

PAPER • OPEN ACCESS

Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels

To cite this article: Vladyslav C Usenko *et al* 2012 *New J. Phys.* **14** 093048

View the [article online](#) for updates and enhancements.

You may also like

- [Entanglement reactivation in separable environments](#)
Stefano Pirandola
- [How to control decoherence and entanglement in quantum complex systems?](#)
V M Akulin, G Kurizki and D A Lidar
- [Effect of depolarizing noise on entangled photons](#)
Ruchipas Bavontaweepanya

Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels

Vladyslav C Usenko^{1,2,6}, Bettina Heim^{3,4,5,6}, Christian Peuntinger^{3,4}, Christoffer Wittmann^{3,4}, Christoph Marquardt^{3,4}, Gerd Leuchs^{3,4} and Radim Filip¹

¹ Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

² Bogolyubov Institute for Theoretical Physics of National Academy of Sciences, Metrolohichna Street 14-b, 03680 Kiev, Ukraine

³ Max Planck Institute for the Science of Light, Guenther-Scharowsky-Strasse 1/Building 24, 91058 Erlangen, Germany

⁴ Institute of Optics, Information and Photonics, Friedrich-Alexander University of Erlangen-Nuremberg (FAU), Staudtstrasse 7/B2, 91058 Erlangen, Germany

⁵ Erlangen Graduate School in Advanced Optical Technologies (SAOT), FAU, Paul-Gordan-Strasse 6, 91052 Erlangen, Germany

E-mail: usenko@optics.upol.cz and bettina.heim@mpl.mpg.de

New Journal of Physics **14** (2012) 093048 (20pp)

Received 3 July 2012

Published 26 September 2012

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/14/9/093048

Abstract. Entanglement properties of Gaussian states of light as well as the security of continuous variable quantum key distribution with Gaussian states in free-space fading channels are studied. These qualities are shown to be sensitive to the statistical properties of the transmittance distribution in the cases when entanglement is strong or when channel excess noise is present. Fading, i.e. transmission fluctuations, caused by beam wandering due to atmospheric turbulence, is a frequent challenge in free-space communication. We introduce a method of fading discrimination and subsequent post-selection of the corresponding sub-states and show that it can improve the entanglement

⁶ Authors to whom any correspondence should be addressed.



Content from this work may be used under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike 3.0 licence](https://creativecommons.org/licenses/by-nc-sa/3.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

resource and restore the security of the key distribution over a realistic fading link. Furthermore, the optimal post-selection strategy in combination with an optimized entangled resource is shown to drastically increase the protocol's robustness to excess noise, which is confirmed for experimentally measured fading channel characteristics. The stability of the result against finite data ensemble size and imperfect channel estimation is also addressed.

Contents

1. Introduction	2
2. Fading channels	3
3. Fading due to beam wandering	9
4. Real fading channel	13
5. Effects of a limited ensemble size for the key rate and channel estimation	16
6. Summary and conclusions	19
Acknowledgments	19
References	19

1. Introduction

Entanglement in quantum states of light is well known to be an essential resource for quantum information processing, in particular for quantum key distribution (QKD) [1, 2], which is to date the most developed application in the field of quantum information. As an alternative to the first proposals [3, 4] and numerous QKD implementations based on discrete variable coding (e.g. the recent ones in fiber [5, 6] and open-space [7] channels), protocols for QKD were developed using a continuous variable (CV) approach [8], aimed at improving the robustness and applicability of quantum information protocols. The implementation of CV QKD protocols in their optical realization is well studied in the case of optical fiber channels. In particular, the security of CV QKD with Gaussian states was proven for any channel with pure constant attenuation and, to some extent, for noisy channels with constant attenuation [9–14]. However, Gaussian protocols need additional analysis when atmospheric channels are considered, since such channels show a prominent, temporal evolution of the channel transmission. Indeed, in free-space links, fixed attenuation is never the case, as the transmittance fluctuates due to atmospheric effects. Such fading channels are characterized by a distribution of transmittance values. At the same time, atmospheric links are of utmost importance, providing the possibility for short- and mid-range communication without strong requirements to the infrastructure and, moreover, the possibility for truly long-distance communication, e.g. over satellite connections.

In the case of discrete variable states and protocols, the impact of atmospheric channels on qubit-based QKD was actively investigated, for example, in [15–19]. The most negative effect of the free-space channel in this case is the background light (in the CV-based implementations, it is effectively filtered out by the homodyne detection [20]). The impact of fading channels on discrete variable protocols is similar to that of a constant attenuation and results in a decrease of the communication rate (which can also be partly compensated for by filtering [23]), but can preserve the entanglement properties upon post-selected measurements [24]. However, the effect of fading on CV quantum states is essentially different from the typical fixed loss and

additive Gaussian noise present in fiber-type channels. The fading noise is multiplicative, which on the one hand quickly destroys the Gaussian quantum features such as entanglement and purity but on the other hand offers different possibilities to recover them [25–28]. The noise due to atmospheric fluctuations is relatively slow (typically several kHz [29]) compared to the achievable homodyne detection rates (hundreds of MHz [30]), which means that it can be partially estimated using a strong optical beam when entanglement properties are analyzed. In the case of QKD, the eavesdropping scenario must be considered. Therefore, the fading properties must be identified using the same alphabet of quantum states as that used for communication.

In this paper, we analyze the effect of an atmospheric fading channel on the entanglement and security properties of protocols using Gaussian quantum states of light and consider the use of post-selection (PS) of sub-channels, with the aim of improving the entangled resource and restoring the security of the CV QKD protocol in case it was broken by atmospheric fluctuations. We demonstrate the negative impact of fading on Gaussian entanglement and security, considering a general class of fading channels as well as a particular theoretical model of fading caused by beam wandering [31] and show the possibility to restore entanglement and security by PS of sub-channels. Thus, based on the knowledge of the overall channel properties obtained from estimation, a higher key rate or stronger entanglement can be shared by the proper selection of sub-channels with less fading. Such a method presents a feasible alternative to the experimentally challenging state distillation [25]. Moreover, we analyze the PS method considering experimentally measured transmission statistics of a real free-space channel and find an increase of the secret key rate in such a realistic scenario.

The paper is organized as follows. In section 2, we describe fading channels in general and show the negative effect of fading on Gaussian states entanglement and the possible application to CV QKD. In section 3, we theoretically consider the particular case of fading channels, where transmittance fluctuations are caused by beam wandering, showing the effect of fading on entanglement and security. We introduce PS, which we show to be capable of restoring entanglement of the states and security of the respective Gaussian protocol. In section 4, we apply our analysis to a real fading channel, the transmittance distribution of which was measured experimentally. In section 5, we numerically address the finite-size effects of the limited data ensembles and imperfect estimation on the PS of sub-channels, showing the stability of our results in the finite-size context.

2. Fading channels

A quantum communication scheme over a fading channel is presented in figure 1. Alice and Bob share an entangled two-mode squeezed vacuum [8] state, which is characterized by the quadrature variance V of each of its modes. Half of the entangled state is sent through a fading channel to Bob. Bob makes a homodyne measurement of the amplitude or phase quadrature, and Alice measures both quadratures in a balanced heterodyne scenario. Such an entanglement-based CV QKD scheme is equivalent to a prepare-and-measure scheme (see figure 1, left inset), in which Alice generates a coherent state, applies random Gaussian displacement of variance $\sigma = V - 1$ to the generated state and sends it through a fading channel to Bob, who then also makes a homodyne measurement. Note that while the entangled state variance V is related to the non-classicality of a pure state (being $V = \cosh 2r$, where r is the squeezing parameter) and high values (tens of shot-noise units (SNU)) are experimentally challenging

