# Unidimensional continuous-variable quantum key distribution using squeezed states

Vladyslav C. Usenko[*]

*Department of Optics, Palacký University, 17 Listopadu 50, 772 07 Olomouc, Czech Republic*
*and Bogolyubov Institute for Theoretical Physics of National Academy of Sciences, Metrolohichna St. 14-b, 03680 Kiev, Ukraine*

(Received 25 July 2018; published 20 September 2018)

The possibility of using squeezed states in the recently suggested unidimensional continuous-variable quantum key distribution based on a single quadrature modulation is addressed. It is shown that squeezing of the signal states expands the physicality bounds of the effective entangled state shared between the trusted parties due to the antisqueezing noise in the unmodulated quadrature. Modulation of the antisqueezed quadrature, on the other hand, effectively shrinks the physicality bounds due to the squeezing in the unmodulated quadrature and also provides noise on the reference side of the protocol, thus limiting the possibility of eavesdropping in noisy channels. This strategy is practical for low-loss (i.e., short-distance) channels, especially if direct reconciliation scheme is applied.

DOI: 10.1103/PhysRevA.98.032321

## I. INTRODUCTION

Quantum key distribution (QKD) [1] is the practical application of quantum information science, which is aimed at the development of methods (protocols) for the distribution of secure keys such that the security of a key is provided by the laws of quantum physics. The key can be used later in classical one-time pad cryptography, thus providing the complete postquantum solution for secure communication resilient against foreseen effective quantum computing. After starting with qubit-based discrete-variable protocols (see [2] for review) QKD was recently extended to continuous-variable (CV) [3] protocols (see [4] for review) which are aimed at providing higher key rates and simpler implementation compared to their discrete-variable counterparts. The first ideas in the field of CV QKD were based on discrete modulation and decoding of coherent and quadrature-squeezed [5] states of light as well as photon-number squeezed states [6–8], but had limited security proofs. It was an important step in the development of CV QKD when the use of Gaussian modulation [9] was suggested [10] for quadrature-squeezed states [11] and later shown to be applicable for coherent states as well [12]. It was shown that Gaussian protocols using squeezed [10,13–15] and coherent [12,16–23] states are secure against collective attacks and can tolerate, in principle, any level of channel attenuation if reverse information reconciliation is used [16]. In addition, a family of measurement-device-independent CV QKD protocols was developed and tested using coherent states of light [24]. Importantly, security of CV QKD against collective attacks implies security against general attacks in the asymptotic limit [25–27] of an infinite number of data as well as, under certain constraints, in the finite-size regime [28–31], when the number of data is finite.

Security analysis of Gaussian CV QKD protocols against collective attacks is based on the extremality of Gaussian states [32] and subsequent optimality of Gaussian collective attacks [33,34]. This enables security analysis based on the covariance matrix formalism, which is sufficient for characterization of Gaussian states, and imposes that trusted parties perform the channel estimation and are able to derive the covariance matrix of an entangled state effectively shared between them [35]. In order to know the channel properties the trusted parties perform modulation and measurement of both the complementary quadratures and then optimally switch between channel estimation and key distribution [36]. Therefore, both the amplitude and the phase modulators must be employed by a trusted sender party in order to apply Gaussian modulation of amplitude and phase quadratures. Recently a simplified unidimensional (UD) CV QKD protocol [37] was suggested and experimentally tested [38] on the basis of coherent states of light in order to provide simpler implementation potentially based on a single (e.g., phase) quadrature modulation with no need to perform modulation in a complementary quadrature. It was shown that if the remote trusted party is able to estimate the variance of the unmodulated quadrature, an eavesdropper can be limited by the physicality bounds on the effective entangled state shared between the trusted parties, and security of the protocol can be accessed by using a pessimistic assumption on the correlation between the sender and the receiver in the unmodulated quadrature.

It was previously shown that the use of squeezed states can make CV QKD more robust against imperfections, such as channel noise and limited postprocessing efficiency [13–15]; moreover, squeezing, if used optimally, can potentially eliminate information leakage from purely attenuating channels [39]. Moreover, the use of squeezed states in CV QKD becomes more and more feasible, in particular, with the development of compact on-chip squeezers [40,41]. Thus it is important to verify the effect of signal-state squeezing and identify its possible advantages in UD CV QKD.

