entropy

MDPI

Article

Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense

Vladyslav C. Usenko * and Radim Filip

Received: 21 May 2015; Accepted: 30 December 2015; Published: 5 January 2016
Academic Editor: Stefano Pirandola

Department of Optics, Palacký University, 17. listopadu 1192/12, 77146 Olomouc, Czech Republic; filip@optics.upol.cz
* Correspondence: usenko@optics.upol.cz; Tel.: +420-585-634-248

Abstract: We address the role of the phase-insensitive trusted preparation and detection noise in the security of a continuous-variable quantum key distribution, considering the Gaussian protocols on the basis of coherent and squeezed states and studying them in the conditions of Gaussian lossy and noisy channels. The influence of such a noise on the security of Gaussian quantum cryptography can be crucial, even despite the fact that a noise is trusted, due to a strongly nonlinear behavior of the quantum entropies involved in the security analysis. We recapitulate the known effect of the preparation noise in both direct and reverse-reconciliation protocols, as well as the detection noise in the reverse-reconciliation scenario. As a new result, we show the negative role of the trusted detection noise in the direct-reconciliation scheme. We also describe the role of the trusted preparation or detection noise added at the reference side of the protocols in improving the robustness of the protocols to the channel noise, confirming the positive effect for the coherent-state reverse-reconciliation protocol. Finally, we address the combined effect of trusted noise added both in the source and the detector.

Keywords: quantum cryptography; quantum optics; quantum key distribution; continuous variables; quantum entanglement; coherent states; squeezed states

1. Introduction

Quantum key distribution (QKD; see [1,2] for reviews) is the branch of quantum information science, whose goal is to develop methods (protocols) that allow two trusted parties to share a random secret key so that its security is provided by the very laws of quantum physics. The key can be then used in the one-time pad cryptographic system [3], which was shown to be information-theoretically secure [4]. Therefore, QKD provides a quantum-cryptographic physics-based solution as an alternative to the classical asymmetrical cryptosystems, which are currently widely used, but are based on the mathematical complexity assumptions.

The first theoretical idea of QKD was the BB84 protocol (named after its authors Bennett and Brassard) [5] based on the use of the discrete-variable (DV) quantum systems, namely single photons, so that the key bits were encoded to (and obtained from) the measurements of the polarization degree of freedom in the two randomly-switched bases. BB84 and its modifications, such as B92 (named after its author Bennett) [6] or SARG (named after its authors Scarani, Acín, Ribordy and Gisin) [7], was used as the basis of DV QKD in the prepare-and-measure (P & M) implementations typically performed with weak coherent pulses or heralded singe photon sources using, besides polarization, e.g., phase or time encoding [6,8]. The presence of the additional photons in the weak coherent pulses was shown to be a potential vulnerability of DV QKD in the case of photon number splitting attacks, and the use of the decoy states was suggested to overcome such a threat [9]. On the other hand, the use of photonic entanglement was suggested in the entanglement-based (also called EPR-based

after the famous Einstein–Podolsky–Rosen paradox [10]) E91 protocol [11], where trusted parties are supposed to perform polarization measurements in the certain sets of bases on the two spatially distant non-classically correlated photons. By verifying a loophole-free violation of the Bell inequalities [12,13] from the measurements in one set of bases, the trusted parties can ensure the security of the key obtained from the measurements in another one. Although the E91 protocol can be seen as an alternative way of implementing BB84 [14], it also offers potential device independence based on the quantum nonlocality. While the security of the protocols was first considered against particular eavesdropping strategies, it was later extended on the general information-theoretical security proofs against collective [15] and coherent attacks [16] and then extended to composable security (being the systematic way of specifying the security requirements of cryptographic tasks) [17] for certain DV QKD protocols [18–20].

As an alternative to the DV coding, the use of the continuous variables (CVs; see [21] for a review) of multiphoton Gaussian states of light (see [22] for a review on Gaussian quantum information) was suggested in the CV QKD protocols. Typically the continuous quadrature observables are used to encode key bits, and subsequently, the homodyne detection of the quadrature (or heterodyne measurement of two complementary quadratures simultaneously) is applied contrary to the photon-counting measurement in DV QKD. Alternatively, polarization [23] or photon-number coding [24–28] can in principle be used. The preliminary version of CV QKD was firstly suggested [29] and studied against particular eavesdropping strategies [30] by Ralph based on the binary quadrature displacement of coherent state produced by a laser or two-mode quadrature-squeezed states, which can be produced by an optical parametric oscillator. In the latter case, both the entangled modes were supposed to be sent to the remote trusted party for a homodyne measurement. Later, a protocol based on the quadrature modulation of a single-mode squeezed states was suggested by Hillery [31] and studied against arbitrary attacks taking into account error correction by Gottesman and Preskill [32], while the encoding of a pre-determined key using entangled states and verification of nonclassical correlations similarly to E91 protocol to prove security against particular eavesdropping attacks was suggested by Reid [33]. The CV QKD protocol based on the two-mode entangled beams shared between the trusted parties who use amplitude or phase measurements to decode binary data was alternatively suggested by Silberhorn *et al.* [34]. The security of the protocols was shown against certain eavesdropping strategies mainly in purely attenuating channels and typically relied on the uncertainty principle, which does not allow a potential eavesdropper to measure both quadratures precisely and simultaneously. The CV states of light were also suggested by Cerf *et al.* [35] to distribute a continuous Gaussian key with security being shown against the whole class of individual attacks using the optimal entangling cloner attack. Importantly, it was then shown by Grosshans and Grangier [36] that Gaussian protocols secure against individual attacks can be implemented even with coherent states with no need in nonclassicality, such as squeezing. The Gaussian protocols were however limited by the 50% loss in the optical link, because it otherwise led to the information advantage of an eavesdropper with respect to the sender trusted party when the standard direct reconciliation (DR) of data was used, *i.e.*, when the remote trusted party was correcting its errors to exactly reproduce the dataset at the trusted sender side. The problem can be solved by using post-selection, as was shown by Silberhorn *et al.* [37]. Remarkably, the reverse reconciliation (RR) can be used and allows achieving theoretical security of coherent-state CV QKD upon any channel loss, as shown by Grosshans *et al.* [38]. The RR protocol was extended by Weedbrook *et al.* [39] to the heterodyne detection allowing coherent-state CV QKD with no bases switching. Recently, the simplified unidimensional CV QKD protocol based on a single-quadrature modulation was suggested by Usenko and Grosshans [40]. The Gaussian individual attacks were shown to be optimal for the Gaussian CV QKD protocols by Grosshans and Cerf [41]. It was then an important step in CV QKD when the security of the Gaussian protocols was generalized and proven against the Gaussian collective attacks by Navascués *et al.* [42] and by García-Patrón and Cerf [43]. Such attacks were shown optimal using the extremality of Gaussian states [44], studied by Pirandola *et al.* [45,46], and then extended to the general attacks using the de Finetti theorem by Renner and Cirac [47]. This established the clear framework for theoretical security analysis of the CV QKD protocols in asymptotic regime, but many

issues related to the real implementation of the protocols remained open. Differently from many other CV quantum information protocols, such as CV quantum teleportation [48] in the Gaussian regime [49–51] or Gaussian CV quantum cloning [52–54], the Gaussian CV QKD involves more complex aspects of the Gaussian quantum states and measurements due to the strong nonlinearity of the quantum entropies, involved in the analysis of the security of the protocols.