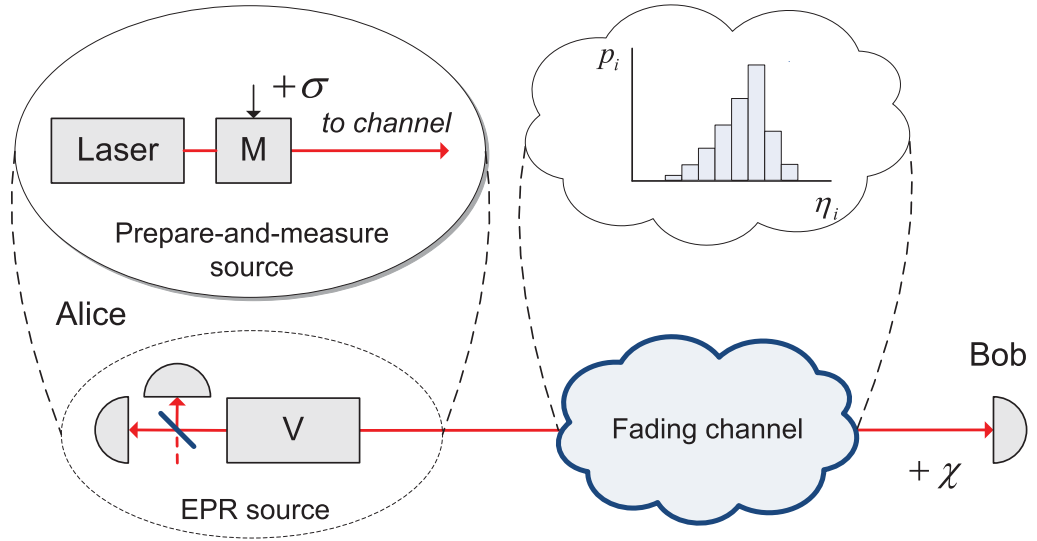


Figure 1. EPR entanglement-based QKD over a fading channel. Alice and Bob share an entangled state of variance V ; one of the modes is transmitted to Bob through a fading channel described by a distribution of transmittance values $\{\eta_i\}$. While Alice directly applies heterodyne measurements, Bob makes homodyne measurements allowing him to characterize the channel and estimate excess noise. Left inset: the equivalent prepare-and-measure scheme. Alice generates a coherent state, displaces it in phase space with a variance of $\sigma = V - 1$ using the modulator M and sends it to Bob. Right inset: illustrative discretized transmittance distribution of a fading channel.

to achieve, the displacement variance σ in the prepare-and-measure scenario is the result of a feasible modulation and can reach high values (up to hundreds of SNU). Thus, despite the simple equivalence between those two implementations, we stick to the limited values of V when considering entanglement properties, but assume a wider region for σ when estimating the security, as it can always be implemented with a high modulation variance in the prepare-and-measure scenario.

In our work, we deal with Gaussian states of light. Such states can be explicitly described by the covariance matrices, i.e. matrices of the second moments of the quadrature operators, which we introduce through mode annihilation and creation operators as $x = a^\dagger + a$ and $p = i(a^\dagger - a)$. Thus, the variance of the vacuum fluctuations is 1.

Let the channel be described by a distribution of transmittance values $\{\eta_i\}$ with probabilities $\{p_i\}$. The evolution of a Gaussian state over a purely attenuating fading channel was shown to be governed by two parameters of the attenuation distribution—the mean value of transmittance $\langle\eta\rangle$ and the mean of the square root of transmittance $\langle\sqrt{\eta}\rangle$ [28]. Indeed, the covariance matrix of a two-mode squeezed vacuum state with variance $V \geq 1$

$$\gamma_{AB} = \begin{pmatrix} V\mathbb{I} & \sqrt{V^2 - 1}\sigma_z \\ \sqrt{V^2 - 1}\sigma_z & V\mathbb{I} \end{pmatrix} \quad (1)$$

after a channel with transmittance η_i in mode B is given by

$$\gamma_{AB}^i = \begin{pmatrix} V\mathbb{I} & \sqrt{\eta_i}\sqrt{V^2-1}\sigma_z \\ \sqrt{\eta_i}\sqrt{V^2-1}\sigma_z & (V\eta_i + 1 - \eta_i + \chi)\mathbb{I} \end{pmatrix} \quad (2)$$

following the input–output relation for the quadrature vectors $r = (x, p)^T$ of modes 1 (signal mode B in our case) and 2 (vacuum input mode of the purely lossy i th sub-channel) in the form

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}_{\text{out}} = \begin{pmatrix} \sqrt{\eta_i}\mathbb{I} & \sqrt{1-\eta_i}\mathbb{I} \\ -\sqrt{1-\eta_i}\mathbb{I} & \sqrt{\eta_i}\mathbb{I} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}_{\text{in}}, \quad (3)$$

where $\sqrt{\eta_i}$ stands for the transmittance of a coupling beam splitter, $\mathbb{I} = \text{diag}(1, 1)$ is the unity matrix and $\sigma_z = \text{diag}(1, -1)$ is the Pauli matrix. We also assume the presence of excess noise χ , which we later consider untrusted in the so-called ‘pessimistic scenario’ (this can be detector noise or untrusted channel noise, scaled by the channel attenuation).

The overall state after a fading channel is the mixture of states after individual sub-channels; thus the Wigner function of the state is the sum of Wigner functions of the states after sub-channels weighted by sub-channel probabilities [28]. The elements of the total covariance matrix after the fading channel $\{\eta_i\}$ are then the convex sum of the moments given by (2) and the covariance matrix of the resulting mixed state after a fading channel $\{\eta_i\}$ in mode B is then given by

$$\gamma'_{AB} = \begin{pmatrix} V\mathbb{I} & \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\sigma_z & (V\langle\eta\rangle + 1 - \langle\eta\rangle + \chi)\mathbb{I} \end{pmatrix}. \quad (4)$$

Let us estimate the impact of a fading channel on the quantum properties of a state propagating through such a channel and on the security of coherent state CV QKD. From the covariance matrix of the state after the fading channel (4) it is evident that the noiseless fading channel can be considered as a non-fading channel with transmittance $\langle\sqrt{\eta}\rangle^2$ and excess noise caused by fading $\epsilon_f = \text{Var}(\sqrt{\eta})(V-1)$ so that the variance of the mode B after the fading channel becomes

$$V'_B = \langle\sqrt{\eta}\rangle^2(V-1) + \epsilon_f + \chi + 1, \quad (5)$$

where $\text{Var}(\sqrt{\eta}) = \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2$. Thus, the effect of a fading channel in terms of the covariance matrix can be described as Gaussian state variance-dependent excess noise. Further, we focus on the properties of the state, described by the covariance matrix, as they are crucial for Gaussian CV QKD protocols.

Evidently, fading reduces the purity of the initially pure Gaussian states compared to channels with a fixed attenuation. The purity of a Gaussian two-mode state, described by the covariance matrix γ_{AB} , can be expressed as $p(\gamma_{AB}) = 1/\sqrt{\text{Det}\gamma_{AB}}$ [32] (thus having the meaning of the Gaussian mixedness of the state), $\text{Det}\gamma_{AB}$ being the determinant of the covariance matrix. In the case of the fading channel, acting on the state (1), the purity reads

$$p(\gamma'_{AB}) = \frac{1}{\text{Var}(\sqrt{\eta})V(V-1) + V(1 - \langle\sqrt{\eta}\rangle^2) + \langle\sqrt{\eta}\rangle^2}. \quad (6)$$

As fading increases (which means an increase of the variance $\text{Var}(\sqrt{\eta})$), the purity is reduced, while for an arbitrarily strong fading $\text{Var}(\sqrt{\eta}) = 1/4$ (corresponding to equiprobable

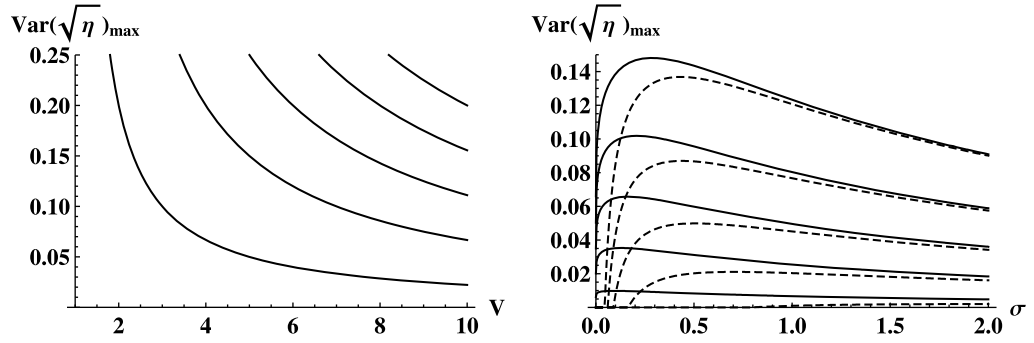


Figure 2. Left: maximal entanglement-preserving $\text{Var}(\sqrt{\eta})$ (in terms of logarithmic negativity) versus the state variance V for different values of $\langle \sqrt{\eta} \rangle^2$ (from top to bottom: 0.9, 0.7, 0.5, 0.3, 0.1) in the absence of excess noise (which otherwise does not significantly affect the obtained dependences). Right: maximal security-preserving $\text{Var}(\sqrt{\eta})$ (in the case of collective attacks) versus the Gaussian modulation variance $\sigma = V - 1$ for different values of $\langle \sqrt{\eta} \rangle^2$ (from top to bottom: 0.9, 0.7, 0.5, 0.3, 0.1) in the absence of untrusted noise (solid lines) and upon untrusted detection noise $\chi = 0.012$ (dashed lines).

transmittance values of 0 and 1) the purity is given by $p(\gamma_{AB}) = 4/(V + 1)^2$, which is degraded with increasing V compared to any channel with fixed transmission. In the opposite limit of two uncorrelated vacuum modes $V = 1$, the state is always pure with $p = 1$.