In the current paper we generalize the result considering the use of quadrature-squeezed signal states in UD CV QKD. We show that the presence of antisqueezing noise makes the

[*] usenko@optics.upol.cz

protocol worse compared to its coherent-state counterpart if the squeezed quadrature is modulated. On the other hand, we show, surprisingly, a positive effect arising from the modulation of the noisy antisqueezed quadrature, which is concerned with the fact that the unmodulated quadrature remains squeezed and therefore allows better tolerance of channel noise and losses if direct information reconciliation is used. We therefore suggest the effective UD CV QKD protocol for short-distance channels, which benefits from the reduced fluctuations of the unmodulated quadrature and the trusted excess noise present in the modulated quadrature. Thus we fill the gap in the analysis of UD CV QKD by studying squeezed-state protocols as well as suggest the improvement of UD CV QKD by using modulation of the antisqueezed quadrature, which increases the key rate, secure distance of the protocol, and robustness to noise of the UD CV QKD with direct reconciliation, thereby contributing to solution of the major current challenges in QKD [42]. The paper is structured as follows: in Sec. II we consider the generalized squeezed-state UD CV QKD protocol; in Sec. III we study the security and physicality bounds in the general phase-insensitive channels; in Sec. IV we consider the typical case of phase-insensitive Gaussian channels, and we devise analytical expressions for lower bounds on the secure key rate in the limit of strong modulation and compare the performance of the protocols based on the modulation of coherent and squeezed states; and in Sec. V we give our Summary and Conclusions.

## II. SQUEEZED-STATE BASED UNIDIMENSIONAL CV QKD PROTOCOL

We consider the protocol based on the preparation of quadrature-squeezed states [11] (e.g., using an optical parametric oscillator) and their subsequent Gaussian modulation in one of the quadratures. The scheme is depicted in Fig. 1.

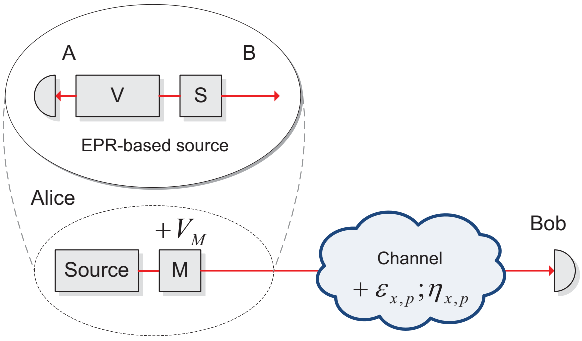

FIG. 1. Scheme of the squeezed-state UD CV QKD protocol. Alice prepares quadrature-squeezed states using, e.g., an optical parametric oscillator, and then modulates a state by displacing it along the modulated quadrature using the modulator M so that the modulation variance is $V_M$. The states travel through an untrusted, generally phase-sensitive channel (with transmittance values $\eta_x$ and $\eta_p$ and excess noise values $\epsilon_x$ and $\epsilon_p$ in the $x$- and $p$-quadratures, respectively) to a remote party, Bob, who performs homodyne measurement of the modulated quadrature. Inset: The equivalent entanglement-based scheme using a two-mode squeezed vacuum source; mode A is measured by Alice using a homodyne detector, and mode B is squeezed on the squeezer S and sent to a channel.

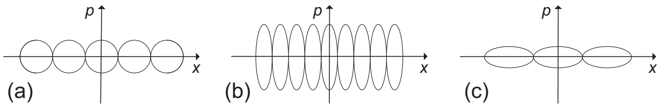

FIG. 2. Modulation schemes for unidimensional protocols: (a) using coherent states [37], (b) using $x$-quadrature squeezed states and modulation in the squeezed quadrature, and (c) using $p$-quadrature squeezed states and modulation in the antisqueezed quadrature.

In the following with no loss of generality we assume that the signal states are squeezed or antisqueezed in the $x$-quadrature. Therefore if the source generates pure $x$-quadrature-squeezed states characterized by the quadrature values $x_S$ and $p_S$, respectively, their variances are $\mathrm{Var}(x_S) = V_S < 1$ and $\mathrm{Var}(p_S) = 1/V_S > 1$. Alternatively, the source can generate $p$-quadrature-squeezed states so that $\mathrm{Var}(x_S) = V_S > 1$ and $\mathrm{Var}(p_S) = 1/V_S < 1$. The modulator then displaces $x$-quadrature, therefore performing modulation of the squeezed or antisqueezed quadrature, so that the modulated quadrature of the signal state sent to the channel in the case of $x$-quadrature modulation becomes $x_A = x_S + x_M$, where $x_M$ is the value of displacement, randomly picked from a zero-centered Gaussian distribution with variance $V_M$ and so $\mathrm{Var}(x_A) = V_S + V_M$ and $p_A \equiv p_S$ since no modulation was performed in the $p$-quadrature. Therefore two modulation schemes are possible in the case of squeezed states: modulation in the squeezed quadrature and modulation in the antisqueezed quadrature. The modulation schemes are depicted in Fig. 2 along with the single-quadrature modulation of coherent states [37,38] for comparison.

