Gaussian entanglement for quantum key distribution from a single-mode squeezing source

2013 New J. Phys. 15 053049

(http://iopscience.iop.org/1367-2630/15/5/053049)

New Journal of Physics
The open access journal for physics

Gaussian entanglement for quantum key distribution from a single-mode squeezing source

Tobias Eberle[1,2], Vitus Händchen[1,2], Jörg Duhme[2,3], Torsten Franz[2,3], Fabian Furrer[4], Roman Schnabel[1,2,5] and Reinhard F Werner[2,3]

[1] Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and Institut für Gravitationsphysik, Leibniz Universität Hannover, Callinstraße 38, D-30167 Hannover, Germany
[2] Centre for Quantum Engineering and Space-Time Research—QUEST, Leibniz Universität Hannover, Welfengarten 1, D-30167 Hannover, Germany
[3] Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstraße 2, D-30167 Hannover, Germany
[4] Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
E-mail: roman.schnabel@aei.mpg.de

New Journal of Physics **15** (2013) 053049 (14pp)
Received 6 March 2013
Published 30 May 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/5/053049

Abstract. We report the suitability of an Einstein–Podolsky–Rosen entanglement source for Gaussian continuous-variable quantum key distribution at 1550 nm. Our source is based on a single continuous-wave squeezed vacuum mode combined with a vacuum mode at a balanced beam splitter. Extending a recent security proof, we characterize the source by quantifying the extractable length of a composable secure key from a finite number of samples under the assumption of collective attacks. We show that distances in the order of 10 km are achievable with this source for a reasonable sample size despite the fact that the entanglement was generated including a vacuum mode. Our security analysis applies to all states having an asymmetry in the field quadrature variances, including those generated by superposition of two squeezed modes with different squeezing strengths.

[5] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Quantum key distribution (QKD) enables two remote parties to generate a shared key which is guaranteed to be unknown to any potential eavesdropper. Discrete variable systems implementing, for example, the famous *BB84* protocol [1] are well established [2] and commercial systems exist. Recently, also first commercial continuous variable (CV) systems have been launched in which the field quadratures of laser light are measured by homodyne detection. Compared to discrete variable systems, they have the advantage that for homodyne detection PIN photo diodes can be used which are well developed and widely used telecommunication components. They offer high bandwidth, low dark noise and high quantum efficiencies. Most of todays CV QKD systems use prepare-and-measure schemes employing coherent states with Gaussian or discrete modulation [3–7]. Prepare-and-measure schemes with squeezed states have been considered in [8, 9]. The less common entanglement-based schemes do not need signal modulation [10], and instead exploit directly the correlations in the field quadratures of an Einstein–Podolsky–Rosen (EPR) entangled state. EPR entangled states are usually generated by interfering two squeezed beams at a beam splitter [11–22].

An implementation of a suitable source for a CV entanglement-based scheme was shown in [23] and a demonstration of a fully implemented table-top QKD system was given in [24]. In both cases the security analysis assumed an infinite number of measured samples which is experimentally unfeasible. Security proofs for CV systems including the effect of a finite number of samples were only recently published [25, 26]. In [27] an experiment including finite-size effects was performed using Gaussian modulation and coherent states with a security analysis under the assumption of collective attacks. The first quantitative security analysis against coherent attacks, which also includes finite-size effects, was shown for a protocol using EPR entangled states [26].

In this paper, we characterize EPR entangled states generated by superimposing a squeezed vacuum mode with a vacuum mode at a balanced beam splitter in terms of extractable key length. Using only one squeezed mode instead of two minimizes the necessary resources and reduces the complexity of the setup. Our source is implemented at the telecommunication wavelength of 1550 nm to, in principle, allow for efficient coupling to existing telecommunication fiber networks. We calculate the extractable key rate as a function

of measured samples for various communication distances through an optical fiber. We assume that the source is located in the lab of an honest party such that only one part of the beam is affected by transmission losses. The key rate is computed by applying the security proof for composable security under the assumption of collective attacks including finite-size effects given in [26] to states with asymmetric field quadrature variances. As asymmetries in the field quadrature variances are experimentally unavoidable even for entanglement generated by two squeezed modes, our analysis can also be applied to such states.

The paper is organized as follows, In section 2 we describe the protocol, give the security definitions and extend the proof given in [26] to asymmetric states. Section 3 is devoted to the details of the experimental setup. The main results are presented in section 4. The paper ends with the conclusions in section 5.

2. Security analysis

In this section we extend the security proof for composable security against collective Gaussian attacks including finite-size effects given in [26] toward two-mode squeezed states with an asymmetry of the noise distributions of the field quadratures. By superimposing a squeezed mode with a vacuum mode at a balanced beam splitter, the two output modes are still squeezed in one quadrature which we assume to be the amplitude quadrature X, and anti-squeezed in the orthogonal quadrature, the phase quadrature P.

2.1. Protocol

The protocol we use goes as follows:

(i) *Preparation and measurement.* Alice prepares an entangled state with her EPR source, keeps one subsystem and sends the other to Bob. Both parties perform homodyne measurements in either the X or P quadrature which is individually chosen at random. An outcome of such a synchronous measurement is called a sample. This process is repeated until $2N$ samples were recorded, forming two strings x''_A and x''_B of length $2N$.