Similarly, fading reduces Gaussian entanglement, which we consider in terms of log-negativity [33] $E_{\text{LN}}(\gamma) = \max[0, -\ln(\tilde{\lambda}_-)]$, where $\tilde{\lambda}_-$ is the smallest symplectic eigenvalue of the partially transposed state of the Gaussian state described by the covariance matrix γ [32]. Gaussian entanglement of the state described by the covariance matrix (4) is then broken given a variance V by the value of $\text{Var}(\sqrt{\eta})_{\text{max,ent}} = 2\langle \sqrt{\eta} \rangle^2 / (V - 1)$. If the detector or other excess noise is present, then the maximum entanglement-breaking fading variance is

$$\text{Var}(\sqrt{\eta})_{\text{max,ent}} = \frac{2(\langle \sqrt{\eta} \rangle^2 - 1) - \chi + \sqrt{4(1 + \langle \sqrt{\eta} \rangle^2)^2 + \chi^2}}{2(V - 1)}, \quad (7)$$

where χ is the excess noise after the channel, assumed to be independent of fading. For high state variance $V \gg 1$, the maximum tolerable $\text{Var}(\sqrt{\eta})_{\text{max,ent}}$ tends to 0, which means that even small fading is Gaussian entanglement breaking. At the same time, when the variance is low ($V \rightarrow 1$), entanglement is preserved for any fading. The typical behavior of the fading variance threshold with respect to state variance is given in figure 2 (left) for different mean transmittance values. Evidently, the robustness of entanglement to fading is drastically decreased with an increase of the state variance, while additional detection (or channel) excess noise of reasonably small amounts does not play a significant role.

Let us now consider the impact of a fading channel on the security of a protocol based on Gaussian states. We refer to a certain CV QKD coherent state protocol [9], whose security analysis in the general case is based on virtual Gaussian entanglement [34]. Robustness of the protocol against collective attacks (which also implies security against the most general coherent attacks [35]) was shown using the extremality of Gaussian states [36] and the subsequent optimality of Gaussian attacks [37, 38]. This enables a security analysis based solely on the covariance matrix description of the states. However, this implies the necessity for the trusted

parties to know the channel characteristics in order to explicitly derive the upper bound on the knowledge about the key bits accessible to a potential eavesdropper. This and the further assumptions required to analyze the security of the coherent state protocol over a fading channel are explicitly given below.

Firstly, we make the standard CV QKD assumption that the trusted parties are able to estimate the channel transmittance η and check its stability during the transmission of data, which will contribute to the secure key (we refer to a given relatively stable transmittance as a sub-channel). This is experimentally feasible, as the typical rate of atmospheric channel fluctuations is of the order of kHz, while the modulation and detection rate is typically of the order of several MHz, i.e. at least thousands of signal or probe states can be transmitted during the stability time of the fading atmospheric channel. Thus, each measurement result in our case can be reliably attributed to the respective sub-channel within the given transmittance window over which the given signal state was transmitted.

Secondly, in order to make our analysis clear and focus on the discussed effects, we assume that the entangled (or prepared) states are pure. Consideration of realistic noisy sources will be the subject of further research. For the same reason and with the same perspectives, we assume perfect data post-processing.

Thirdly, we perform the analysis in the asymptotic limit, but finish the paper with the numerical estimation of finite data ensemble size effects, as it could be crucial in the conditions of the ensemble reduction due to PS. Similarly, we address the effect of imperfect channel loss estimation on our results.

Relying on the above-given assumptions, we consider in detail the effect of fading channels and the possibility to improve entanglement of the Gaussian states and the security of the respective CV QKD protocols by PS.

A lower bound on the key rate in the case of the most effective collective eavesdropping attacks in a reverse reconciliation scenario is well known to be $K = I_{AB} - \chi_{BE}$ [37, 38], where χ_{BE} is the Holevo quantity, which gives an upper bound for the leaked information, and is calculated through the von Neumann entropy of the eavesdropper state before the measurement on mode B and the state conditioned by the result of the measurement.

The mutual information I_{AB} between the trusted parties can be expressed through variances and conditional variances of the modes A and B as $I_{AB} = (1/2)\log(V_A^M/V_{A|B}^M)$ after heterodyne measurement at Alice (corresponding to conditional coherent state preparation). In this case Alice is measuring the observable $x_A^M = (x_A + x_0)/\sqrt{2}$ (x_M being the quadrature of mode A prior to heterodyne and x_0 being the quadrature of the vacuum input of the free port of a heterodyne detector), and mutual information reads

$$I_{AB} = \frac{1}{2} \log \frac{1}{1 - \frac{\langle \sqrt{\eta} \rangle^2 \sigma}{1 + \langle \eta \rangle \sigma + \chi}}. \quad (8)$$

The Holevo quantity, under the assumption that Eve is able to purify the state [12], is calculated through the symplectic eigenvalues $\lambda_{1,2}$ of the covariance matrix (4) after the channel and the symplectic eigenvalue λ_3 of the conditional matrix

$$\gamma_A^{xB} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{\text{MP}}\sigma_{AB}^T, \quad (9)$$

where γ_A , γ_B are the matrices describing the modes A and B individually and σ_{AB} is the matrix which characterizes correlations between the modes A and B . These matrices all together

construct the covariance matrix (4). MP stands for the Moore–Penrose inverse of a matrix (also known as pseudoinverse), and

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \quad (10)$$

Here, with no loss of generality, we assume that the x -quadrature is measured by Bob.

The Holevo quantity is then directly expressed through the symplectic eigenvalues as

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \quad (11)$$

where $G(x) = (x + 1)\log(x + 1) - x\log x$ is the bosonic entropic function [32]. Thus, a lower bound on the key rate can be estimated. Unfortunately, the expression for the case of collective attacks is too lengthy to be presented in the paper and the corresponding calculations were performed numerically.

Similarly to the entanglement and purity, the positivity of the key rate (being the prerequisite for secure key distribution) appears to be sensitive to interdependence of the mean values of $\{\eta_i\}$, in particular, to the variance $\text{Var}(\sqrt{\eta})$, which limits the security of the scheme.

Security breaking due to fading can already be observed in the case of individual attacks [9], where the maximum value of $\text{Var}(\sqrt{\eta})$ can be obtained analytically:

$$\text{Var}(\sqrt{\eta})_{\text{max,ind}} = \frac{\langle \sqrt{\eta} \rangle^2 \sigma - 2(\sigma + 1)(\chi + 1) + \sqrt{\langle \sqrt{\eta} \rangle^4 \sigma^2 + 4(\sigma + 1)^2}}{2\sigma(\sigma + 1)}. \quad (12)$$

Here, as mentioned, $\sigma = V - 1$ corresponds to the variance of coherent state modulation in the prepare-and-measure scenario and will be used in the security considerations as a measure of the modulation depth.

Similar behavior is observed in the case of collective attacks. Moreover, since Gaussian excess noise ϵ_f caused by fading is state variance dependent, it appears that for each $\langle \sqrt{\eta} \rangle$ there is an optimal value of modulation σ , which maximizes the tolerable fading variance $\text{Var}(\sqrt{\eta})$. The corresponding plot of maximal variance $\text{Var}(\sqrt{\eta})$ versus modulation σ is given in figure 2 (right) for different values of $\langle \sqrt{\eta} \rangle^2$. One can see that the stronger the attenuation is, the lower must be the applied modulation, in order to minimize the negative impact of fading. If an additional untrusted noise χ is present, then the maximal $\text{Var}(\sqrt{\eta})$ is drastically reduced in the regime of low modulation σ , even under the amount of untrusted noise, which is negligible for high modulation.