The states then travel through an untrusted, generally phase-sensitive channel, which is characterized by transmittance values $\eta_x$ and $\eta_p$ and excess noise values $\epsilon_x$ and $\epsilon_p$ in the $x$- and $p$-quadratures, respectively. After the channel, the states are measured by Bob using a homodyne detector set to measure the $x$- or $p$-quadrature. Bob has to switch between the quadratures often enough in order to characterize the variance in both quadratures and estimate the correlation in the modulated quadrature, but in the asymptotic limit the fraction of $p$-quadrature measurements can be assumed to be negligible [37]. After a sufficient number of runs of the protocol, Alice and Bob analyze the security of the protocol and perform error correction and privacy amplification in order to distill the key using either the direct or the reverse reconciliation scheme when Alice or Bob are, respectively, the reference sides for the error correction algorithms. In the following section we estimate the security region of the squeezed-state UD protocol depending on the modulation scheme and reconciliation direction and compare it to the coherent-state-based UD CV QKD protocol.

## III. SECURITY OF THE SQUEEZED-STATE UD PROTOCOL

Let us analyze the security of the protocol against the optimal Gaussian collective attacks, which, as mentioned above, implies security against general attacks in the asymptotic limit. To do so we follow the purification-based security analysis, where Eve is assumed to be able to purify (i.e., control) all the noise added in the untrusted quantum channel. Following the extension of the classical Csiszár-Körner theorem [43] to the quantum measurements, performed by Devetak and Winter [44], the secure key can be distilled once the trusted parties Alice and Bob have the information advantage over the adversary Eve. Therefore, the protocol is secure once the lower bound on the key rate

$$K_{\mathrm{DR}} = \beta_{\mathrm{DR}} I_{AB} - \chi_{AE}, \quad K_{\mathrm{RR}} = \beta_{\mathrm{RR}} I_{AB} - \chi_{BE} \tag{1}$$

is positive for either direct (DR) or reverse (RR) reconciliation, i.e. when the mutual classical information between the trusted parties $I_{AB}$ exceeds the Holevo quantity [45] $\chi_{AE/BE}$. The latter upper bounds the information available to an eavesdropper on the key bits possessed by a reference-side trusted party in the case of DR or RR, respectively. The mutual information between the trusted parties is scaled by the postprocessing efficiency $\beta_{\mathrm{DR/RR}} \in (0, 1)$, which depends on the effectiveness of the error correction algorithms for a given signal-to-noise ratio and is specific for a particular implementation of the protocol and direction of postprocessing. In the current paper we aim to compare the ultimate performance of the protocols, therefore we set $\beta = 1$; effects arising from the realistic finite-size regime shall not change the interplay between the protocols.

After the signal travels through the untrusted quantum channel, the trusted parties perform the estimation of the channel parameters, publicly revealing optimized fraction of the data [36]. A Gaussian phase-sensitive channel acts as a linear map that transforms quadratures so that the output reads $\{x', p'\} = \sqrt{\eta_{\{x,p\}}}\{x, p\} + \{x, p\}_N + \sqrt{(1-\eta_{\{x,p\}})}\{x, p\}_0$, where $\eta_{\{x,p\}}$ are the channel transmittance values, and $\{x, p\}_N$ and $\{x, p\}_0$ are the excess and vacuum noise contributions, respectively, with $\mathrm{Var}(\{x, p\}_N) = \epsilon_{\{x,p\}}$ and $\mathrm{Var}(\{x, p\}_0) = 1$ for the $x$- and $p$-quadratures.

The classical mutual information $I_{AB}$ can be explicitly obtained from the variances and the correlations between the modulation data on the side of trusted sender (Alice) and measurement data on the side of trusted receiver (Bob) after the channel as $I_{AB} = \frac{1}{2}\log_2 V_A/(V_{A|B}$, where $V_A = V_M$ is the variance of Alice's data, $V_{A|B} = V_A - C_{AB}^2/V_B$ is the conditional variance of Alice's data, $C_{AB} = \sqrt{\eta_x}V_M$ is the correlation between Alice's and Bob's data after the channel, and $V_B = \eta_x(V_S + V_M + \epsilon_x) + 1 - \eta_x$ is the variance of Bob's measured data after the channel. The mutual information then reads

$$I_{AB} = \frac{1}{2}\log_2\left[1 + \frac{\eta_x V_M}{1 + \eta_x(V_S + \epsilon_x - 1)}\right] \tag{2}$$

and is the same for DR and RR protocols.

