A 2004 *Phys. Rev. Lett.* **93** 080501
[29] Ast S, Moghadas Nia R, Schönbeck A, Lastzka N, Steinlechner J, Eberle T, Mehmet M, Steinlechner S, and Schnabel R 2011 *Opt. Lett.* **36** 3467–9
[30] Takeno Y, Yukawa M, Yonezawa H, Furusawa A 2007 *Opt. Express* **15** 4321–7
[31] Franzen A, Hage B, DiGuglielmo J, Fiurasek J, and Schnabel R 2006 *Phys. Rev. Lett.* **97** 150505
[32] Hage B, Samblowski A, DiGuglielmo J, Franzen A, Fiurasek J, and Schnabel R 2008 *Nature Physics* **4** 915–918
[33] Hamill D C 1981 *Wireless World* **August** 59–64
[34] Mehmet M, Eberle T, Steinlechner S, Vahlbruch H, and Schnabel R 2010 *Opt. Lett.* **35** 1665-7
[35] Mehmet M, Vahlbruch H, Lastzka N, Danzmann K, and Schnabel R 2010 *Phys. Rev.* A **81** 013814