The information-theoretical research in CV QKD is currently focused on extending the security proofs against general attacks on the finite-size regime, which is always the case in real QKD systems. The first step in this direction was done by Leverrier *et al.* [55], who considered finite-size effects in coherent-state CV QKD secure against collective attacks mainly focusing on the channel estimation. The channel estimation was recently optimized for CV QKD with arbitrary signal states and Gaussian modulation by Ruppert *et al.* [56]. The optimality of Gaussian collective attacks against the Gaussian CV QKD was confirmed in the finite-size regime by Leverrier and Grangier [57]. The security of CV QKD against arbitrary attacks was shown using Gaussian post-selection (incorporated to the protocol) in the asymptotic limit by Walk *et al.* [58] using the equivalence between post-selection and noiseless linear amplification, also shown by Fiurašek and Cerf [59]. The composable security of the protocol based on the two-mode squeezed vacuum state against arbitrary attacks in the finite-size regime was shown by Furrer *et al.* [60] using entropic uncertainty relations for smooth entropies. A similar proof was later constructed by Furrer for squeezed-state protocol [61], preceded by the security proof of coherent-state protocol against arbitrary attacks in the finite-size regime derived by Leverrier *et al.* using post-selection and phase-space symmetries [62]. The composable security proof for the coherent-state protocol against collective attacks (and general attacks using post-selection or the de Finetti theorem) was also recently derived by Leverrier [63]. The general security bounds derived up to now are however fragile against imperfections, apply to particular cases of coherent or squeezed signal states and often require additional procedures, such a post-selection or signal monitoring. Hence, the study of the effective general composable security proofs for CV QKD protocols in the finite-size regime is still ongoing.

Another line of information-theoretical research concerned with CV QKD protocols is dedicated to the post-processing algorithms, particularly error correction codes. Error correction is a demanding procedure for Gaussian random variables, especially in the regime of low signal-to-noise ratio (SNR), RR and one-way classical communication. Realistic error correction in this regime scales down the mutual information between the trusted parties and therefore limits the secure key rate, which was first pointed out for CV QKD protocols by Heid and Lütkenhaus [64]. It appeared to be one of the main limiting factors in the early practical implementations of CV QKD, as shown in [65] by Lodewyck *et al.*, where the 10% reduction of mutual information due to imperfect error correction along with other imperfections resulted in the secure distance of the coherent-state protocol being limited by 25 km, similarly to another field test of the coherent-state CV QKD prototype performed by Fossier *et al.* [66]. The novel codes for reconciliation of the Gaussian data in CV QKD were developed afterwards, such as multidimensional codes by Leverrier *et al.* [67], polar and low density parity check codes by Jouguet *et al.* [68,69]. By applying the optimal codes at low SNR regime, Jouguet *et al.* [70] proved that the achievable distance of the coherent-state CV QKD protocols can be extended to 80 km. An alternative way to using the advanced post-processing codes can also be the state engineering. It was in particular shown by Usenko and Filip that the CV QKD protocol with feasible squeezed states and limited Gaussian modulation can be robust against imperfect post-processing [71].

From the point of view of quantum-theoretical analysis, the implementation of CV QKD is naturally limited by physical effects causing the practical imperfections, such as losses and noise in the quantum communication channel. In all of the CV QKD security analysis, the channel is assumed to be fully controlled by an eavesdropper, who can purify the channel noise and compensate the channel loss; therefore, the channel is untrusted. As was mentioned, any level of channel loss is in principle tolerable by a perfect CV QKD protocol with RR [38] even for collective attacks as shown by Grosshans [72] contrary to the DR schemes, which are limited by 50% of channel transmittance. The presence of loss however increases the vulnerability of the protocols to other imperfections, first of all to the

channel excess noise. This was theoretically demonstrated already for the case of individual attacks by Grosshans *et al.* [73] using the equivalent entanglement-based representation of the CV QKD protocols. It was shown that the tolerable channel noise for Gaussian CV QKD protocols is upper bounded by one shot-noise unit (SNU) being the level of the vacuum fluctuations (used as a unit to characterize the amounts of quantum noise), which is more strict than the bound on the Gaussian entanglement breaking, being two SNU of excess noise. The more tight security bounds on the Gaussian channel noise (which complies with the optimality of Gaussian attacks summarized by Leverrier and Grangier [57]) were obtained for the case of collective attacks for coherent- and squeezed-state protocols by Navascués and Acín [74] and for coherent-state protocol, including post-selection, by Heid and Lütkenhaus [75]. It was also shown by Blandino *et al.* that the robustness of the coherent-state CV QKD protocol to the channel imperfections can be improved by the use of noiseless amplifiers [76].

However, channel imperfections are not the only threat to the security of the protocols coming from the physical effects in the set-up, and device imperfections may also contribute to the information on the key, which is accessible to a potential eavesdropper. There are two main approaches to studying the security of QKD with imperfect devices. One is the device-independent (DI) approach, when the protocols are designed in such a way that device imperfections have no impact on the security of the key. This is achieved by verifying the fragile nonclassical properties of the quantum states in the DI QKD, which was inspired by the above-mentioned E91 protocol [11]. The idea of using nonclassical correlations to verify the security of QKD when the devices (including the source of the quantum states) are not trusted was first stated by Mayers and Yao [77] and developed by Barrett *et al.* [78] and by Acín *et al.* [79] to prove security against no-signaling post-quantum eavesdropper, which goes beyond the typical assumption used in QKD that an eavesdropper is limited by the laws of quantum physics. The security of DI QKD protocols against collective attacks in its connection with Bell-type inequality violation was shown by Acín *et al.* [80], and a practical proposal based on heralded qubit amplifier for the implementation of DI QKD protocols was suggested by Gisin *et al.* [81]. The full security of DI QKD was recently shown by Vazirani and Vidick [82]. For the Gaussian CV QKD, however, the possibility to build the fully DI schemes based on the Bell-inequality violation is limited and requires non-Gaussian resources or measurements [83–85]. DI CV QKD protocol was recently suggested by Marshall and Weedbrook [86] based on the qubit encoding [87] using squeezed states and homodyne detection. The potentially more feasible measurement device-independent (MDI) QKD being a way to at least isolate detectors and prevent side-channel attacks was suggested by Braunstein and Pirandola [88] and by Lo *et al.* [89] and supposes the use of an untrusted relay between the trusted parties. Differently from DI QKD, the MDI QKD can be potentially realized only with Gaussian states and measurements. Therefore, the concept of MDI QKD was recently applied to the CV protocols by Pirandola *et al.* [90,91] and studied by Zhang *et al.* [92] and by Li *et al.* [93].