The calculation of the Holevo bound in either of the reconciliation scenarios is, however, more involved. In the case of Gaussian modulation, the Holevo bound is the difference $\chi_{AE} = S(E) - S(E|A)$ or $\chi_{BE} = S(E) - S(E|B)$ between the von Neumann entropy $S(E)$ of the state available to Eve for collective measurement and the von Neumann entropy of Eve's state conditioned by data on Alice's $S(E|A)$ or Bob's $S(E|B)$, respectively, for DR and RR. In the general case of channel noise being present it is assumed that Eve holds purification of the channel noise [33,34] and then the equalities $S(E) = S(AB)$, $S(E|A) = S(B|A)$, and $S(E|B) = S(A|B)$ hold, where $S(AB)$ is the entropy of an initially pure state shared between the trusted parties through the noisy channel and $S(B|A)$, $S(A|B)$ are entropies of this state conditioned on the measurement results on Alice's or Bob's side in the DR and RR scenarios, respectively. Therefore, in order to assess the security of Gaussian CV QKD protocols in the case of collective attacks in noisy quantum channels, one needs to build an equivalent purification scheme, corresponding to the state preparation on Alice's side and state measurement on Bob's side. To do so for the UD squeezed-state CV QKD protocol, we start from the covariance matrix of a pure two-mode squeezed vacuum state with variance $V$, which purifies the Gaussian symmetrical modulation scheme [35]. In order to comply with the UD modulation of squeezed or antisqueezed states, we apply a squeezing operation on one of the modes with the squeezing parameter set to $-\log VV_S$. The resulting state is then described by the covariance matrix

$$\gamma_{AB} = \begin{bmatrix} V & 0 & \sqrt{VV_S(V^2-1)} & 0 \\ 0 & V & 0 & -\sqrt{\frac{V^2-1}{VV_S}} \\ \sqrt{VV_S(V^2-1)} & 0 & V^2V_S & 0 \\ 0 & -\sqrt{\frac{V^2-1}{VV_S}} & 0 & \frac{1}{V_S} \end{bmatrix}. \tag{3}$$

It is easy to see that when Alice performs homodyne detection in the $x$-quadrature on mode $A$, she conditionally prepares the signal squeezed or antisqueezed state in mode B described by the diagonal covariance $\gamma_{B|x_A} = \gamma_B - \sigma_{AB}[x\gamma_B x]^{\mathrm{MP}}\sigma_{AB} = \mathrm{diag}(V_S, 1/V_S)$, where $\gamma_A$ and $\gamma_B$ are diagonal single-mode submatrices of (3) standing for modes A and B, respectively, $\sigma_{AB}$ is the off-diagonal correlation submatrix of (3), the diagonal matrix $x = \mathrm{diag}(1, 0)$ stands for homodyne detection in the $x$-quadrature, and MP stands for the Moore-Penrose inverse of a matrix, applicable to singular matrices. On the other hand, the state of mode B, which is characterized by the diagonal single-mode covariance matrix $\gamma_B = \mathrm{diag}(V^2V_S, 1/V_S)$, corresponds to the modulated signal squeezed or antisqueezed state in the prepare-and-measure scheme once $V = \sqrt{1 + V_M/V_S}$, then $\gamma_B = \mathrm{diag}(V_S + V_M, 1/V_S)$, which is exactly the same as the state of the signal mode, sent to the channel in the prepare-and-measure scheme. Therefore, the entanglement-based scheme, depicted in the inset in Fig. 1, is equivalent to the prepare-and-measure scheme based on squeezed or antisqueezed states with squeezed or antisqueezed variance $V_S$ modulated with modulation variance $V_M = V_S(V^2 - 1)$.

Since the $p$-quadrature is not modulated, the correlation term in the unmodulated quadrature remains unknown to the trusted parties, similarly to the the coherent-state UD CV QKD [37]. Therefore, after the quantum channel, the covariance matrix of the initially pure state, (3), shared between Alice and Bob, in terms of the modulation variance $V_M$ reads

$$\gamma'_{AB} = \begin{bmatrix} \sqrt{1+\frac{V_M}{V_S}} & 0 & \sqrt{\eta_x V_M}(1+\frac{V_M}{V_S})^{\frac{1}{4}} & 0 \\ 0 & \sqrt{1+\frac{V_M}{V_S}} & 0 & C_p \\ \sqrt{\eta_x V_M}(1+\frac{V_M}{V_S})^{\frac{1}{4}} & 0 & V_x^B & 0 \\ 0 & C_p & 0 & V_p^B \end{bmatrix}, \tag{4}$$

where $C_P$ is the unknown correlation in the $p$-quadrature and $V_x^B = \eta_x(V_S + V_M + \epsilon_x) + 1 - \eta_x$.