(ii) *Sifting.* In the second step Alice and Bob perform sifting, i.e. they communicate which quadrature they measured. Samples measured with a different choice of quadrature are discarded from x''_A and x''_B leaving Alice and Bob with strings x'_A and x'_B of length N in average. The discarded data are used for parameter estimation.

(iii) *Parameter estimation.* In the third step Alice and Bob chose randomly a common subset of length k from x'_A and x'_B which they reveal. From these data and the data discarded by the sifting procedure, they reconstruct the covariance matrix. In particular, they estimate a confidence set $\mathcal{C}_{\epsilon_{\text{pe}}}$ with the property that with probability $1-\epsilon_{\text{pe}}$ the real covariance matrix lies within $\mathcal{C}_{\epsilon_{\text{pe}}}$.

(iv) *(Optional) Discarding X or P quadrature measurements.* As the X and P quadrature measurements of Alice and Bob are correlated with different strengths due to the asymmetric nature of the bipartite entangled state, it might be beneficial to discard the measurements performed in the P quadrature from the raw key. To take into account all three possibilities, i.e. discarding X measurements, discarding P measurements and discarding nothing at all, we introduce a parameter p_X which describes the probability of a sample being measured in the X quadrature. For taking both X and P quadrature

measurements to generate a raw key $p_X \approx 0.5$ depending on the actual run. By discarding all X measurements $p_X = 0$ and 1 for dicarding all P quadrature measurements. The number of samples left after this step is denoted by n.

(v) *Binning.* In the fourth step Alice and Bob group their unrevealed samples into bins $\left(-\infty, -\alpha_{\{X,P\}} + \delta_{\{X,P\}}\right)$, $\left(-\alpha_{\{X,P\}} + \delta_{\{X,P\}}, -\alpha_{\{X,P\}} + 2\delta_{\{X,P\}}\right)$, ..., $\left(\alpha_{\{X,P\}} - \delta_{\{X,P\}}, \infty\right)$. Each bin is assigned a unique bit combination so that after the conversion Alice and Bob both have a bit string representing their raw key. In practice, we always choose α such that for no sample the quadrature measurement exceeded α. In that sense, only δ is a free parameter in the protocol.

(vi) *Classical postprocessing.* In the last step Alice and Bob perform error correction and privacy amplification to extract ℓ secure bits. We assume that they execute a reverse information reconciliation protocol (error correction) in which Bob only sends information to Alice and denote the number of bits revealed by Bob by ℓ_{EC}. In the final privacy amplification step both parties apply two-universal hash functions to reduce the key length to ℓ bits, where ℓ is computed according to equation (3).

2.2. Security definitions

It is important to ensure that the key is secure in any further cryptographic sub-protocol like, for instance, the one-time pad to securely transmit messages between Alice and Bob. To guarantee this we use the composable security definitions from [28, 29]. In the following, we denote by S_A and S_B the random variables associated with the final key of Alice and Bob at the very end of the protocol.

Robustness. We call a protocol robust if it does not abort when no eavesdropper is present. This ensures that the protocol is not trivial.

Correctness. A protocol is ϵ_{c}-correct if

$$\mathrm{Prob}[S_A \neq S_B] \leqslant \epsilon_{\mathrm{c}}.$$

If $\epsilon_{\mathrm{c}} \ll 1$, this implies that Alice's and Bob's key agree with high probability.

Secrecy. Let $\omega_{S_B E}$ denote the classical-quantum state of Bob's final key S_B and a possible eavesdropper E. Such a state can always be written as

$$\omega_{S_B E} = \sum_{s_B \in S_B} p(s_B) |s_B\rangle\langle s_B| \otimes \omega_E^{s_B},$$

where $p(s_B)$ is the probability distribution of the key. We then call a protocol ϵ_{s}-secret if for any eavesdropper E

$$\frac{p_{\mathrm{pass}}}{2} \| \omega_{S_B E} - \tau_{S_B} \otimes \omega_E \|_1 \leqslant \epsilon_{\mathrm{s}}$$

holds. Here, $\| \cdot \|_1$ is the trace norm, τ_{S_B} is the uniform distribution over S_B, ω_E is the reduced state of $\omega_{S_B E}$ and $1 - p_{\mathrm{pass}}$ is the probability that the protocol aborts.

Security. A protocol is ϵ-secure if it is ϵ_{c}-correct and ϵ_{s}-secret with $\epsilon_{\mathrm{c}} + \epsilon_{\mathrm{s}} \leqslant \epsilon$.

For a detailed discussion of the above security conditions we refer to [30].

2.3. Secure key rates

Let us consider the stage of the protocol before applying error correction and privacy amplification. We call the remaining n samples at this stage the raw keys and denote the corresponding random variables on Alice's and Bob's side by X_A^n and X_B^n. One can assume that X_A^n and X_B^n are obtained by performing n times a quadrature measurement where amplitude X is chosen with probability p_X and phase P with $p_P = 1 - p_X$. Note that for the following security discussion p_X can be arbitrarily chosen. Let in the following E^n be the eavesdropper system which can be infinite dimensional and $\omega_{X_A^n X_B^n E^n}$ the corresponding classical-quantum state conditioned on the event that the protocol passes. It was shown in [31] that an ϵ_c-correct and ϵ_s-secret key of length

$$\max_{\epsilon_1} \left[H_{\min}^{\epsilon}(X_B|E)_\omega - \ell_{EC} - \log_2 \frac{1}{4\epsilon_1^2 \epsilon_c} \right] \tag{1}$$

can be extracted. $H_{\min}^{\epsilon}(X_B^n|E^n)_\omega$ denotes the conditional smooth min-entropy of $\omega_{X_B^n E^n}$ for $\epsilon \leqslant (\epsilon_s - \epsilon_1)/2$ introduced in [29] and generalized to infinite-dimensional systems in [31, 32]. Hence, it remains to obtain a lower bound on $H_{\min}^{\epsilon}(X_B^n|E^n)_\omega$ for any possible eavesdropping strategy.