Thus, in order to restore the security of CV QKD upon fading channels either upon high modulation variance or in the presence of even a small amount of untrusted noise, the variance $\text{Var}(\sqrt{\eta})$ must be minimized. In practice, this could be achieved by demanding experimental efforts such as distillation [25], which is aimed at restoring the state prior to the measurement, or by the use of PS, when a subset of the channel transmittance distribution $\{\eta_i\}$ is selected to contribute to the statistical ensemble of the post-selected state and to the key data, in the case of the QKD. From the security point of view, this can be done in the already stated assumption that Alice and Bob are able to estimate the actual channel transmittances $\{\eta_i\}$, i.e. the estimation and information transmission are faster than the channel fluctuations. Thus, they post-select the sub-channels, which construct a new state with the covariance matrix of the form (4), and all Gaussian security analyses based on the extremality of Gaussian states and optimality of Gaussian attacks are valid for the new set of sub-channels and the new resulting state.

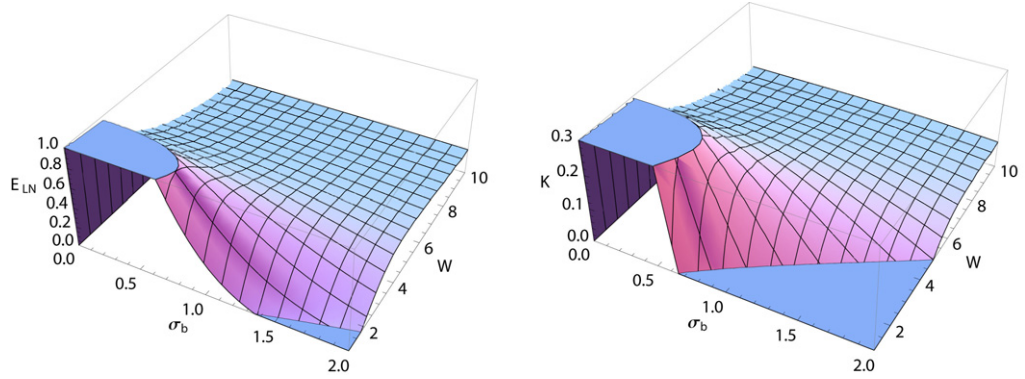


Figure 3. Left: the logarithmic negativity E_{LN} of the initially pure entangled state after a fading channel; right: key rate secure against collective attacks (in bits per measurement) for the initially pure entangled state after a fading channel. The state variance $V = 10$, the channel is characterized by the beam position variance σ_b and the spot size W relative to the aperture size $a = 1$.

In the further sections, we consider a particular theoretical model of a fading channel and then apply our results to the experimentally obtained distributions.

3. Fading due to beam wandering

In realistic atmospheric channels, the main impact of turbulence is beam wandering, when the beam spatially fluctuates around the receiver's aperture. Fading due to beam wandering is well described by a recently obtained statistical distribution [31], which, in the case of beam alignment around the aperture center, is given by the log-negative Weibull distribution. The distribution is governed by the shape and scale parameters, expressed by beam-center position variance σ_b^2 , beam-spot radius W , aperture radius a , and is cut at the maximum transmission value, which is given by

$$\eta_0^2 = 1 - \exp\left(-2\frac{a^2}{W^2}\right). \quad (13)$$

Here we numerically analyze the entanglement properties of the Gaussian states and the security of the respective CV QKD protocols over the fading channels, governed by beam wandering. First, we show how the logarithmic negativity behaves with respect to beam position variance σ_b and spot size W (normalized by the dimensionless aperture size $a = 1$, as the fading due to beam wandering depends on the ratio a/W); the results are given in figure 3 (left). Then, we estimate the key rate, secure against collective attacks, in the same fading channel assuming pure channel loss and no untrusted detection noise (results are given in figure 3, right). It is evident that both entanglement and security are sensitive to the variance of beam position fluctuations. At the same time, an increase of the beam spot radius is able to partly compensate for its negative effect (which is already known from classical communications [39]), restoring the security and Gaussian entanglement, but limiting the values of the key bits and logarithmic negativity obtained from the covariance matrix.

Now let us assume that PS of sub-channels is applied by reducing the region of transmittance values for which the data contributing to the resulting state and to the key are

taken. We define each sub-channel η_i as the set of events, in which the transmittance was relatively stable and lies within the region of width $\Delta\eta$ centered around η_i . By the stability of transmittance, we mean that the transmittance fluctuations within the region $\Delta\eta$ are negligible (fractions of maximum variance, shown in figure 2). Thus, the set of sub-channels corresponds to the uniform binning of the continuous transmittance distribution with a bin size of $\Delta\eta$. In the simplest case of normally distributed transmittance values, the binning effect on the second moments would be described by Sheppard's correction [40], while for the Weibull distribution, cut at η_0 (13), the correction caused by a uniform binning changes unevenly due to the cut (i.e. the binning must be optimized). In any case, if the number of bins is larger than 1, the second moment of the discretized distribution is always larger than that of an actual continuous distribution, thus being a pessimistic assumption and complying well with the security considerations. The detailed study of the effect of fading discretization on security at practically achievable estimation precision will be the subject of future research, while in the following we take 10^3 bins for the theoretical analysis and 10^2 bins for the experimental data as a good although pessimistic approximation of the channel properties.

The security assumptions imply that the trusted parties know the effect of the channel on the signal states and are able to reconstruct the corresponding two-mode covariance matrix. The proper sub-channel estimation requires a large number of estimation states to be sent through the channel during its stability. The estimation states must be indistinguishable from the signal states so that an eavesdropper could not affect the estimation and signal states separately. Then, some of the states (at least one) for each sub-channel occurrence are randomly chosen as signal ones to contribute to the raw key and the corresponding covariance matrix. Thus, the security is not shown for each sub-channel occurrence separately (as this would require an asymptotic number of signal states combined with multiple estimation pulses sent upon each such event). Instead, the security is shown for the state, being conditionally prepared from the set of data obtained upon the post-selected sub-channels. The schematic time flow of the Gaussian CV QKD protocol in a fading channel with PS is given in figure 4, illustrated by the set of estimation and randomly chosen signal pulses upon each sub-channel occurrence.

Let us first consider PS of a single sub-channel and estimate entanglement per state and the amount of secret key per state (not taking into account the overall success probability of PS). The maximum key and maximum entanglement per state will then be achieved for a fixed non-fluctuating channel with the highest transmission possible, given by (13). Thus the ratio between the beam spot and the aperture size must be maximized if the maximum secure information per measurement is required, regardless of success probability and, accordingly, transmission time.

The principle of PS of a maximally transmitting sub-channel is schematically depicted in figure 5(a). The data are accumulated in different sub-channel transmittance regions, in which the transmittance fluctuations are assumed to be negligible. Then only the data from the post-selected maximally transmitting sub-channel are chosen to contribute to the post-selected state and the respective two-mode covariance matrix.

However, if the overall success probability is taken into account, then the PS region must be extended (schematically shown in figure 5(b)) in order to provide the optimal trade-off between the probability for transmittance to fall within the post-selected region and the fading variance of the post-selected sub-channels, reducing the secure key rate.

Let us consider the effect of the single most transmitting sub-channel PS on the entanglement properties of Gaussian states and the security of the respective CV QKD protocol.