The covariance matrices of the conditioned states after the signal propagation through the channel and after Alice's or Bob's measurements in the $x$-quadrature read, respectively,

$$\gamma'_{B|x_A} = \begin{bmatrix} \eta_x(V_S+\epsilon_x-1)+1 & 0 \\ 0 & V_p^B \end{bmatrix} \tag{5}$$

and

$$\gamma'_{A|x_B} = \begin{bmatrix} \frac{\sqrt{1+\frac{V_M}{V_S}}[\eta_x(V_S+\epsilon_x-1)+1]}{V_x^B} & 0 \\ 0 & \sqrt{1+\frac{V_M}{V_S}} \end{bmatrix}. \tag{6}$$

Now the Holevo bound can be assessed in either the DR or the RR scenario by calculating the von Neumann entropies of state (5) or (6), respectively, and subtracting them from the von Neumann entropy of the two-mode state, (4), which is done using the bosonic entropic function [46] of the symplectic eigenvalues of the respective covariance matrices [9] (see [47] for details on Gaussian security analysis). The von Neumann entropy $S(AB)$ of the two-mode state, (4), then depends on the unknown correlation parameter $C_P$ in the unmodulated quadrature, which can, in principle, be set arbitrary by an eavesdropping attack in the untrusted channel. Nevertheless, the parameter can be bounded by the physicality considerations. Indeed, Eve's attack on the protocol should preserve the physicality of the state, effectively measured by Alice and Bob. In terms of the covariance matrix this is given by the constraint, following from the uncertainty principle,

$$\gamma'_{AB} + i\Omega \geqslant 0, \tag{7}$$

where $\Omega$ is the symplectic form

$$\Omega = \bigoplus_{i=1}^{n} \omega, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{8}$$

which imposes limitations on the possible values of $C_p$. The physicality constraint in the general case can be represented by the parabolic equation on the $\{V_p^B, C_p\}$ plane,

$$(C_p - C_0)^2 \leqslant \frac{V_M}{\sqrt{V_S(V_S+V_M)}}\big(1 - \eta_x V_S V_0^B\big)\big(V_p^B - V_0^B\big), \tag{9}$$

with vertex $(V_0^B, C_0)$, defined as

$$V_0^B = \frac{1}{1+\eta_x(V_S+\epsilon_x-1)} \tag{10}$$

and

$$C_0 = -\frac{V_0^B\sqrt{\eta_x V_M}}{\left(\frac{V_M}{V_S}+1\right)^{\frac{1}{4}}}. \tag{11}$$

The typical physicality regions are given in Fig. 3. In addition, squeezing or antisqueezing of the signal and, respectively, antisqueezing or squeezing of the unmodulated quadrature also influence the security bounds of the protocol, given by the condition $K_{\rm DR} = 0$ or $K_{\rm RR} = 0$ for DR or RR, respectively. In the general case the security can be evaluated numerically and the typical bounds are given in Fig. 3 along the physicality bounds.

It is evident from the physicality bounds plotted in Fig. 3 that the use of squeezed or antisqueezed states as the signal carriers shifts the physicality region. Indeed, if the squeezed states are used, the region is shifted towards higher values of noise $V_p^B$ and expanded, because the antisqueezing noise present in the $p$-quadrature should result in above-shot-noise fluctuations in the

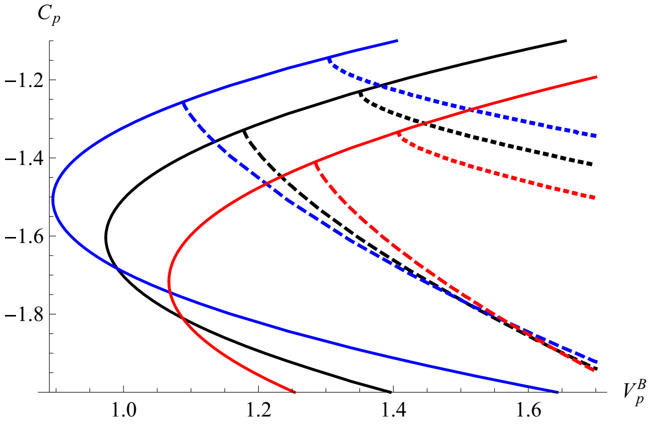

FIG. 3. Physicality (solid lines) and security within the physicality (dotted lines, DR; dashed lines, RR) regions of the UD protocol. Modulation variance $V_M = 10$, channel transmittance in $x$ $\eta_x = 0.9$, noise in $x$ $\epsilon_x = 3\%$ SNR. Plots are given for coherent-state ($V_S = 1$; middle, black lines), squeezed-state ($V_S = 0.9$;lower, red lines), and anti-squeezed-state ($V_S = 1.1$; upper, blue lines) protocols.