Under the assumption of collective attacks, we can assume that the state $\omega_{X_A^n X_B^n E^n}$ has tensor product structure, i.e. $\omega_{X_A^n X_B^n E^n} = \omega_{X_A X_B E}^{\otimes n}$. The smooth min-entropy of a product state can then be approximated by the conditional von Neumann entropy $H(X_B|E)_\omega$ of $\omega_{X_B E}$ via the asymptotic equipartition property [32]

$$H_{\min}^{\epsilon}(X_B|E)_\omega \geqslant n H(X_B|E)_\omega - \sqrt{n}\Delta, \tag{2}$$

where n has to be sufficiently large and

$$\Delta = 4 \log_2 \left(2^{\frac{1}{2} H_{\max}(X_B)+1} + 1 \right) \sqrt{\log_2 \frac{2}{\epsilon^2}}.$$

In the next step, we use that the state $\omega_{X_B E}$ is of form $\omega_{X_B E} = p_X |X\rangle\langle X|_\theta \otimes \omega_{X_B E}^X + (1 - p_X)|P\rangle\langle P|_\theta \otimes \omega_{X_B E}^P$ where $\omega_{X_B E}^X$, $\omega_{X_B E}^P$ are the states obtained when the honest parties are measuring amplitude or phase, respectively. The system denoted by θ is a classical register which is assigned to the eavesdropper and keeps track which measurements were performed by the honest parties. Using elementary properties of the von Neumann entropy, we can now expand $H(X_B|E\theta)_\omega = p_X H(X_B|E)_{\omega^X} + p_P H(X_B|E)_{\omega^P}$. Combining this estimation of the smooth min-entropy with the assumption of Gaussian attacks, we can use the confidence set $\mathcal{C}_{\epsilon_{pe}}$ to obtain a lower bound on the key length given by

$$\ell = n \inf_{\gamma \in \mathcal{C}_{\epsilon_{pe}}} \sum_\theta p_\theta H(X_B|E)_{\omega^{\gamma,\theta}} - \sqrt{n}\Delta - \ell_{EC} - \log_2 \frac{1}{\epsilon_s^2 \epsilon_c}. \tag{3}$$

Here, the infimum is taken over all states compatible with covariance matrices γ within the confident set. For simplicity, we have chosen $\epsilon_1 = \epsilon_s/2$ which can be justified by the fact that for large enough n the term in the logarithm can be neglected. Note further that due to the definition of $\mathcal{C}_{\epsilon_{pe}}$, the key length from equation (3) is now ϵ-secure with $\epsilon = \epsilon_{pe} + \epsilon_s + \epsilon_c$.

The von Neumann entropy for both quadratures $\theta = X, P$ can now be computed under the non-restricting assumption that the eavesdropper holds the purification of Alice's and Bob's state, that is, we assume that ω_{ABE}^γ is the purification of the Gaussian state ω_{AB}^γ with covariance

matrix γ. It then follows by applying the definition of the conditional von Neumann entropy $H(X_B|E) = H(X_B E) - H(E)$ and the self-duality $H(E)_{\omega^\gamma} = H(AB)_{\omega^\gamma}$ that

$$H(X_B|E)_{\omega^{\gamma,\theta}} = H(E|X_B)_{\omega^{\gamma,\theta}} + H(X_B)_{\omega^{\gamma,\theta}} - H(AB)_{\omega^\gamma} . \tag{4}$$

As shown in [26, 33, 34]

$$H(E|X_B)_{\omega^{\gamma,X}} \geqslant H(E)_{\omega^{\gamma,X}(X=0)} = H\left(A - C(M_X B M_X)^{\mathrm{MP}} C^{\mathrm{T}}\right)_{\omega^\gamma}$$

and

$$H(E|X_B)_{\omega^{\gamma,P}} \geqslant H(E)_{\omega^{\gamma,P}(P=0)} = H\left(A - C(M_P B M_P)^{\mathrm{MP}} C^{\mathrm{T}}\right)_{\omega^\gamma} ,$$

where $H(E)_{\omega^{\gamma,\{X,P\}(\{X,P\}=0)}}$ is the post-measurement state at the eavesdropper's side when Bob measured $X = 0$ or $P = 0$. The bipartite covariance matrix is written in block form, i.e.

$$\gamma = \begin{pmatrix} A & C \\ C^{\mathrm{T}} & B \end{pmatrix}$$

and $M_X = \mathrm{diag}(1, 0)$ and $M_P = \mathrm{diag}(0, 1)$ are the projectors to the X and P quadrature, respectively. MP denotes the Moore–Penrose inverse.