Contrary to DI and MDI QKD, a more practical and robust way to provide security with imperfect devices is to perform a comprehensive characterization of the devices and suggest the feasible methods allowing one to compensate or reduce the possibility of eavesdropping through the device imperfections. In this approach, alternative to DI and MDI QKD, the devices can be assumed trusted, which can be referred to as the device-dependent (DD) approach in QKD. In this case, the devices must be properly studied, modeled and calibrated in order to distinguish their imperfections from the influence of the untrusted quantum channel (otherwise, the so-called 'paranoid' approach in DD QKD, when all of the imperfections are attributed to the channel, has typically very limited applicability, since the security of conventional DD QKD protocols in this case is quickly degraded by the imperfect devices). The trusted noise despite being directly inaccessible to an eavesdropper may, however, still contribute to the information leakage and limit the security of the protocols. On the other hand, the proper amounts of the trusted noise may improve the security of DD QKD protocols by decoupling an eavesdropper from the reference side of the data reconciliation. The two approaches to security of QKD with imperfect devices were recently generalized by Pirandola [94] in their connection to quantum discord (being sufficient for DD QKD and upper bounding the secure key rate) and entanglement (being necessary for DI QKD).

In the current paper, we review the main known results of the studies of trusted noise in CV QKD and also provide some new results filling the gaps that existed in the comprehensive analysis of the role of trusted preparation and detection noise in CV QKD. We show the negative effect of trusted noise on the receiver side of the protocols and the potentially positive role of such noise on the reference side. The novel results of the paper include: the negative role of the trusted detection noise in the DR scheme and the analytical bound on such a noise; the advantage of the squeezed-state protocol above the coherent-state one in the DR regime and the imperfect post-processing; the positive role of the preparation noise in the squeezed-state DR protocol; analysis of the joint influence of the two types of noise simultaneously present in the protocols.

2. Gaussian Continuous-Variable Quantum Key Distribution Protocols

In our work we deal with the Gaussian states of the modes of electromagnetic radiation defined as the states with a Gaussian Wigner function (see [22] for a review). In particular, we consider the coherent states, each being the eigenstate $a|\alpha\rangle = \alpha|\alpha\rangle$ of the annihilation operator of a given mode, as the possible signal states for CV QKD protocols. We study the one-way Gaussian CV QKD protocols based on the Gaussian modulation of the amplitude and phase quadratures, which can be defined as the real and the imaginary parts of the complex amplitude of an n-th mode: $x_n = a_n^\dagger + a_n$ and $p_n = i(a_n^\dagger - a_n)$ with the commutation relation $[x_n, p_n] = 2i$. In such notation, the quadrature fluctuations of a coherent (or of the vacuum) state are equal to one, which is defined as a shot noise unit (SNU). We also consider squeezed states with the fluctuations of one of the quadratures being suppressed below the shot noise.

We study the one-way Gaussian CV QKD protocols as depicted in Figure 1a. The sender trusted party, Alice, prepares a signal state using a source, which can be a laser (in the case of coherent states) or an optical parametric oscillator (in the case of squeezed states). The signal states are characterized by the quadrature values x_S, p_S randomly distributed around zero according to Gaussian distributions with variances $Var(x_S) = \langle x_s^2 \rangle \equiv V_{xS}$ and $Var(p_S) = \langle p_s^2 \rangle \equiv V_{pS}$, while coherent states saturate the uncertainty principle with $V_{xS} = V_{pS} = 1$ SNU. Alice uses the amplitude and phase modulator to apply random quadrature displacements x_M, p_M of amplitude and phase quadratures of the signal states, respectively, so that the resulting modulated state is characterized by quadratures $\{x, p\}_A = \{x, p\}_S + \{x, p\}_M$ with variances $Var(\{x, p\}_A) = V_{\{x,p\}S} + V_{\{x,p\}M}$, where $V_{\{x,p\}M}$ is the variance of the Gaussian modulation applied to x and p quadratures, respectively. All together, the state generation and modulation can be defined as the state preparation.

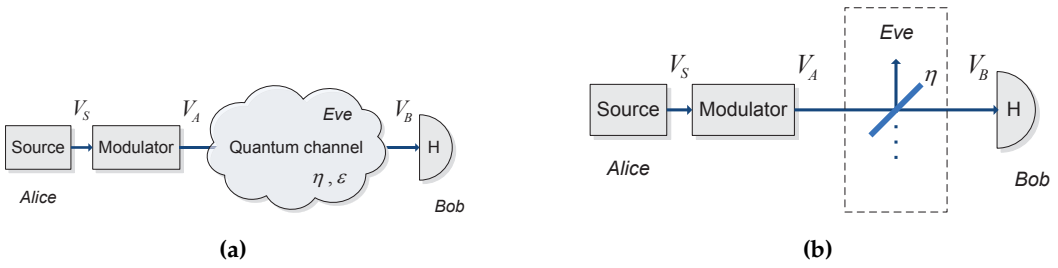

Figure 1. (**a**) Continuous variable (CV) QKD prepare-and-measure (P & M) scheme based on the signal state preparation (with variance V_S in the measured quadrature) in the source and the subsequent modulation using the modulator (up to variance V_A in the measured quadrature) on the side of Alice, propagation through an untrusted quantum channel with loss η and excess noise ϵ, and measurement of the resulting state (with variance V_B in the measured quadrature) by Bob using homodyne detector H; (**b**) Beam splitter model of the eavesdropping attack on P & M CV QKD protocol for the purely attenuating channel. The beam splitter with transmittance η, corresponding to the channel loss, couples the signal to a vacuum mode. The reflected mode is available to an eavesdropper, Eve, for collective measurement.