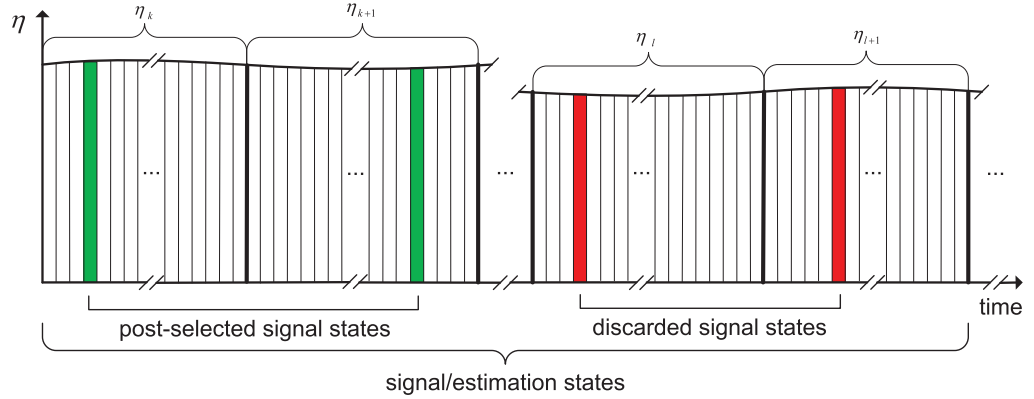


Figure 4. Time flow of the Gaussian CV QKD protocol in a fading channel with PS. The slowly variable transmittance η is divided into sub-channels of width $\Delta\eta$ centered around $\{\eta_i\}$, when the transmittance lies within the region $\eta \in [\eta_i \pm \Delta\eta/2]$ and is considered approximately stable. Multiple quantum states are sent through the channel during its stability time, thus corresponding to a given sub-channel, with the number of pulses being large enough for the proper estimation of sub-channel properties. Then, a few states (at least one per each occurrence of a given sub-channel) are randomly chosen to carry the signal (the events depicted as filled), thus being indistinguishable from the estimation states. Further, depending on the PS region, the results of the signal states measurements either are discarded (sub-channels η_l, η_{l+1} , events in red) or contribute to the resulting post-selected covariance matrix, used for security analysis, and to the raw key data (sub-channels η_k, η_{k+1} , events in green).

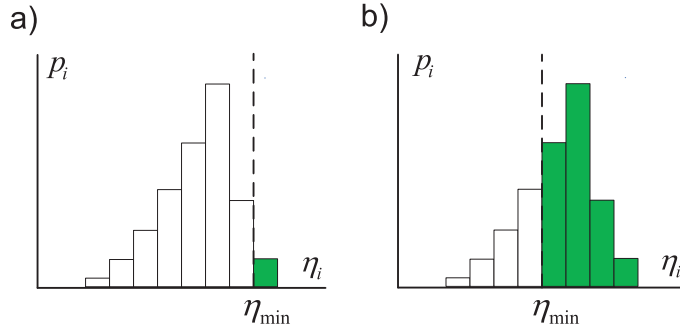


Figure 5. Scheme of PS of sub-channels. The data are accumulated upon different transmittance values, which lie within the sub-channel transmittance regions. Then only data from the post-selected maximally transmitting non-zero probability sub-channel (a, filled) or several sub-channels (b, filled) are selected to contribute to the post-selected state and the respective key whose security is derived from the covariance matrix of the post-selected state.

We access the available overall entanglement (beyond the Gaussian one) by estimating the conditional entropy of the state after PS, which corresponds to the lower bound on the distillable entanglement [41]:

$$E_D > S(\rho_A) - S(\rho), \quad (14)$$

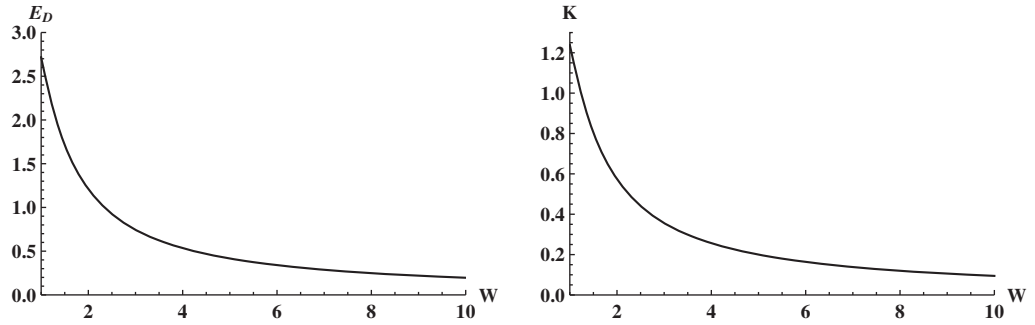


Figure 6. The maximum conditional entropy (left) and the maximum lower bound on the key rate (right, in bits per measurement) for the post-selected maximally transmitting sub-channel with respect to the spot size W (normalized by $a = 1$) upon the initially pure entangled state with variance $V = 10$.

where $S(\cdot)$ denotes the von Neumann entropy of the state, the density matrix ρ refers to the state after the fading channel and PS and ρ_A refers to the reduced state with respect to the sub-system A. The entropies are directly calculated from the symplectic eigenvalues of the respective covariance matrices. Thus, we can check whether entanglement of the state is restored by confirming a non-zero conditional entropy as well as quantify the amount of entanglement by the PS. The logarithmic negativity cannot be used for this purpose since it represents an upper bound on the entanglement.

The results of the calculations are given in figure 6 for the conditional entropy (left) and the key rate (right). It is evident that PS of the highest transmitting sub-channel increases the entanglement and security properties of the state as well as removes the dependence on the beam fluctuations variance, as the maximum available transmission (13) does not depend on the variance.

However, the key rate essentially depends on the overall success probability of the PS. Thus, we weight the post-selected key rate by the overall probability for transmittance to fall within the PS range. Such a weighted key now can be maximized by the optimal choice of the PS region, i.e. of the boundary η_{\min} between the selected and neglected sub-channels (see figure 5(b)), which (for a typical single-peaked fading distribution) explicitly describes the optimal PS region. The position of such a boundary depends on the effective modulation $\sigma = V - 1$ and untrusted excess noise, as well as on the parameters of the setup. We plot the typical dependence of the optimal PS region boundary with respect to the state modulation in figure 7 for the case of no untrusted excess noise present (left) and of additional untrusted noise $\chi = 0.01$ (right) upon different values of beam wandering variance σ_b for the beam spot being twice as high the aperture size: $W = 2$. The beginning of the PS region η_{\min} is compared with the cut of the transmittance distribution, given by (13). Thus, the offset between solid and dashed lines illustrates the width of the optimal PS region for different modulation depths and beam wandering variances.

Here we are interested in restoring security when it is lost due to fading, while quantitative estimations will be done in the next sections. It is evident from the graph that if no untrusted noise is present, the optimal PS region shrinks continuously with an increase of modulation, i.e. stronger PS must be optimally applied for highly modulated states. However, even if only a small fraction of untrusted noise is present, the protocol, based on Gaussian states over a fading

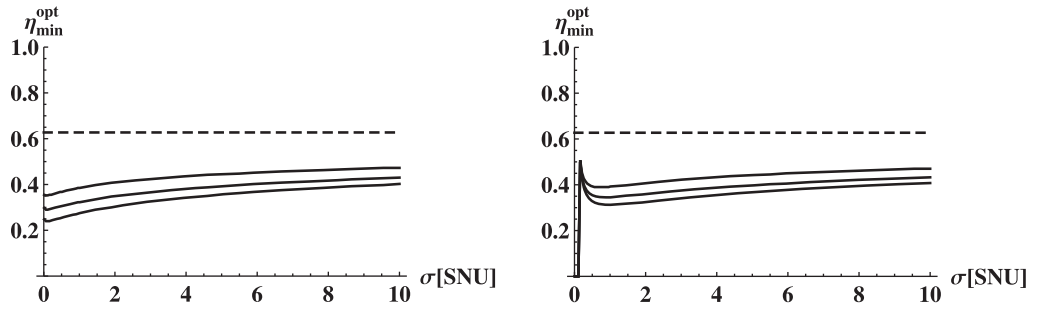


Figure 7. The beginning of the optimal PS region versus the effective state modulation $\sigma = V - 1$ upon no untrusted noise (left) and in the presence of untrusted noise $\chi = 0.01$ (right). The horizontal dashed line represents the cut of the transmittance distribution, given by (13). The beam wandering variance σ_b is 0.5, 1, 3 (from top to bottom), aperture size $a = 1$ and beam spot size $W = 2$.