To compute Δ, we have to estimate $H_{\max}(X_B)$ which can be approximated by [32]

$$H_{\max}(X_B) \leqslant 2\log_2\left(\sqrt{p_X}\sum_y \sqrt{\omega^X_{X_B}(y)} + \sqrt{(1-p_X)}\sum_y \sqrt{\omega^P_{X_B}(y)}\right),$$

where $\omega^X_{X_B}$ and $\omega^P_{X_B}$ are the probability distributions of Bob's X and P quadrature measurements, respectively.

While in a practical experiment the number of bits ℓ_{EC} can be directly measured for each run, we need to estimate the leakage term here. We assume the term to be [35]

$$\begin{aligned}\ell_{\mathrm{EC}} = {} & p_X \left(H(X_B)_{\omega^{\gamma,X}} - \beta I(X_A, X_B)_{\omega^{\gamma,X}}\right) \\ & + (1-p_X)\left(H(X_B)_{\omega^{\gamma,P}} - \beta I(X_A, X_B)_{\omega^{\gamma,P}}\right),\end{aligned}$$

where $\beta \in (0, 1)$ is the error correction efficiency and $I(A, B)$ is the mutual information. In this paper we will assume an error correction efficiency of $\beta = 0.9$ [36].

With these results the secure key rate $r = \ell/n$ can be calculated by

$$\begin{aligned} r = \inf_{\gamma\in\mathcal{C}_{\epsilon_{\mathrm{pe}}}} {} & p_X\left[H(E|X_B)_{\omega^{\gamma,X}} + H(X_B)_{\omega^{\gamma,X}}\right] \\ & + (1-p_X)\left[H(E|X_B)_{\omega^{\gamma,P}} + H(X_B)_{\omega^{\gamma,P}}\right] \\ & - H(AB)_{\omega^\gamma} - \frac{1}{\sqrt{n}}\Delta - \frac{\ell_{\mathrm{EC}}}{n} - \frac{1}{n}\log_2\frac{1}{\epsilon_{\mathrm{s}}^2\epsilon_{\mathrm{c}}}. \end{aligned}$$

In the theoretical asymptotic limit for an infinite number of samples $n \to \infty$ and perfect security $\epsilon \to 0$, the key rate r tends to

$$\begin{aligned} r_\infty = {} & p_X\left(\beta I(X_A, X_B)_{\omega^{\gamma,X}} + H(E)_{\omega^{\gamma,X(X=0)}} - H(AB)_{\omega^\gamma}\right) \\ & + (1-p_X)\left(\beta I(X_A, X_B)_{\omega^{\gamma,P}} + H(E)_{\omega^{\gamma,P(P=0)}} - H(AB)_{\omega^\gamma}\right). \end{aligned}$$

Note that in the asymptotic limit the error correction protocol achieves the Shannen rate, and thus, one could set $\beta = 1$. However, since we only use the asymptotic limit to compare the key rate to the finite-size effects which are not connected to the efficiency of the error correction protocol, we treat β as a constant over all sample sizes.

2.4. Parameter estimation

To calculate the secure key rate we need to construct the confidence set $\mathcal{C}_{\epsilon_{\text{pe}}}$ which is defined such that the covariance matrix describing the real state lies within $\mathcal{C}_{\epsilon_{\text{pe}}}$ with probability $1-\epsilon_{\text{pe}}$. As our states are two-mode squeezed vacuum states, the first moment vanishes and the state is fully described by its covariance matrix. It is reconstructed during the parameter estimation step from the discarded samples and the revealed common subset of length k using a maximum likelihood estimator. The sample covariance matrix is then estimated by

$$\tilde{\gamma}_{\mu\nu} = \frac{1}{n_{\mu\nu}} \sum_{i=1}^{n_{\mu\nu}} x_i^{\mu} x_i^{\nu},$$

where x_i^{μ} and x_i^{ν} are the samples measured simultaneously by Alice and Bob in μ and ν quadrature, respectively. $n_{\mu\nu}$ is the number of samples used for the covariance estimation which might in our case be different for different entries. The distribution of the sample covariance matrix $\tilde{\gamma}$ is given by [37]

$$n\tilde{\gamma} \sim W_4(\gamma, n-1),$$

where $W_4(\gamma, n-1)$ is the Wishart distribution. Hence, the standard deviation for a single entry of the covariance matrix takes the form

$$\sigma_{\mu\nu} \approx \sqrt{\frac{\tilde{\gamma}_{\mu\nu}^2 + \tilde{\gamma}_{\mu\mu}\tilde{\gamma}_{\nu\nu}}{n_{\mu\nu}}}.$$

For a large enough number of samples the confidence set is then constructed by

$$\mathcal{C}_{\epsilon_{\text{pe}}} = \left\{\gamma \,|\, \tilde{\gamma}_{\mu\nu} - z_{\epsilon_{\text{pe}}}\sigma_{\mu\nu} \leqslant \gamma_{\mu\nu} \leqslant \tilde{\gamma}_{\mu\nu} + z_{\epsilon_{\text{pe}}}\sigma_{\mu\nu}\right\}, \tag{5}$$

where $z_{\epsilon_{\text{pe}}}$ is chosen such that

$$1 - \text{erf}\left(\frac{z_{\epsilon_{\text{pe}}}}{\sqrt{2}}\right) \leqslant \epsilon_{\text{pe}}$$

is fulfilled. Here, erf is the error function which is defined by

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \mathrm{d}t \exp\left(-t^2\right).$$