The modulated state then travels through the untrusted quantum channel, which is generally lossy and noisy, and is measured by the remote trusted party (Bob) using homodyne measurements.

Following the optimality of Gaussian collective attacks on the Gaussian CV QKD, which we discuss later, we assume a Gaussian channel, parametrized by transmittance η and by the variance of the excess noise with respect to the input of the channel ϵ. Then, the quadrature values at the output of the channel, which are measured by the remote trusted party Bob, are $\{x,p\}_B = \sqrt{\eta}(\{x,p\}_A + \{x,p\}_N) + \sqrt{1-\eta}\{x,p\}_0$, where $\{x,p\}_N$ are the quadrature values of the excess noise with variances $Var(\{x,p\}_N) = \epsilon$ (we assume the typical case of the phase-insensitive quantum Gaussian channel), and $\{x,p\}_0$ are the quadrature values of the vacuum state to which the signal is coupled in the standard model for the channel loss, $Var(\{x,p\}_0) = 1$. The variances of the quadratures on the output of the channel are therefore $Var(\{x,p\}_B) = \eta[Var(\{x,p\}_A) + \epsilon] + 1 - \eta$.

In the following, we assume that Bob is measuring the $x-$quadrature, which is also squeezed by Alice if the squeezed-state protocol is considered (*i.e.*, the "x–x" protocol is implemented). We omit the discussion of the heterodyne measurement at Bob's side, because its role is mainly in adding noise to the quadrature measurement. Such noise is known to make the heterodyne protocol suboptimal in the DR case. On the other hand, the noise in the heterodyne detection can also improve the robustness of the protocols in the noisy channels in the RR case, but this improvement can be optimized beyond coupling to a vacuum, as we discuss below. Note that the trusted parties need to perform bases switching in their preparation and measurement to estimate the channel parameters in both the quadratures, but the discussion of the channel estimation is not within the scope of the current paper, so we only consider the measurements, which are contributing to the key rate, assuming that the channel parameters are properly estimated.

The variance of the data measured by Bob in the $x-x$ protocol is then $V_B = \eta(V_A + \epsilon) + 1 - \eta$, where $V_A = V_S + V_M$ is the variance of that modulated at the input of the channel, V_S is the signal state variance and V_M is the modulation variance. The correlation between the datasets at Alice and Bob is then $C_{AB} = \sqrt{\eta}V_M$, scaled down by the channel loss.

The security of the key in QKD protocols is based on the generalization of the Csiszár–Körner theorem [95], which states that the information shared between the trusted parties must exceed the information that a potential eavesdropper (Eve) has on the data that either of the parties possesses, then the classical algorithms can distill the secure key. It was extended to the case of quantum communication taking into account the possibility of an eavesdropper to perform the more general collective measurement (which involves storing probe states after their interaction with the signal in a quantum memory and then optimal collective measurement on the probes) by Devetak and Winter [15], who derived the lower bound on the secure key in QKD as:

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

where indexes DR and RR stand for direct and reverse reconciliation, respectively. The positivity of the lower bound Equation (1) means that the quantum protocol is secure because the classical data processing algorithms (error correction, privacy amplification) are then able to distill the secret key from the data shared between the trusted parties if they have the information advantage over an eavesdropper.

The Gaussian states were shown to minimize the functions of the states that satisfy the continuity in the trace norm, the invariance under local unitary transformations and the strong super-additivity [44]. The lower bound on the key rate satisfies these conditions, and therefore, the attacks, which preserve the Gaussian character of the states are optimal [42,43]. This allows us to analyze the security of CV QKD protocols considering only Gaussian channels (characterized by transmittance η and Gaussian excess noise ϵ) and the Gaussian properties of the states.

The quantity I_{AB} in Equation (1) is the classical mutual information, which is the symmetrical quantity, expressed though the entropies of the input random variable X and the output random variable Y of a channel as $I_{XY} = H(X) + H(Y) - H(XY) = H(X) - H(X|Y)$, where $H(XY)$ is the

joint entropy, quantifying the amount of transmission errors, and $H(X|Y)$ is the conditional entropy of the input with respect to the output. On the other hand, χ_{AE} and χ_{BE} are the Holevo quantities [96] in the case of DR and RR, respectively, being the capacity of a hypothetical bosonic channel between an eavesdropper and the reference side of data reconciliation. The Holevo quantity then upper bounds the classical information available to an eavesdropper upon collective attacks. Finally, the post-processing efficiency $\beta \in (0,1)$, typically taking values of up to 0.95 for the Gaussian data in RR at low SNR [68], is introduced as a factor to the mutual information in the lower bounds Equation (1). It defines how close the trusted parties can approach the classical mutual information, taking into account the reduction of data ensembles in the process of error correction. For the finite efficiency β, the modulation variance V_M needs to be limited and optimized [65,71].

In the case of the Gaussian-distributed continuous random variables, the classical mutual information between the trusted parties can be calculated from the variances and the conditional variances of the data possessed by these parties as, for example,

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}} \tag{2}$$

where V_A is the variance of Alice's data (V_M in our case) and $V_{A|B}$ is the variance of Alice's data conditioned on the measurement results of Bob, which can be expressed through the correlation C_{AB} between Alice and Bob, and the variance V_B of Bob's data as $V_{A|B} = V_A - C_{AB}^2/V_B$. Taking base-two logarithms, we estimate the mutual information and other information quantities further (e.g., the lower bound on the key rate) in bits per use of the channel.

The Holevo bound $\chi_{YE} = S(E) - S(E|Y)$ between Eve and the reference trusted party Y is calculated as the difference of the von Neumann (quantum) entropy $S(E)$ of the state available to an eavesdropper and the conditional entropy $S(E|Y)$ of the eavesdropper's state conditioned on the measurement results of the reference side of the protocol, here denoted as Y (the latter entropy in the general case should be integrated over all possible outcomes of the measurement on Y, but collapses in the case of the Gaussian-distributed data). A generally multimode Gaussian state is explicitly described by a covariance matrix γ with elements $\gamma_{ij} = (\langle r_i r_j\rangle + \langle r_j r_i\rangle)/2 - \langle r_i\rangle\langle r_j\rangle$ containing the second moments of the quadratures in the form $r_i = \{x_i, p_i\}$ for an i-th mode, *i.e.*, variances of the modes' quadratures and quadrature correlations between the modes. Following the above-mentioned optimality of Gaussian collective attacks, it is the worst case assumption that the states involved in CV QKD are Gaussian, and therefore, the covariance matrix formalism is sufficient for security analysis of the Gaussian protocols.