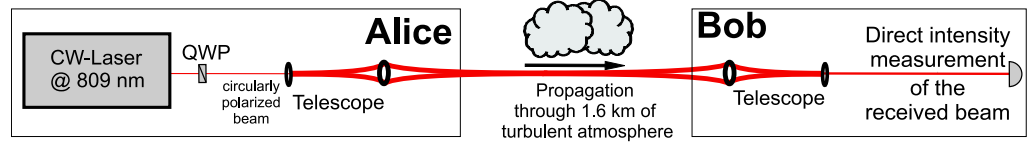


Figure 8. Experimental setup: a circularly polarized laser beam is sent through the 1.6 km free-space channel after having been expanded with the help of a telescope. At the receiver, the beam diameter is reduced again and its intensity is directly measured.

channel, first becomes insecure upon any PS (when σ is low), then strong PS must be applied, as weakly modulated states are more sensitive to the combination of fading and untrusted noise and then as the modulation increases, the PS can be first released and then made more strict upon further increase of effective modulation.

In the following section, we apply our analysis to the particular experimentally obtained distribution, which is well fitted by the beam wandering and fixed attenuation.

4. Real fading channel

We check the above-given considerations for a real short-distance atmospheric fading channel, where fading is mostly the result of beam wandering. We consider a particular experimental distribution obtained by a relative intensity measurement over a free-space link.

The experimental data were recorded within the framework of a setup on free-space quantum communication using continuous polarization variables, see figure 8 [42]. This experiment is a further development of earlier work performed in the laboratory [21] and on the roof of the MPL's building in Erlangen [20, 22]. We use a grating-stabilized diode laser, with a wavelength of 809 nm that lies within an atmospheric transmission window. The linearly polarized laser beam is transferred to a circularly polarized state and sent through the 1.6 km free-space channel from the institute's building to a tall university building, after having been expanded. Bob then reduces the beam diameter of approximately 120 mm by a telescope with an entrance aperture of 80 mm.

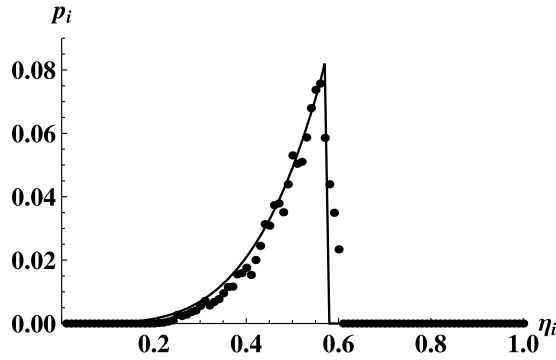


Figure 9. Distribution of transmittance η_i through the atmospheric fading channel (dots) as well as fitted log-negative Weibull distribution [31] (solid line). The intensity of the received beam was directly measured at a sampling rate of 150 kHz. The figure shows a histogram of the channel transmission for 10 s of experimental data with a bin size of $\Delta\eta = 0.01$. The intensity of the outgoing beam was 12 mW and the mean value of the received beam was 5.92 mW, with a standard deviation 0.92 mW.

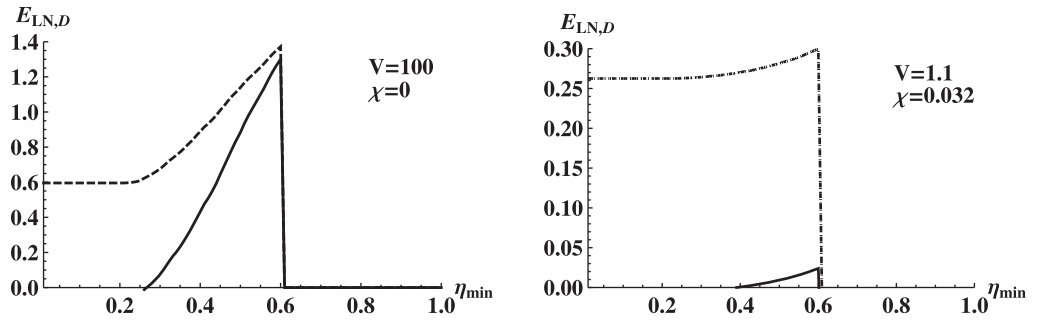


Figure 10. Effect of PS (represented by the beginning of PS region) after the fading channel given in figure 9 on the entanglement of the states in terms of logarithmic negativity (dashed line) and conditional entropy (solid line) for high state variance $V = 100$ (left) and low variance $V = 1.1$ (right) in the presence of noise $\chi = 3.2 \times 10^{-2}$.

For the scheme mentioned in [42], this beam will serve as a carrier beam for quantum information modulated onto its polarization degree of freedom. Here, on the other hand, in order to characterize the transmission properties of the fading atmospheric channel, we perform a direct detection of the carrier beam power. The data, normalized by the outgoing beam power at Alice, are shown in the histogram in figure 9, along with a fit according to the log-negative Weibull distribution [31]. The experimental data match very well the theoretical distribution given in the previous section with $\sigma_b = 0.6$, $W/a = 1.5$ and upon an additional fixed attenuation of 25% (given by fixed losses at optical components).

Let us first analyze the effect of PS on the entanglement properties of the states after passing through the experimental channel. Estimation of entanglement with respect to PS in terms of the beginning of the PS region (ending at $\eta_i = 1$) was performed numerically and is given in figure 10.

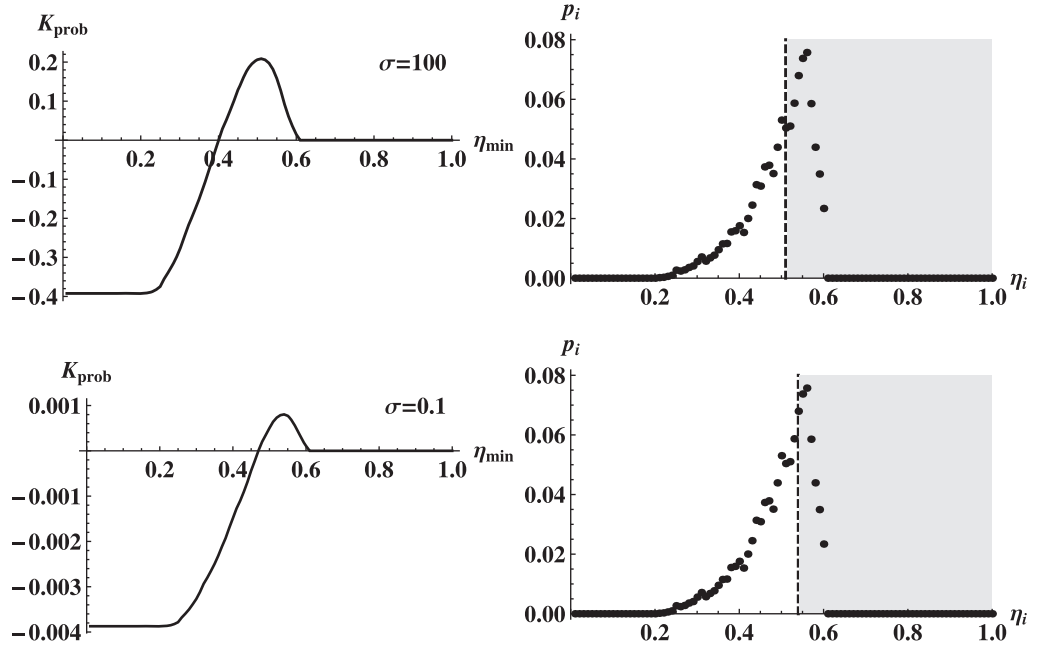


Figure 11. Left: effect of PS (represented by the start of the PS region) after the fading channel given in figure 9 on the security of the states against collective attacks in terms of the lower bound on the key rate (in bits per measurement), weighted by PS success probability, for high modulation variance $\sigma = 100$ (top) and low modulation variance $\sigma = 0.1$ in the presence of noise $\chi = 0.032$. Right: respective optimal PS region (bounded by the corresponding η_{min}), maximizing the weighted key rate for given parameters, indicated atop of the experimentally obtained fading distribution.

The channel shown in figure 9 appears to be entanglement preserving in terms of logarithmic negativity. However, the lower bound on distillable entanglement (given by the conditional entropy) is below 0 without PS (which is due to the fact that distillable entanglement is more sensitive to noise induced by fading for high state variance or to additional noise for low variance), but can be restored by PS, which thus guarantees the increase of entanglement in the resulting state, especially upon higher state variance.