3. Experiment

A schematic view of the experiment is shown in figure 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 [38] and served as a pump for the squeezed-light source which consisted of a $1 \times 2 \times 9.3\,\text{mm}^3$ PPKTP crystal. One of the end faces of the squeezed-light source's crystal 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 and 1550 nm, respectively. The other end face 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 a 23 mm air gap between

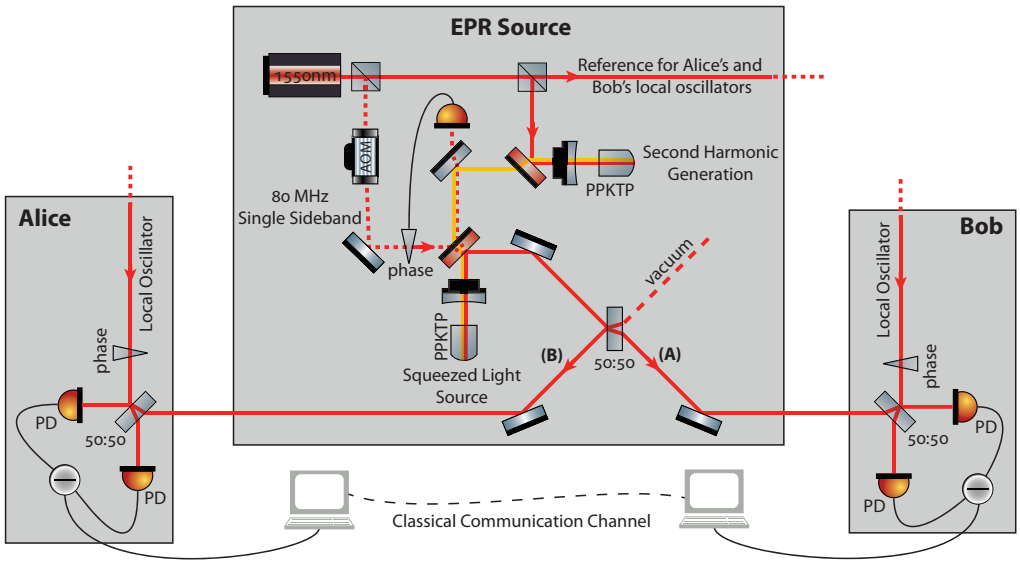


Figure 1. Schematic view of the experiment. The beam of a 1550 nm fiber laser (red) was frequency doubled (yellow) and used as a pump for the squeezed-light source. The squeezed beam was overlapped with a vacuum mode at a 50 : 50 beam splitter to produce a pair of EPR entangled beams. The field quadratures 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.

the crystal and the coupling mirror the cavity had a finesse of 60 at 1550 nm, a 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 that was coupled into the cavity through the high-reflective mirror was used to lock both the length of the cavity and the phase of the pump. The output of the squeezed-light source was split from the pump by a dichroic beam splitter and superimposed 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. For this 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. By changing the relative phase between the local oscillator and the quantum field, the measured field quadrature could be chosen. Whereas for QKD Alice and Bob only have to randomly measure the amplitude and phase quadrature, also a linear combination of these is needed to reconstruct the full covariance matrix. Therefore, we implemented a single sideband technique to be able to lock both homodyne detectors independently to any quadrature angle. An 80 MHz frequency shifted beam, produced by an acousto-optical modulator, was coupled into the squeezing path through the dichroic beam splitter and was phase locked to the control beam leaking through 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 the homodyne detector could be set to measure any field quadrature angle.

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

4. Experimental results

To characterize our EPR source we fully reconstructed the covariance matrix of the bipartite state. The full reconstruction of the covariance matrix followed a protocol described in [23], where the complete covariance matrix of a Gaussian state was measured for the first time. The protocol goes as follows:

(i) Alice and Bob both measure the amplitude quadrature.

(ii) Alice and Bob both measure the phase quadrature.

(iii) Alice measures the amplitude quadrature, whereas Bob simultaneously measures the phase quadrature.

(iv) Alice measures the phase quadrature, whereas Bob simultaneously measures the amplitude quadrature.

(v) Alice and Bob both measure a linear combination of the amplitude and phase quadrature. In our case we chose the 45° angle for both parties.

Following the protocol above we recorded 5×10^6 samples for each quadrature combination using a pump power of 235 mW for the squeezed-light source which allowed the observation of 11.1 dB squeezing and 16.6 dB anti-squeezing. From these data, we reconstructed the covariance matrix which reads

$$\Gamma = \left(\begin{array}{cc|cc} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ \hline 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{array}\right). \tag{6}$$

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 anti-correlations 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 deviations from zero show that the measurements were not perfectly orthogonal but close. To verify that our source is indeed an EPR source we calculated the EPR–Reid covariance product [39]

$$\min_g \mathrm{Var}(X_A - g X_B) \min_h \mathrm{Var}(P_A - h P_B) < 1,$$

which was $0.31 < 1$ for our states setting a new benchmark with entanglement generated by a squeezed mode superimposed with a vacuum mode. In comparison with [20] this was achieved by reducing the optical loss and thus, by producing more squeezing. Furthermore, the excess noise which was present in [20] was reduced.