The von Neumann entropy $S(E)$ of a general N-mode Gaussian state can be directly calculated using the symplectic eigenvalues $\lambda_{\{1..N\}}$ of the covariance matrix γ_E of a state through the bosonic entropic function [97] $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ as:

$$S(E) = \sum_{i=1}^{N} G\Big(\frac{\lambda_i - 1}{2}\Big) \tag{3}$$

Similarly, the conditional entropy is in the case of the Gaussian states straightforwardly calculated though the symplectic eigenvalues of the conditional covariance matrix $\gamma_{E|Y}$, calculated after the homodyne measurement in x-quadrature on mode Y as:

$$\gamma_{E|Y} = \gamma_Y - \sigma_{EY}\,(X\cdot\gamma_Y\cdot X)^{MP}\,\sigma_{EY}^T \tag{4}$$

where σ_{EY} is the correlation matrix between the mode(s) accessible to an eavesdropper and the mode Y measured by a trusted party; the diagonal matrix $X = Diag(1,0)$ (similarly, matrix $P = Diag(0,1)$ would stand for the measurement in p-quadrature); and MP stands for the Moore–Penrose (pseudo-)inverse of a matrix [98], which is used because the matrix $X\cdot\gamma_Y\cdot X$ is singular.

The symplectic eigenvalues of the covariance matrices can be analytically found using the Williamson's form of a covariance matrix for one- and two-mode matrices [99] or numerically for a higher number of modes.

In the P & M scheme assuming the symmetrical modulation of both the quadratures of a signal state with the diagonal covariance matrix $\gamma_S = Diag(V_S, 1/V_S)$ with the same variance V_M, the covariance matrix of the modulation data possessed by Alice is given by $\gamma_A^{mod} = Diag(V_M, V_M)$. After the channel characterized by loss η and excess noise ϵ, the signal state measured by Bob is characterized by the matrix $\gamma_B = Diag\big(\eta[V_S + V_M + \epsilon] + 1 - \eta, \eta[1/V_S + V_M + \epsilon] + 1 - \eta\big)$. The mutual information between Alice and Bob is then given by:

$$I_{AB} = \frac{1}{2}\log_2\left[1 + \frac{\eta V_M}{\eta(V_S + \epsilon) + 1 - \eta}\right] \tag{5}$$

In the simple case of a purely-attenuating channel ($\epsilon = 0$), the state γ_E is explicitly defined as the output of the beam splitter with transmittance η, which models the channel by coupling the signal to a vacuum [72], as shown in Figure 1b. In this case, the covariance matrix of the state available to Eve for collective measurement is given by $\gamma_E = Diag\big([1-\eta](V_S + V_M) + \eta, [1-\eta](1/V_S + V_M) + \eta\big)$, while the matrices describing the correlation between Eve and Alice and Eve and Bob, respectively, are $\sigma_{AE} = -\sqrt{1-\eta}V_M\mathbb{I}$, where $\mathbb{I}$ is the 2×2 unity matrix, and $\sigma_{BE} = Diag(\sqrt{\eta(1-\eta)}[1 - V_S - V_M], \sqrt{\eta(1-\eta)}[1 - 1/V_S - V_M])$. The straightforward calculations based on the symplectic eigenvalues of covariance matrices γ_E and $\gamma_{E|B}$ or $\gamma_{E|A}$ result in the analytical lower bounds on the key rate Equation (1), which can be simplified in the limit of arbitrarily strong modulation $V_M \to \infty$ and in the regime of perfect post-processing $\beta = 1$ as:

$$K_{DR}^{V_M\to\infty} = \frac{1}{2}\left[\log_2\frac{\eta}{1-\eta} - \log_2\frac{V_S\eta + 1 - \eta}{V_S(1-\eta) + \eta}\right] \tag{6}$$

and:

$$K_{RR}^{V_M\to\infty} = \frac{1}{2}\left[\log_2\frac{1}{1-\eta} - \log_2\left(\eta V_S + 1 - \eta\right)\right] \tag{7}$$

for an arbitrary signal state with variance V_S or as:

$$K_{DR,coh}^{V_M\to\infty} = \frac{1}{2}\log_2\frac{\eta}{1-\eta}, K_{RR,coh}^{V_M\to\infty} = \frac{1}{2}\log_2\frac{1}{1-\eta} \tag{8}$$

for coherent states ($V_S = 1$) and as:

$$K_{DR,sq}^{V_M\to\infty} = \log_2\frac{\eta}{1-\eta}, K_{RR,sq}^{V_M\to\infty} = \log_2\frac{1}{1-\eta} \tag{9}$$

for the infinitely-squeezed states ($V_S \to 0$), which gives a lower bound on the key rate twice as large compared to the infinitely-modulated coherent states [72].

In the more general case, when the channel noise is present, it is assumed that Eve is able to purify the channel noise, and so, the Holevo bound can be assessed by using the purification method [43]. When Eve is holding the purification of the channel noise, the state of the system ABE shared between Alice, Bob and Eve is pure, so that $S(ABE) = 0$ and, from the triangle inequality [100], directly follows that $S(E) = S(AB)$. Similarly, when Alice or Bob perform the projective measurement of the respective subsystem A or B, the state of the systems BE or AE is pure, and it follows that $S(E|A) = S(B|A)$ or $S(E|B) = S(A|B)$. This allows estimating the Holevo bound from the entropic characteristics of the state shared between Alice and Bob, where all of the impurity is attributed to Eve.

To analyze the security in the above described case of collective attacks in a noisy channel, the equivalent EPR-based representation [73] is used to purify the state preparation at Alice's side, as shown in Figure 2. Indeed, the state of the system AB must be pure before the interaction in the quantum channel with Eve's system in order to distinguish between the trusted and untrusted noise; otherwise, all of the impurity of this state would also be attributed to Eve. If the prepared state on the input of the channel is a zero-mean thermal state with variance V_A, being symmetric on the phase space, the state preparation is purified by a two-mode squeezed vacuum quadrature-entangled state with variance V_A of the spatial modes A and B shared between Alice and Bob, respectively. Such a state is described by a two-mode covariance matrix of the form:

$$\gamma_{AB} = \begin{pmatrix} V_A \mathbb{I} & \sqrt{V_A^2 - 1}\sigma_z \\ \sqrt{V_A^2 - 1}\sigma_z & V_A \mathbb{I} \end{pmatrix} \tag{10}$$

with $\sigma_z = Diag(1, -1)$.