$p$-quadrature and allows for a wider region of correlation term $C_p$ values than those for the coherent-state protocol. On the other hand, modulation in the antisqueezed quadrature shifts the physicality region to $V_p^B$ below shot noise, since the $p$-quadrature in this case is squeezed, and allows for a narrower region of correlation term values for given noise $V_p^B$. In the next section we consider the role of signal-state squeezing and antisqueezing in UD CV QKD protocols in the typical class of phase-insensitive Gaussian channels.

## IV. ROLE OF SIGNAL SQUEEZING OR ANTISQUEEZING IN SYMMETRICAL CHANNELS

In the previous section we have derived the general physicality and security bounds considering generally phase-sensitive channel, having different transmittance and excess noise in the $x$- and $p$-quadratures. However, in practice the quantum channels (fiber or free space) are typically inclined to the same transmittance and the same excess noise in both quadratures, thus being phase insensitive (symmetric). In the current section we focus on the role of signal-state squeezing and antisqueezing in UD CV QKD protocols over such channels.

First, we assume that the channel transmittance is symmetrical, $\eta_x = \eta_p \equiv \eta$; then the structure of noise measured in the $p$-quadrature on Bob's side is $V_p^B = \eta(1/V_S + \epsilon_p)$. In Fig. 4 we plot physicality and security bounds in this case similarly to the ones given in Fig. 3. This allows us to compare the robustness of the UD protocols to channel noise. It is evident from the plot that in the case of the squeezed-state protocol (lower, red lines) the security upon arbitrary $C_p$ is lost at lower excess noise for DR (dotted lines) than for RR (dashed lines) and, in both cases, at lower noise than for the coherent and antisqueezed protocols. On the other hand, the coherent-state protocol (middle, black lines) demonstrates almost the same tolerance to channel noise for RR and DR under a given transmittance and with the given modulation. Finally, the antisqueezed protocol (upper, blue lines) demonstrates a similar tolerance to channel noise as the coherent-state protocol for RR but is more robust against channel noise in the case of DR. Indeed, the antisqueezed protocol allows for weaker noise-infusing attacks due to squeezing of the $p$-quadrature; on the other hand, it is known that the DR protocol is more robust against trusted preparation noise [47–49]. On the contrary, the squeezed-state UD protocol loses this advantage, allowing for broader attacks within the noisy antisqueezed $p$-quadrature, which is not compensated by having less noise in the modulated (squeezed) $x$-quadrature.

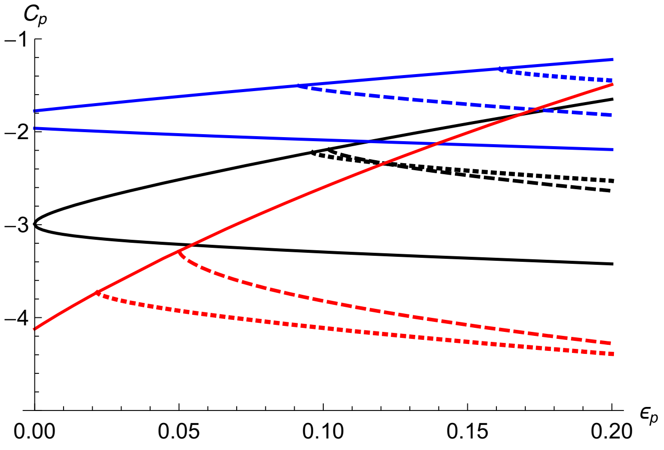

FIG. 4. Physicality (solid lines) and security within the physicality (dotted lines, DR; dashed lines, RR) regions of the UD protocol in channels with symmetric transmittance $\eta_x = \eta_p = 0.9$ with respect to excess noise $\epsilon_p$. Modulation variance $V_M = 10$, noise in $x$ $\epsilon_x = 3\%$ SNR. Plots are given for coherent-state ($V_S = 1$; middle, black lines), squeezed-state ($V_S = 0.9$; lower, red lines), and anti-squeezed-state ($V_S = 1.1$; upper, blue lines) protocols.

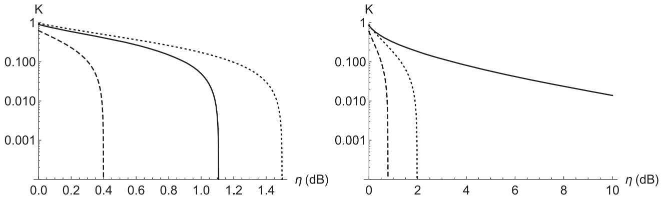

FIG. 5. Secure key rate versus channel attenuation (on dB scale), secure against collective attacks for the DR (left) and RR (right) protocols, for the coherent-state (solid lines), squeezed-state ($V_S = 0.5$; dashed lines), and anti-squeezed-state ($V_S = 2$; dotted lines) protocols. Channel noise $\epsilon = 3\%$ SNU, modulation variance $V_M = 100$.