Security against collective attacks is also sensitive to fading in the channel given in figure 9, but restorable with PS. The channel, being characterized by $\langle \sqrt{\eta} \rangle^2 \approx 0.492$ and $\text{Var}(\sqrt{\eta}) \approx 3 \times 10^{-3}$, appears to be Gaussian CV QKD security breaking either upon high modulation variance $\sigma = 100$ (which, for given $\langle \sqrt{\eta} \rangle^2$, can tolerate $\text{Var}(\sqrt{\eta})$ not larger than 1.2×10^{-3}) or in the presence of untrusted noise. However, PS is able to restore security and must be optimized with respect to the key rate, weighted by the PS success probability. This is evident from the graphs of the weighted key rate versus the PS region given in figure 11 for both high and low modulation variances along with the optimal PS regions for the given modulation. Here we have to take into account the overall success probability (i.e. the probability for channel transmission to appear in the post-selected region) and weight the key rate by this success rate, which requires optimization of the PS region to maximize the weighted key.

Here we assume that the estimation is reliable and not affected by the PS. Investigation of Eve's possible impact on estimation efficiency (which can seriously affect the security analysis

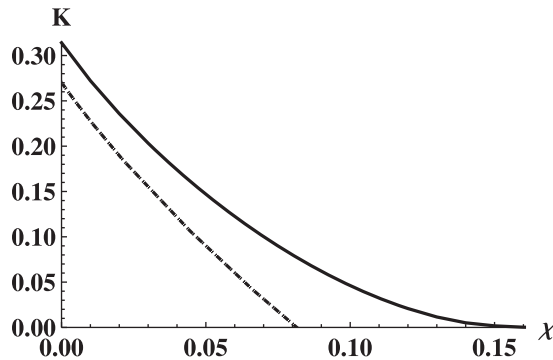


Figure 12. Secure key rate K (in bits per measurement) over the fading channel described by the experimentally obtained distribution (given in figure 9) for the given untrusted excess noise χ (in SNU) upon optimized PS and optimal modulation σ (solid line) and without PS, upon optimal modulation σ (dashed line).

already for non-fading channels) is beyond the scope of this paper and will be the subject of future work.

Evidently, there exists a trade-off between robustness of the protocol to fading (provided by reduced modulation) and robustness to noise (provided by increased modulation and requiring optimal PS). To generalize the result, we performed an optimization of both the state modulation σ and the PS region, for a given untrusted excess noise χ , modeled in the experimentally measured channel, and compared the resulting key rate to that with optimized modulation σ , but no PS. The corresponding plot is given in figure 12. The effect of PS is clearly visible from the graphs. In the presence of untrusted excess noise above the threshold (being approximately 0.08 SNU for the given distribution), no modulation can provide security over the given channel without PS. Contrary to this, if the optimized PS is performed and the modulation is also optimal, the scheme is able to tolerate almost double the amount of untrusted noise.

5. Effects of a limited ensemble size for the key rate and channel estimation

The security considerations above were performed in the standard assumption of the asymptotic limit, when the size of the data ensemble contributing to the key rate is assumed infinite. However, this is never the case in practice and the consideration of finite-size effects is essential for a CV QKD analysis with the first step in this direction already being performed in [43]. The issue becomes even more important when PS is applied as it reduces the ensemble size. Thus, in this section we briefly analyze the statistical properties of the lower bound on the key rate with respect to the ensemble reduction, caused by PS, by checking the convergence of the key rate with the theoretical prediction depending on the PS range.

We perform a statistical simulation introducing two Gaussian number generators, producing quadrature distributions of the two orthogonally squeezed vacuum states. We mix these distributions using a beam splitter with the input–output relation (3). We emulate coupling of the states on the 50:50 beam splitter by setting $\eta = 1/2$ to produce entangled states. The third Gaussian number generator produces the quadrature distributions of the vacuum mode, which emulates a purely lossy channel and is similarly coupled to one of the modes. The value of

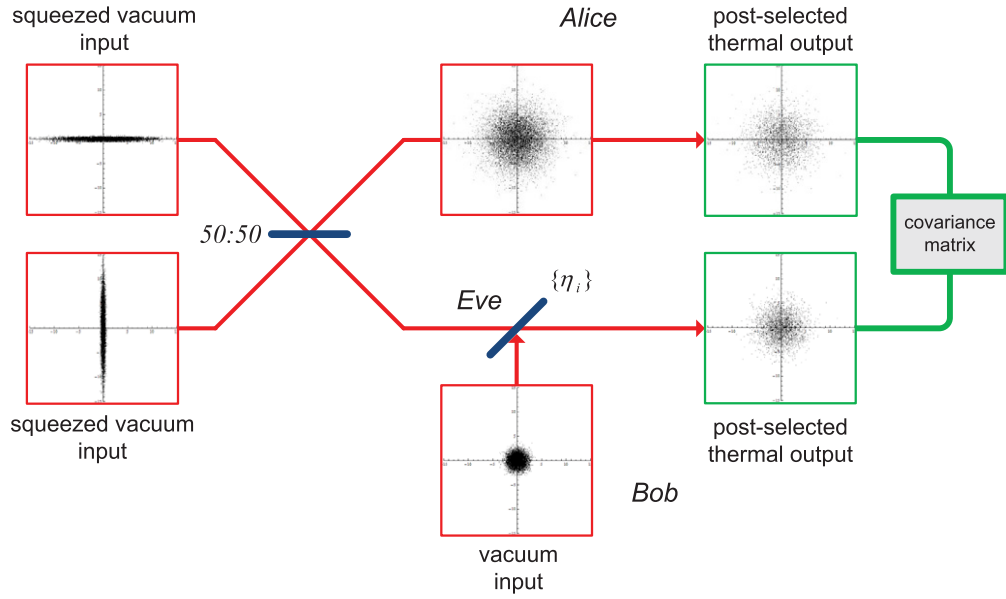


Figure 13. Scheme of numerical modeling for the analysis of the effects of the finite ensemble size on the reliability of PS. Two Gaussian number generators produce distributions of two orthogonally squeezed vacuum states, which are then mixed with the coupling ratio of 50 : 50. One of the modes is coupled to the Gaussian number generator, emulating vacuum input of the purely lossy fading channel, the coupling ratio being generated according to the experimentally obtained transmittance probability distribution in a fading channel. The resulting state is post-selected (as in figure 5(b)) in both modes according to the PS region. The two-mode covariance matrix is calculated and used for the security estimation. The depicted distributions were built for the source variance of $V = 10$ (corresponding to squeezing parameter $r \approx 1.49$) and the PS region starting with $\eta_{\min} = 0.55$.

transmittance is randomly picked for each next data point according to the distribution given in figure 9, i.e. the worst-case assumption of the ability to transmit only a single bit through the given estimated channel is made. After coupling, we obtain the ensemble of the quadrature values of the three modes after the channel transmission. Then we post-select the data according to a certain region and calculate the variance and covariances between the modes to construct the covariance matrix of elements $\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$ ($r = \{x, p\}$). The scheme of the numerical modeling procedure is given in figure 13.

The obtained covariance matrix is checked to comply with the uncertainty principle: $\gamma + i\Omega \geq 0$ (where Ω is the symplectic form) [32] and the physically valid covariance matrix is then used to estimate the key rate, using the above-described Gaussian machinery, in the assumption of purification performed by Eve (as Eve's mode is traced out in the final covariance matrix). The resulting key rate for the given ensemble size can then be compared to the key rate expected in the asymptotic limit. The results of the modeling are given in figure 14 for different initial ensemble sizes along with the theoretical prediction in the asymptotic regime.

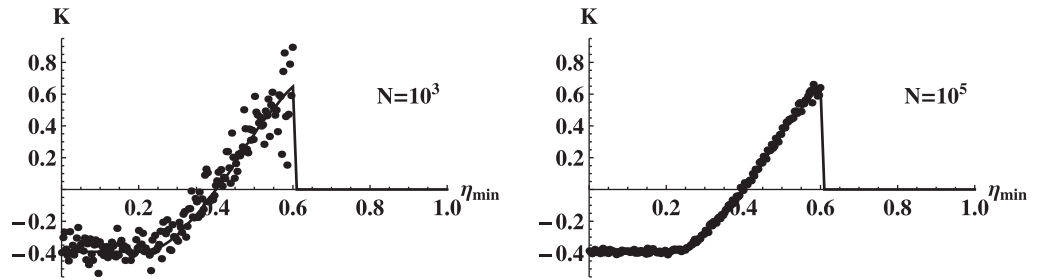


Figure 14. Effect of the finite ensemble size on the post-selected key rate upon high modulation variance $V = 100$ with respect to the beginning of the PS region for an initial ensemble size of 10^3 (left) and 10^5 (right) data points.