After the homodyne measurement on mode A performed by Alice and yielding the result x_A, the squeezed state with variance $1/V_A$ in the x-quadrature is conditionally prepared in mode B, centered around $\sqrt{1 - 1/V^2}(x_A, 0)$ (the variance of the conditionally-prepared states in p-quadrature is respectively V_A). Therefore, the EPR-based scheme with the states Equation (10) and homodyne measurement at Alice becomes fully equivalent to the P & M scheme with $V_S = 1/V_A$ and $V_M = V_A - 1/V_A$, *i.e.*, the squeezed states in the standard protocol are modulated up to the variance of the anti-squeezed quadrature.

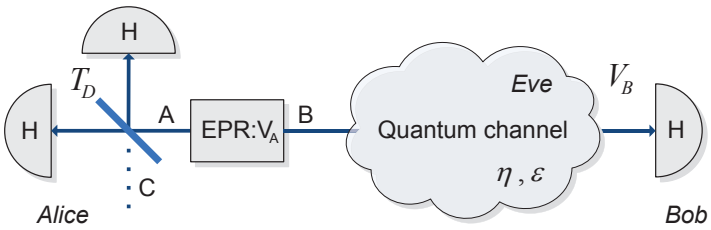

Figure 2. Entanglement-based representation of CV QKD protocols, equivalent to the P & M scheme with the symmetrical state preparation. The entangled source $EPR : V_A$ producing two non-classically correlated modes with quadrature variances V_A in modes A and B is placed at the sender side, Alice, who performs either homodyne measurement (corresponding to setting transmittance $T_D = 1$ for a beam splitter, which couples the mode A to the vacuum mode C), equivalent to the preparation of squeezed states, or heterodyne (corresponding to setting $T_D = 1/2$), equivalent to preparation of coherent states. The rest of the scheme is the same as in the P & M scenario in Figure 1a.

Similarly, if Alice performs heterodyne measurement on her mode A (which is equivalent to splitting the mode A on a beam splitter set to $T_D = 1/2$ with another input mode C being in a vacuum state, and then measurement of both the output modes in x and p quadratures), resulting in the outcome $\{x_A, p_A\}$, the coherent state centered around $\sqrt{2(V-1)/(V+1)}(x_A, p_A)$ is conditionally prepared in the mode B. The EPR-based scheme with heterodyne detection is then fully equivalent to the P & M scheme with coherent signal states ($V_S = 1$) and modulation variance $V_M = V_A - 1$.

Note that in the general case, the modulation variance can be independent of the signal state variance. While this is easily accessible in the case of the coherent-state protocol, where modulation variance V_M is a free parameter, it is not in the standard squeezed-state symmetrical protocol where modulation depth is fixed by the antisqueezing. Therefore, the generalized EPR-based scheme, which is equivalent to the preparation of the arbitrarily-squeezed signal state $V_S \in [0, 1]$ and modulation with arbitrary variance was suggested to analyze the role of squeezing in CV QKD [71] and will be used in

the further analysis instead of the standard EPR-based scheme by replacing the entangled source in the cases when modulation needs to be optimized independently of the signal state squeezing.

In the standard EPR-based scheme, the entropy $S(E) = S(AB)$, being the first part of the Holevo bounds χ_{BE} and χ_{AE}, is calculated from the Gaussian state of modes AB described by the covariance matrix after the propagation through the channel:

$$\gamma'_{AB} = \begin{pmatrix} V_A \mathbb{I} & \sqrt{\eta(V_A^2-1)}\sigma_z \\ \sqrt{\eta(V_A^2-1)}\sigma_z & [\eta(V_A+\epsilon)+1-\eta]\mathbb{I} \end{pmatrix} \tag{11}$$

(the coupling to mode C being in a pure vacuum state can be omitted in this case because it does not affect the purity of the overall state shared between the trusted parties).

Similarly, the entropy $S(E|B) = S(A|B)$, being the second part of the Holevo bound χ_{BE}, can be obtained from the respective conditional matrix of mode A conditioned on the measurement on mode B:

$$\gamma'_{A|B} = \begin{pmatrix} V_A - \frac{\eta(V_A^2-1)}{\eta(V_A+\epsilon)+1-\eta} & 0 \\ 0 & V_A \end{pmatrix} \tag{12}$$

In the case of a squeezed-state protocol, the entropy $S(E|A) = S(B|A)$, being the second part of the Holevo bound χ_{AE}, can be obtained from the respective conditional matrix of mode B conditioned on the measurement on mode A:

$$\gamma'_{B|A} = \begin{pmatrix} \eta(1/V_A+\epsilon)+1-\eta & 0 \\ 0 & \eta(V_A+\epsilon)+1-\eta \end{pmatrix} \tag{13}$$

However, for the entropy $S(E|A)$ in the case of a coherent-state protocol, the structure of the measurement at Alice must be taken into account, so the equality $S(E|A) = S(BC|A)$ holds, and the entropy must be calculated from the matrix of modes BC conditioned on the x-measurement on mode A:

$$\gamma'_{BC|A} = \begin{pmatrix} 1+\eta\epsilon & 0 & -\frac{\sqrt{2\eta}(V_A-1)}{\sqrt{V_A^2-1}} & 0 \\ 0 & \eta(V_A+\epsilon)+1-\eta & 0 & \frac{\sqrt{\eta(V_A^2-1)}}{\sqrt{2}} \\ -\frac{\sqrt{2\eta}(V_A-1)}{\sqrt{V_A^2-1}} & 0 & \frac{2V_A}{V_A+1} & 0 \\ 0 & \frac{\sqrt{\eta(V_A^2-1)}}{\sqrt{2}} & 0 & \frac{1+V_A}{2} \end{pmatrix} \tag{14}$$

From the derived matrices, the key rate can be calculated numerically.

The security of the protocols in terms of the positivity of the lower bound on the secure key rate is thus limited by the channel transmittance and channel noise, which have a joint negative impact on security. Therefore, the protocols are mainly studied in terms of the tolerable loss (or, equivalently, the secure distance, assuming a standard telecom fiber with -0.2 dB attenuation per kilometer) and tolerable channel excess noise. We illustrate the typical performance of the protocols in the regime of optimal modulation for the given $\beta = 0.95$ for RR and $\beta = 0.99$ for DR (since the SNR is typically higher as the DR is applicable only for low loss, and the post-processing is less demanding in the DR regime) in Figure 3. It is evident that RR CV QKD provides security at much stronger values of attenuation, while DR CV QKD can tolerate higher noise in the low-loss channels. The squeezed-state protocol shows better performance and robustness to noise in the RR case both for the perfect and imperfect post-processing. Interestingly, in the regime of non-ideal post-processing, the squeezed-state protocol also becomes superior to the coherent-state one in the DR case.