The above result is confirmed in fully phase-insensitive (symmetrical) channels with the same transmittance as well as the same noise $\epsilon_x = \epsilon_p \equiv \epsilon$ in both quadratures. We first plot the lower bound on the key rate, (1), for the DR and RR squeezed-, coherent-, and anti-squeezed-state protocols upon fixed channel excess noise in Fig. 5.

It can be clearly seen that upon RR the coherent-state protocol provides much better robustness against channel attenuation at given noise levels than the squeezed- or anti-squeezed protocol (therefore allowing for a much longer secure distance in the same fiber or free-space channels). The weak performance of anti-squeezed-state-based CV QKD can be explained by the sensitivity of RR protocols to the noise in the state preparation [47,50,51]. On the contrary, in the case of DR the antisqueezed protocol can tolerate more channel loss than the squeezed-state one (demonstrating very poor results) and even outperforms the coherent-state protocol. In a telecom fiber with attenuation of −0.2 dB/km the higher robustness of the antisqueezed DR UD CV QKD at the considered levels of noise would result in an almost-double increase in the maximum secure distance (from 4.5 to 7.5 km) compared to the coherent-state protocol. Note that the positive effect of antisqueezing noise of signal states is observed in the noisy channels and can be seen as the manifestation of the effect known as "fighting noise with noise," when noise on the reference side of the protocol makes it more robust against channel noise [13,47]. In this regime, quantum squeezing of signal states in terms of the sub-shot-noise fluctuations may, in principle, not be needed and signal states with above-shot-noise fluctuations in the modulated ($x$-) quadrature and shot-noise and even above-shot-noise fluctuations in the unmodulated ($p$-) quadrature can be sufficient for improving the robustness of the DR UD CV QKD once impure signal states are considered.

For symmetrical channels and in the limit of infinitely strong modulation of pure squeezed states, the lower bound on the key rate in the DR scenario can be simplified as

$$K_{\mathrm{DR}}|_{V_M\to\infty} = (\log_2 e)\left[C\,\mathrm{ArcTanh}\frac{1}{C} - 1\right] + \log_2\frac{\eta|1-V_S|}{1+\eta|1-V_S|}, \tag{12}$$

where $C \equiv \sqrt{[1+\eta(1/V_S-1)][1+\eta(V_S-1)]}$. For the coherent-state protocol $V_S = 1$ the expression further simplifies as

$$K_{\mathrm{DR}}^{(\mathrm{coh})}\Big|_{V_M\to\infty} = \log_2 2\eta - \frac{1}{2}\log_2[\eta(1-\eta)] - \log_2 e, \tag{13}$$

which is lower by $\log_2[e] - 1 \approx 0.44$ than the asymptotic expression for the lower bound on the key rate for the standard coherent-state protocol upon DR, being $\frac{1}{2}\log_2\frac{\eta}{1-\eta}$ [47].

On the other hand, in the case of the RR scenario, in the limit of infinitely strong modulation the key rate in the symmetrical channel reads

$$K_{\mathrm{RR}}|_{V_M\to\infty} = \frac{D}{2}\left[\log_2\frac{D+1}{2} - \log_2\frac{D-1}{2}\right] - \log_2[1+\eta|1-V_S|] - \log_2 e, \tag{14}$$

where $D \equiv \sqrt{\frac{1+\eta(V_S-1)}{\eta V_S}}$. This can be further simplified for the coherent-state protocol, i.e., for $V_S = 1$, as

$$K_{\mathrm{RR}}^{(\mathrm{coh})}\Big|_{V_M\to\infty} = \frac{1}{\ln 2}\left[\frac{\mathrm{ArcTanh}(\sqrt{\eta})}{\sqrt{\eta}} - 1\right], \tag{15}$$

which, in the limit of low transmittance $\eta \to 0$, can be well approximated by $\frac{\eta\log_2 e}{3}$, being lower by a factor of 2/3 than the similar limit for the standard coherent-state CV QKD protocol [37].

We observe similar behavior (disadvantage of squeezing or antisqueezing in the RR scenario and advantage of antisqueezing in the DR scenario even compared to the coherent-state protocol) if we consider the robustness to excess channel noise at a given transmittance in the case of symmetrical channels, as plotted in Fig. 6.