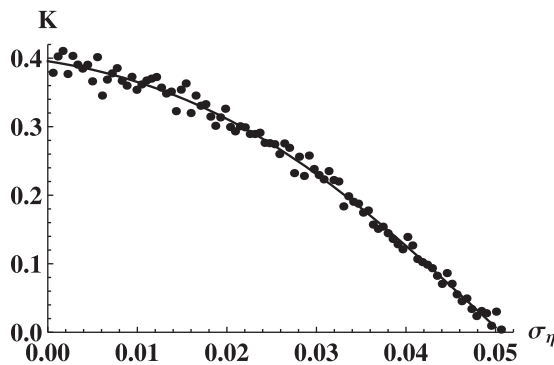


Figure 15. Effect of the imperfect estimation, modeled as the normal distribution of actual transmittance values with variance σ_η around the ‘estimated’ values, corresponding to the distribution in figure 9, on the optimally post-selected key rate at a high modulation $V = 100$ and an ensemble size of 10^5 points. The results of numerical modeling (dots) are given along with the fitting curve (solid line).

It is evident from the graph that while an ensemble size of 10^3 gives strongly fluctuating results and is sensitive to PS, which additionally increases the fluctuations, an ensemble size of 10^5 already gives good convergence with the theoretical prediction of the asymptotic limit with some divergence upon the most tight PS. Thus, our previous analysis performed in the asymptotic regime is valid upon finite ensemble size (assuming perfect estimation) and the positive effect of PS is confirmed in the finite-size regime (provided the estimation is still precise).

We also address the effect of imperfect estimation (which can also be the result of the finite number of signal pulses) on the efficiency of PS. In the context of our finite-size modeling, we now assume that the actual values of channel transmittance are normally distributed with variance σ_η around the transmittance, picked according to the experimentally obtained distribution (see figure 9). The effect of such a randomization on the optimally post-selected key rate for a high modulation variance $V = 100$ is shown in figure 15. The results show the stability of PS improvement against the imperfect estimation, which breaks the security of the protocol for a transmittance measurement variance of about 0.05. The number of data points for the numerical analysis is taken as 10^5 and still causes some visible fluctuations. States with weaker modulation appear to be more robust against imperfect estimation, which thus has a similar

effect as fading. Moreover, such a transmittance randomization due to imperfect estimation appeared to be more threatening to security than worst-case assumptions for transmittance to be constantly decreased by $3\sigma_\eta$ or $6\sigma_\eta$. This is due to the fact that fading in certain conditions more strongly affects security than the reduction of constant attenuation.

6. Summary and conclusions

We investigated the effect of fading channels on the entanglement properties of Gaussian states and the security of coherent states-based CV QKD and showed the sensitivity of entanglement, purity and security of the scheme to the interdependence of transmittance mean values $\langle\sqrt{\eta}\rangle$ and $\sqrt{\langle\eta\rangle}$. The effect of a fading channel is equivalent to state variance-dependent untrusted excess noise. Thus, weakly modulated states are less sensitive to the statistical properties of the transmittance distribution. However, the presence of further untrusted excess noise reduces the tolerance of weakly entangled states to fading. Moreover, for a short-distance fading channel, where fluctuations in transmittance are caused by beam wandering, the variance of the spot distribution is more destructive to entanglement and security, while an increase of the spot size with respect to the aperture can partly compensate for its negative effect.

PS of sub-channels (in the assumption of their proper estimation) was shown to be able to restore distillable entanglement and security for both high and low modulation upon noise, and should be the subject for optimization, as shown for the data from the real atmospheric channel. The combination of optimized modulation and optimal PS allows transmission with almost twice as high untrusted noise. The positive effect of PS on QKD security is also confirmed for a finite ensemble size when statistical convergence of the key rate is tested and the requirement of the effective transmittance estimation is addressed. The proposed sub-channel PS method can thus be used as a feasible alternative to the experimentally demanding entanglement distillation protocols if fading channel parameters are properly estimated.

Acknowledgments

VCU was supported by project no. P205/10/P321 of the Grant Agency of Czech Republic and acknowledges valuable discussions with Norbert Lütkenhaus. BH gratefully acknowledges the funding of the Erlangen Graduate School in Advanced Optical Technologies (SAOT) by the German Research Foundation (DFG) in the framework of the German Excellence Initiative. RF acknowledges support from the Alexander von Humboldt Foundation. In addition, the project was supported under FP7 FET Proactive by the integrated project Q-Essence and CHIST-ERA (Hipercom).

References

- [1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* p 175
- [4] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

- [5] Hiskett P A , Rosenberg D, Peterson C G, Hughes R J, Nam S, Lita A E, Miller A J and Nordholt J E 2006 *New J. Phys.* **8** 193
- [6] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
- [7] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 *Opt. Express* **16–23** 18790
- [8] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 513
- [9] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
- [10] Silberhorn Ch, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
- [11] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
- [12] Rigas J, Gühne O and Lütkenhaus N 2006 *Phys. Rev. A* **73** 012341
- [13] Lodewyck J *et al* 2007 *Phys. Rev. A* **76** 042305
- [14] Heid M and Lütkenhaus N 2007 *Phys. Rev. A* **76** 022313
- [15] Jacobs B C and Franson J D 1996 *Opt. Lett.* **21–22** 1854
- [16] Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev. Lett.* **81** 3283
- [17] Buttler W T, Hughes R J, Lamoreaux S K, Morgan G L, Nordholt J E and Peterson C G 2000 *Phys. Rev. Lett.* **84** 5652
- [18] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 *New J. Phys.* **4** 43
- [19] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 *New J. Phys.* **4** 82
- [20] Heim B, Elser D, Bartley T, Sabuncu M, Wittmann C, Sych D, Marquardt C and Leuchs G 2010 *Appl. Phys. B* **98** 635
- [21] Lorenz S, Korolkova N and Leuchs G 2004 *Appl. Phys. B* **79** 273
- [22] Elser D, Bartley T, Heim B, Wittmann C, Sych D and Leuchs G 2009 *New J. Phys.* **11** 045014
- [23] Buttler W T, Hughes R J, Kwiat P G, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev. A* **57** 2379
- [24] Semenov A A and Vogel W 2010 *Phys. Rev. A* **81** 023835
- [25] Heersink J, Marquardt C, Dong R, Filip R, Lorenz S, Leuchs G and Andersen U L 2006 *Phys. Rev. Lett.* **96** 253601
- [26] Wittmann C, Elser D, Andersen U L, Filip R, Marek P and Leuchs G 2008 *Phys. Rev. A* **78** 032315
- [27] Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2008 *Nature Phys.* **4** 919
- [28] Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2010 *Phys. Rev. A* **82** 012312
- [29] Ursin R *et al* 2007 *Nature Phys.* **3** 481
- [30] Zavatta A, Bellini M, Ramazza P L, Marin F and Arecchi F T 2002 *J. Opt. Soc. Am. B* **19** 1189
- [31] Vasylyev D Yu, Semenov A A and Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
- [32] Serafini A, Paris M G A, Illuminati F and De Siena S 2005 *J. Opt. B: Quantum. Semiclass. Opt.* **7** R19
- [33] Vidal G and Werner R F 2002 *Phys. Rev. A* **65** 032314
- [34] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 *Quantum Inf. Comput.* **3** 535
- [35] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
- [36] Wolf M M, Giedke G and Cirac J I 2006 *Phys. Rev. Lett.* **96** 080502
- [37] Navascues M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
- [38] García-Patron R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
- [39] Ma J, Jiang Y, Tan L, Yu S and Du W 2008 *Opt. Lett.* **33–22** 2611
- [40] Schneeweiss H and Komlos J 2009 *Stat. Methodol.* **6** 577
- [41] Eisert J and Wolf M M 2007 Gaussian quantum channels *Continuous-Variable Quantum Information Science* ed E Polzik, N Cerf and G Leuchs (London: Imperial College Press)
- [42] Heim B, Peuntinger C, Wittmann C, Marquardt C and Leuchs G 2011 Free-space quantum communication using continuous polarization variables *Applications of Lasers for Sensing and Free-Space Communications, OSA Technical Digest (CD)* Paper LWD3 (Toronto: Optical Society of America)
- [43] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343