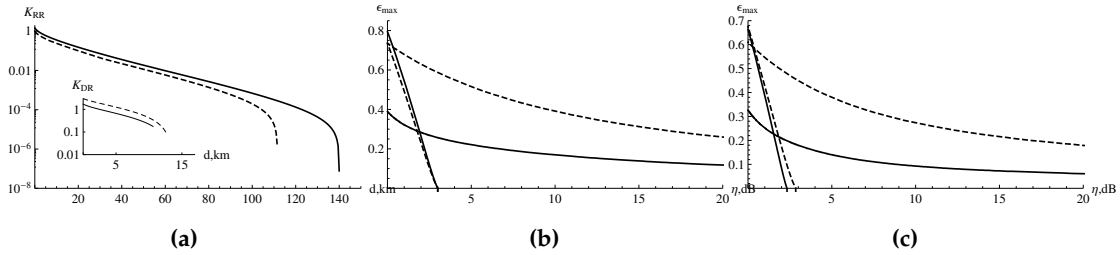

Figure 3. (**a**) Lower bound on secure key rate against channel distance in the telecom fiber with loss of -0.2 dB/km for direct reconciliation (DR) (main graph) and reverse reconciliation (RR) (inset) with imperfect post-processing, finite squeezing $V_S = 0.1$ and optimized modulation; (**b**) maximum tolerable channel excess noise with respect to channel loss in dB for the idealized case with perfect post-processing, infinite squeezing and arbitrarily strong modulation; (**c**) maximum tolerable channel excess noise with respect to channel loss in dB for the realistic case with imperfect post-processing, finite squeezing $V_S = 0.1$ and optimized modulation. In all of the graphs, solid lines are for the coherent-state protocol, and dashed lines are for the squeezed-state one. The imperfect post-processing is taken as $\beta = 0.95$ for RR and $\beta = 0.99$ for DR. The curves on the maximum tolerable channel excess noise plots, which vanish at (or below) 3 dB, correspond to DR; the rest refer to RR.

The above-described P & M CV QKD protocol with coherent states was realized using homodyne detection by Lodewyck *et al.* [65] and by Jouguet *et al.* [70] and using heterodyne detection (corresponding to the no-switching regime) by Lance *et al.* [101].

Besides the fixed (fiber-type) channels, where transmittance is stable and excess noise is relatively low, the Gaussian CV QKD protocols were shown potentially applicable in the free-space atmospheric channels, where transmittance fluctuations due to atmospheric turbulence lead to additional excess noise, which can be however tolerated or compensated by post-selection [102].

The CV QKD protocols were also studied with respect to the imperfections of the trusted devices. First, the real homodyne detectors are inclined to non-unity detection efficiency and electronic noise, which altogether corrupt the data obtained by Bob from the homodyne measurement. The trusted detection noise in the coherent-state RR CV QKD protocol was first taken into account by Lodewyck *et al.* [65] and later considered in the squeezed-state RR protocol by Garcia-Patron and Cerf [103], who had shown that the trusted detection noise can even be helpful to provide robustness against the channel noise. It was also shown by Fossier *et al.* [104] that the negative impact of imperfect detectors in the RR coherent-state CV QKD can be compensated using optical pre-amplifiers.

On the trusted sender side, the state generation and modulation can also be imperfect, which results in the excess noise added to the signal at the stage of the state preparation. The preparation noise can therefore be the noise of the signal state itself (e.g., if a thermal state is produced by a noisy laser instead of a coherent one) or the noise added by an imperfect modulator. Such preparation noise was first addressed by Filip [105] and shown harmful for the RR coherent-state CV QKD protocol for purely attenuating channels and then extended by Usenko and Filip to the noisy channels [106]. It was also shown that the preparation noise can be purified by attenuating the signal (using, e.g., a simple variable beam splitter) prior to sending it to the channel. The method allows reduction (up to complete elimination in the regime of strong modulation) of the preparation noise. Later, it was shown by Weedbrook *et al.* [107,108] that the preparation noise can be tolerable and even helpful for the security of the DR coherent-state CV QKD protocol in the noisy channels.

The role of other practical imperfections in coherent-state CV QKD was analyzed by Jouguet *et al.* [109], who studied the imperfect realistic Gaussian modulation, the calibration of the detectors and the trusted phase noise in the sender station, and it was shown that these effects should be taken into account in the security analysis, especially in the finite-size regime. It was also shown that CV QKD systems can be in principle compromised using a wavelength attack on the local oscillator in

the heterodyne [110,111] and homodyne [112] detection, which can be however prevented by spectral filtering or real-time monitoring of shot noise [113], the latter being also useful against the calibration attacks on the clock pulses in coherent-state CV QKD [114]. Furthermore, the fluctuations of the local oscillator were shown to be potentially harmful in CV QKD [115], which can be compensated by tuning and monitoring of the intensity of the local oscillator by the trusted parties [116].

3. Trusted Preparation and Detection Noise in CV QKD

In the current paper, we complete the analysis of the role of trusted preparation and detection noise in CV QKD with coherent and squeezed states, generalizing and extending the previously-known results. We consider the phase-insensitive excess noise added to the signal prior to the channel (preparation noise with variance ΔV) and added to the signal after the channel (detection noise with variance N), as shown in Figure 4a.

The preparation and detection types of noise in the P & M scheme do not affect the data, which Alice imposes by the modulation, as well as the correlation between Alice and Bob, but they change the covariance matrix of the state measured by Bob to $\gamma_B = Diag(\eta[V_S + V_M + \epsilon + \Delta V] + 1 - \eta + N, \eta[1/V_S + V_M + \epsilon + \Delta V] + 1 - \eta + N)$. Therefore, the mutual information between Alice and Bob reads:

$$I_{AB} = \frac{1}{2}\log_2\left[1 + \frac{\eta V_M}{\eta(V_S + \epsilon + \Delta V) + 1 - \eta + N}\right] \tag{15}$$