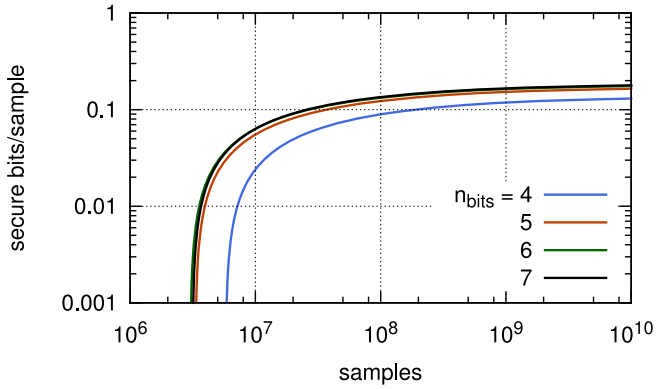
Using the recorded data we analyzed the feasibility to use our state for QKD. For all calculations, we assumed the covariance matrix of equation (6) to be the reconstructed covariance matrix in the parameter estimation phase of the QKD protocol, regardless for how many samples the key rate was calculated. We then constructed the confidence set assuming k samples were used to estimate the correlation terms between Alice and Bob in the covariance matrix. All diagonal terms were assumed to be estimated by using the total of N samples measured in one quadrature by each party. For all of the following simulations, the number of samples k used for parameter estimation was optimized to yield a maximal secure key length.

Figure 2(a) shows the calculated key rate for our state versus the total number of measured samples when omitting all samples measured in the P quadrature (anti-squeezed quadrature), i.e. $p_X = 1$. The key rate is given in secure bits per measured sample, i.e. the total number of samples before sifting. The parameters used for the calculation were $\epsilon_{\text{pe}} = \epsilon_{\text{c}} = \epsilon_{\text{s}} = 10^{-16}$ and $\beta = 0.9$ for the efficiency of the error correction. α was chosen eight times the standard deviation of the quadrature given by the covariance matrix of equation (6). Each curve in the figure was calculated for a different number of bins which was taken as $2^{n_{\text{bits}}}$ by choosing an appropriate δ. For $n_{\text{bits}} \geqslant 6$ the asymptotic maximum of the key rate is reached. For 10^9 samples, which is experimentally challenging but achievable [27], the key rate is already close to the maximum value of about 0.18 bits per sample and even for 10^8 samples it is not much lower.

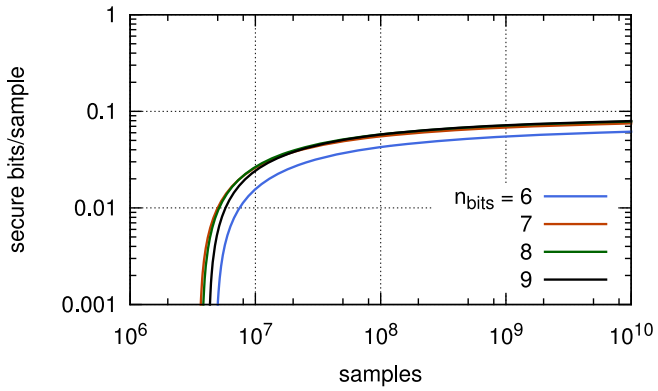
Figure 2(b) shows the same as figure 2(a) but with the samples from the X quadrature omitted, i.e. $p_X = 0$. To reach the asymptotic value for the key rate $n_{\text{bits}} \geqslant 8$ is needed. In comparison to the key rate for only the X quadrature samples the asymptotic key rate is lower with about 0.08 bits per sample. Here, also about 10^9 samples are necessary to reach a value close to the maximum and also for 10^8 samples the key rate is with about 0.06 bits per sample not much lower.

In figure 2(c) samples from both X and P quadrature measurements were used to compute the secure key rate, i.e. $p_X = 0.5$. For the calculation we used $n_{\text{bits}} = 6$ for the X quadrature and $n_{\text{bits}} = 8$ for the P quadrature. The key rate reaches 0.25 bits per sample for a large number of measured samples which is similar to but not quite the sum of the key rates achieved when omitting samples from one of the quadratures. This is due to the larger confidence set since less samples were used for its construction.

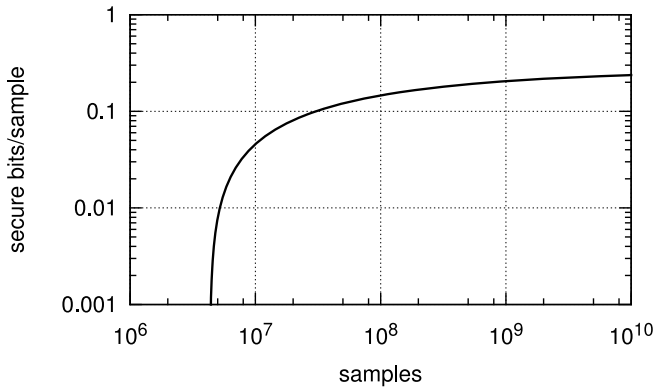
When sending Bob's part of the entangled state through an optical fiber the key rate versus the distance is shown in figure 3. We assumed a coupling efficiency of 95% into the optical fiber [40] and an optical loss of 0.2 dB km^{-1}. To maximize the achievable distance we omitted the samples from the P quadrature. Considering only samples from the P quadrature would yield a maximal distance of only about 2 km and considering both X and P quadrature measurements would yield about 8 km for an infinite number of samples. The parameters used for the calculation were chosen as for figure 2, in particular $n_{\text{bits}} = 6$ and $\epsilon_{\text{pe}} = 10^{-16}$. From the figure we read that the absolute maximal distance for our state is about 37.5 km. Taking a realistic number of samples [27] the reachable distance shrinks to about 9 km for 10^8 samples and about 18 km for 10^9 samples. These values are limited by the parameter estimation. Curves with a relaxed parameter estimation security parameter of $\epsilon_{\text{pe}} = 10^{-12}$ and 10^{-10} are shown for 10^8 samples in the figure. For $\epsilon_{\text{pe}} = 10^{-10}$ [25] the distance increases to about 10.5 km. For the calculation we assumed that no excess noise is introduced by the fiber as stated in [41]. Excess noise introduced by the electronic dark noise of the homodyne detectors is instead already included in the reconstructed covariance matrix. As the error correction efficiency depends