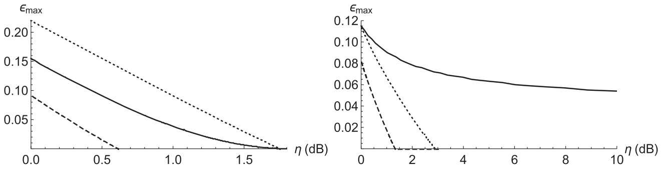

FIG. 6. Maximal tolerable channel noise $\epsilon$ versus channel attenuation (on dB scale) for the protocols, secure against collective attacks for DR (left) and RR (right), based on coherent states (solid lines), squeezed states ($V_S = 0.5$; dashed lines), and antisqueezed states ($V_S = 2$; dotted lines). Modulation variance $V_M = 100$.

Indeed, while the coherent-state protocol is more robust against channel noise in the case of RR, the antisqueezed protocol can tolerate larger amounts of channel excess noise once DR is used. It is evident from the plot that the antisqueezed protocol can tolerate about 50% more channel noise than the coherent-state UD CV QKD. Therefore, surprisingly, modulation of a noisy antisqueezed quadrature (having more noise than the standard shot-noise level of a coherent state) can be advantageous for the UD CV QKD in the short-range quantum channels, increasing the key rate, the secure distance, and the tolerable channel noise of the protocol.

## V. SUMMARY AND CONCLUSIONS

We have considered the possibility of using squeezed or antisqueezed signal states in the unidimensional continuous-variable quantum key distribution protocol based on the Gaussian modulation of a single quadrature. The results show that squeezing or antisqueezing of the signal affects the physicality and security bounds of the protocol in the general case of phase-insensitive channels. In the typical case of phase-insensitive (symmetrical) channels the coherent-state protocol outperforms its squeezed- and anti-squeezed-state counterparts once reverse reconciliation is used. On the other hand, the anti-squeezed-state protocol, based on the modulation of a quadrature, having more noise than a standard shot-noise level of a coherent state, demonstrates higher key rates and better robustness to losses and channel excess noise than coherent- and squeezed-state protocols. The result will be useful for the development of secure quantum communication systems upon short distances using a simplified single-quadrature modulation scheme and compact sources of squeezed light.

## ACKNOWLEDGMENTS

The author acknowledges support from Project LTC17086 of the INTER-EXCELLENCE program of the Czech Ministry of Education and COST Action CA15220, ‘QTSpace.’

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] S. L. Braunstein and P. Van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[4] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).
[5] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
[6] A. C. Funk and M. G. Raymer, Phys. Rev. A **65**, 042307 (2002).
[7] V. C. Usenko and M. G. A. Paris, Phys. Rev. A **75**, 043812 (2007).
[8] V. C. Usenko and M. G. A. Paris, Phys. Lett. A **374**, 1342 (2010).
[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[10] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[11] A. Lvovsky, *Photonics, Volume 1: Scientific Foundations, Technology and Applications* (Wiley, New York, 2014).

[12] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[13] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[14] V. C. Usenko and R. Filip, New J. Phys. **13**, 113007 (2011).

[15] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).

[16] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[17] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[18] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[19] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, Phys. Rev. A **76**, 042305 (2007).

[20] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).

[21] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photon. **7**, 378 (2013).

[22] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Opt. Express **23**, 17511 (2015).

[23] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).

[24] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).

[25] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[26] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[27] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).

[28] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).

[29] F. Furrer, Phys. Rev. A **90**, 042325 (2014).

[30] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).

[31] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[32] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).

[33] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[34] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[35] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Info. Comput. **3**, 535 (2003).

[36] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).

[37] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).

[38] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Quantum Inf. Comput. **16**, 1081 (2016).

[39] C. S. Jacobsen, L. S. Madsen, V. C. Usenko, R. Filip, and U. L. Andersen, npj Quantum Info. **4**, 32 (2018).

[40] A. Dutt, K. Luke, S. Manipatruni, A. L. Gaeta, P. Nussenzveig, and M. Lipson, Phys. Rev. Appl. **3**, 044005 (2015).

[41] G. Masada and A. Furusawa, Nanophotonics **5**, 469 (2016).

[42] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Info. **2**, 16025 (2016).

[43] I. Csiszár and J. Körner, IEEE Trans. Info. Theory **24**, 339 (1978).

[44] I. Devetak and A. Winter, Proc. Roy. Soc. A: Math. Phys. Eng. Sci. **461**, 207 (2005).

[45] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[46] A. Serafini, M. Paris, F. Illuminati, and S. De Siena, J. Opt. B: Quantum Semiclass. Opt. **7**, R19 (2005).

[47] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).

[48] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[49] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).

[50] R. Filip, Phys. Rev. A **77**, 022310 (2008).

[51] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).