(a) Includes only X quadrature measurements, i.e. $p_X = 1$.



(b) Includes only P quadrature measurements, i.e. $p_X = 0$.



(c) Includes both X and P quadrature measurements, i.e. $p_X = 0.5$. $n_{\text{bits}} = 6$ for the X quadrature and $n_{\text{bits}} = 8$ for the P quadrature.

Figure 2. Secure key rate versus the number of measured samples. For each number of samples on the x-axis the number of samples k used for parameter estimation was optimized. (a) Includes only X quadrature measurements, i.e. $p_X = 1$. (b) Includes only P quadrature measurements, i.e. $p_X = 0$. (c) Includes both X and P quadrature measurements, i.e. $p_X = 0.5$. $n_{\text{bits}} = 6$ for the X quadrature and $n_{\text{bits}} = 8$ for the P quadrature.

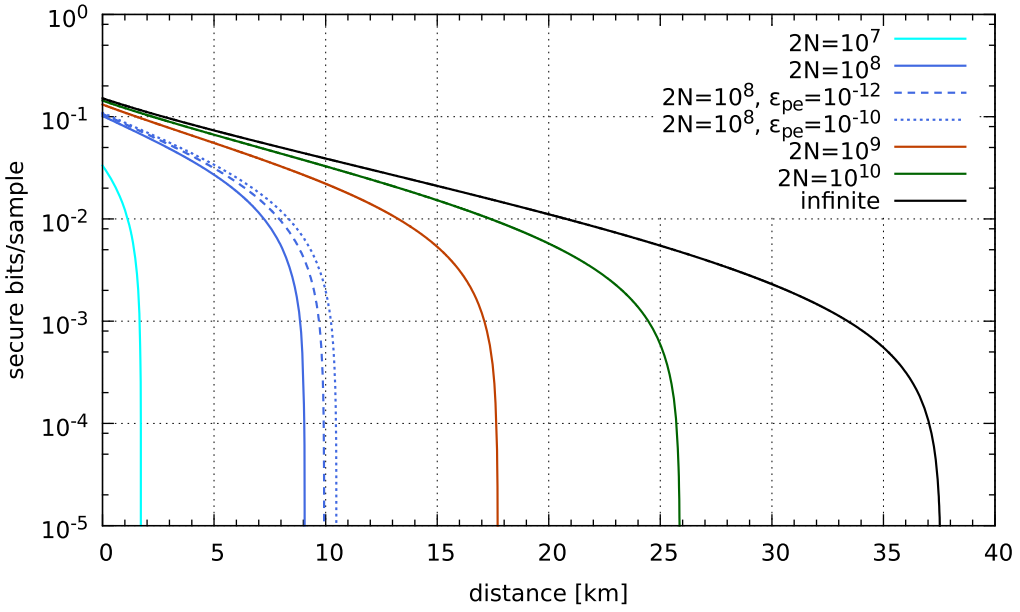


Figure 3. Key rate versus distance when sending one part of the entangled beam through an optical fiber. The key rate is given as the number of secure bits per measured samples, i.e. before sifting. We assumed a coupling efficiency of 95% into the optical fiber and an optical loss of 0.2 dB km^{-1}. The curves are plotted for different numbers of measured samples $2N$. The parameter estimation security was chosen $\epsilon_{\mathrm{pe}} = 10^{-16}$ except for the dashed lines. Samples from the P quadrature were omitted since otherwise only short distances would be possible (see text).

on the given signal-to-noise ratio, the actually maximal achievable distance depends on the availability of efficient error correcting codes [27].

5. Conclusion

We have presented an analysis of a Gaussian entanglement source involving a squeezed mode and a vacuum mode regarding entanglement-based QKD under the assumption of collective attacks including finite-size effects. While in the present experiment the entanglement has been distributed on an optical table, coupling one part of the bipartite state into a standard optical telecommunication fiber and building Bob's detector remotely would allow for QKD in local-area networks. The local oscillator for Bob's homodyne detector could be served e.g. from an auxiliary laser at Bob's site which could be phase locked to the control beam accompanying the entangled state. This scheme also ensures that phase noise introduced by the fiber is not crucial below the unity-gain frequency of the phase-locked loop. Our analysis revealed that a distance of more than 10 km is possible with a reasonable but challenging number of measured samples of 10^9 even though a vacuum mode was included in the generation of the states.

The effective sampling rate without introducing any correlations between samples, was 25 kHz for the implemented data acquisition. Thus, measuring 10^8 samples would take about 66 min. Improving the data acquisition an effective measurement rate of about 1 MHz should

be feasible with the setup, reducing the measurement time to about 2 min. The stability of our setup exceeded 15 min and was only limited by large drifts caused by thermal fluctuations of the environment which could not be compensated by the phase actuators. Hence, to be able to measure 10^9 samples, actuators with larger ranges might be necessary. As for achieving a large distance, only samples measured in the squeezed quadrature are used, a probability larger than 50% for measuring the squeezed quadrature compared to the anti-squeezed quadrature would decrease the necessary measurement time. Since a squeezing bandwidth of more than 100 MHz was already demonstrated [42], a QKD system involving a single squeezed-light source could achieve significant overall key rates.

Although the restriction to a single squeezed input mode, as presented here, reduces the complexity of the source, a full scheme with two squeezed fields superimposed at a balanced beam splitter will achieve higher key rates. For the full scheme the achievable distance for 10^9 samples would be about 28 km in comparison to about 17 km for a single squeezed-light source. While these values were calculated for an entangled state generated by two identical squeezed modes, our security analysis provided here also allows the use of states generated by squeezed modes with different squeezing strengths. Furthermore, the full scheme with two squeezed vacuum modes is a promising candidate for the first implementation ever of a CV QKD system which provides security under coherent attacks [26].

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 number WE-1240/12-1 and from BMBF project QUOREP. FF acknowledges support from Japan Society for the Promotion of Science (JSPS) by KAKENHI grants number 24-02793. RFW acknowledges support by the EU FP 7 project COQUIT (grant agreement number 233747).

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. 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 *et al* 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] Hillery M 2000 *Phys. Rev.* A **61** 022309
[9] Gottesman D and Preskill J 2001 *Phys. Rev.* A **63** 022309
[10] Rodo C, Romero-Isart O, Eckert K and Sanpera A 2007 *Open Syst. Inform. Dyn.* **14** 69–80
[11] Ou Z Y, Pereira S F, Kimble H J and Peng K C 1992 *Phys. Rev. Lett.* **68** 3663–6
[12] Zhang Y, Wang H, Li X, Jing J, Xie C and Peng K 2000 *Phys. Rev.* A **62** 023813
[13] Schori C, Sorensen J L and Polzik E S 2002 *Phys. Rev.* A **66** 033802
[14] Laurat J, Coudreau T, Keller G, Treps N and Fabre C 2005 *Phys. Rev.* A **71** 022313

[15] Keller G, D'Auria V, Treps N, Coudreau T, Laurat J and Fabre C 2008 *Opt. Express* **16** 9351–6
[16] Wang Y, Shen H, Jin X, Su X, Xie C and Peng K 2010 *Opt. Express* **18** 6149–55
[17] Bowen W P, Schnabel R, Lam P K and Ralph T C 2003 *Phys. Rev. Lett.* **90** 043601
[18] Takei N, Lee N, Moriyama D, Neergaard-Nielsen J S and Furusawa A 2006 *Phys. Rev.* A **74** 060101
[19] Hage B, Janousek J, Armstrong S, Symul T, Bernu J, Chrzanowski H M, Lam P K and Bachor H A 2011 *Eur. Phys. J.* D **63** 457–61
[20] Eberle T, Händchen V, Duhme J, Franz T, Werner R F and Schnabel R 2011 *Phys. Rev.* A **83** 052329
[21] Steinlechner S, Bauchrowitz J, Eberle T and Schnabel S 2013 *Phys. Rev.* A **87** 022104
[22] Silberhorn C, Lam P K, Weiß O, König F, Korolkova N and Leuchs G 2001 *Phys. Rev. Lett.* **86** 4267–70
[23] DiGuglielmo J, Hage B, Franzen A, Fiurasek J and Schnabel R 2007 *Phys. Rev.* A **76** 012323
[24] Su X, Wang W, Wang Y, Jia X, Xie C and Peng K 2009 *Europhys. Lett.* **87** 20005
[25] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev* A **81** 062343
[26] Furrer F, Franz T, Berta M, Leverrier A, Scholz V, Tomamichel M and Werner R 2012 *Phys. Rev. Lett.* **109** 100502
[27] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nature Photon.* **7** 378–81
[28] Canetti R 2001 *Proc. IEEE Symp. Found. Comput. Sci.* **42** 136–45
[29] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zürich
[30] Müller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[31] Berta M, Furrer F and Scholz V B 2011 arXiv:1107.5460
[32] Furrer F, Aberg J and Renner R 2011 *Commun. Math. Phys.* **306** 165–86
[33] Eisert J, Scheel S and Plenio M B 2002 *Phys. Rev. Lett.* **89** 137903
[34] Fiurasek J 2002 *Phys. Rev. Lett.* **89** 137904
[35] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[36] Martinez-Mateo J, Elkouss D and Martin V 2012 *Quantum Inf. Comp.* **12** 791–812
[37] Johnson R and Wichern D 2007 *Applied Multivariate Statistical Analysis* 6th edn (Upper Saddle River, NJ: Pearson Prentice-Hall)
[38] 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
[39] Reid M D 1989 *Phys. Rev.* A **40** 913–23
[40] Mehmet M, Eberle T, Steinlechner S, Vahlbruch H and Schnabel R 2010 *Opt. Lett.* **35** 1665-7
[41] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev.* A **72** 050303
[42] Mehmet M, Vahlbruch H, Lastzka N, Danzmann K and Schnabel R 2010 *Phys. Rev.* A **81** 013814