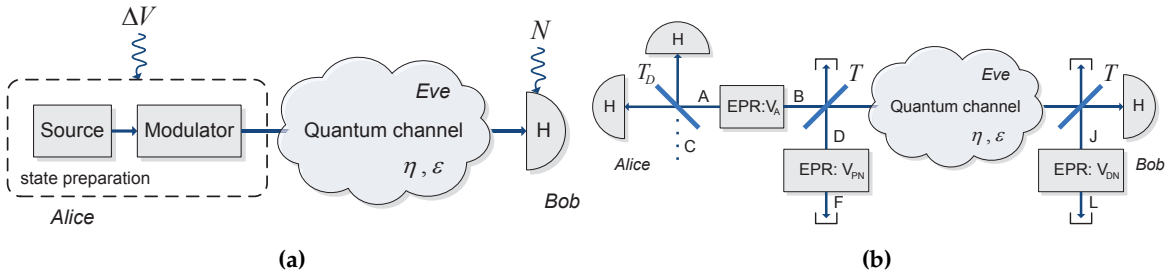

Figure 4. (**a**) CV QKD P & M scheme with trusted preparation excess noise with variance ΔV, affecting the state preparation, and trusted detection excess noise with variance N, which affects the homodyne detector; (**b**) Equivalent EPR-based representation of the P & M scheme used for purification of the trusted noise, which is done by introducing entangled sources with variances V_{PN} and V_{DN} on the sender and receiver side, respectively, and coupling one of the modes of each of the entangled sources to the signal mode on a strongly unbalanced beam splitter with transmittance $T \to 1$ for the signal modes, which, under proper setting of variances V_{PN} and V_{DN}, becomes equivalent to the lossless addition of trusted excess noise.

It is evident that both the preparation and detection types of noise reduce the mutual information. However, the effect on the security of the protocols can be different, as we show in the following sections, since the trusted noise also affects the Holevo bounds, which upper limit Eve's information.

In the simplest case of a purely lossy channel, the covariance matrix of the state available to Eve for collective measurement reads $\gamma_E = Diag\big([1-\eta](V_S + V_M + \Delta V) + \eta, [1-\eta](1/V_S + V_M + \Delta V) + \eta\big)$, the correlation matrix σ_{AE} is not changed, while the correlation matrix σ_{BE} becomes affected by the preparation noise and reads $\sigma_{BE} = Diag(\sqrt{\eta(1-\eta)}[1 - V_S - V_M - \Delta V], \sqrt{\eta(1-\eta)}[1 - 1/V_S - V_M - \Delta V])$. The lower bound on the key rate can be then calculated analytically from these covariance matrices and will be analyzed in the particular cases in the following section.

In the more general case of a noisy untrusted channel, when a purification method must be applied and an equivalent EPR-based scheme is used instead of the P & M one, the trusted preparation and detection noise can be purified by introducing additional EPR sources of modes DF and JL,

respectively, and coupling one of the modes of each of the sources to the signal, as shown in Figure 4b. A similar approach was previously used to purify the preparation [106] and detection noise [65] in CV QKD purification-based security analysis. To losslessly add the trusted excess noise on the preparation and detection stage, the transmittance of the beam splitters used to couple the noisy modes with the signal should be made very high $T \to 1$. Then, after setting variances of the EPR-sources to $V_{PN} = \Delta V/(1-T)$ for the preparation noise and $V_{DN} = N/(1-T)$ for the detection noise, the coupling to EPR modes becomes numerically equivalent to the phase-insensitive trusted preparation excess noise ΔV and detection excess noise N, respectively. Alternatively, purification of the preparation noise (as well as of the detection noise) can be held by a third party [117,118], which however gives the same result as the lossless coupling to an EPR mode.

The calculation of the Holevo bounds in the case of noisy channels is based on the purity of the multimode state shared between the trusted parties and the fact that Eve holds the purification of the channel noise, so that $S(E) = S(ABDFJL)$, $S(E|B) = S(ADFJL|B)$ and $S(E|A) = S(BDFJL|A)$ for squeezed-state protocol and $S(E|A) = S(BCDFJL|A)$ for the coherent-state protocol. The overall covariance matrix of the state of the modes $ABDFJL$ after the propagation through the channel has the form:

$$\gamma'_{ABDFJL} = \begin{pmatrix} V_A\mathbb{I} & \tilde{C}_{AB}\sigma_z & C_{AD}\sigma_z & 0 & C_{AJ}\sigma_z & 0 \\ \tilde{C}_{AB}\sigma_z & \tilde{V}_B\mathbb{I} & C_{BD}\mathbb{I} & C_{BF}\sigma_z & C_{BJ}\mathbb{I} & C_{BL}\sigma_z \\ C_{AD}\sigma_z & C_{BD}\mathbb{I} & \tilde{V}_D & C_{DF}\sigma_z & C_{DJ}\mathbb{I} & 0 \\ 0 & C_{BF}\sigma_z & C_{DF}\sigma_z & V_{PN}\mathbb{I} & C_{FJ}\sigma_z & 0 \\ C_{AJ}\sigma_z & C_{BJ}\mathbb{I} & C_{DJ}\mathbb{I} & C_{FJ}\sigma_z & \tilde{V}_J\mathbb{I} & C_{JL}\sigma_z \\ 0 & C_{BL}\sigma_z & 0 & 0 & C_{JL}\sigma_z & V_{DN}\mathbb{I} \end{pmatrix} \tag{16}$$

where:

$$\begin{aligned} \tilde{C}_{AB} &= T\sqrt{\eta(V_A^2-1)}, \\ C_{AD} &= -\sqrt{(1-T)(V_A^2-1)}, \\ C_{AJ} &= -\sqrt{\eta T(1-T)(V_A^2-1)}, \\ \tilde{V}_B &= T(\eta[TV_A + (1-T)V_{PN} + \epsilon] + 1 - \eta) + (1-T)V_{DN}, \\ C_{BD} &= T\sqrt{\eta(1-T)}(V_{PN} - V_A), \\ C_{BF} &= \sqrt{\eta T(1-T)(V_{PN}^2-1)}, \\ C_{BJ} &= \sqrt{T(1-T)}(V_{DN} - \eta[TV_A + (1-T)V_{PN} + \epsilon] - 1 + \eta), \\ C_{BL} &= \sqrt{(1-T)(V_{DN}^2-1)}, \\ \tilde{V}_D &= TV_{PN} + (1-T)V_A, \\ C_{DF} &= \sqrt{T(V_{PN}^2-1)}, \\ C_{DJ} &= (1-T)\sqrt{\eta T}(V_A - V_{PN}), \\ C_{FJ} &= -(1-T)\sqrt{\eta(V_{PN}^2-1)}, \\ \tilde{V}_J &= TV_{DN} + (1-T)\Big[\eta[TV_A + (1-T)V_{PN} + \epsilon] + 1 - \eta\Big], \\ C_{JL} &= \sqrt{T(V_{DN}^2-1)} \end{aligned} \tag{17}$$

The conditional matrices used for calculation of the conditional von Neumann entropies can be obtained using Equation (4). From these matrices, the Holevo bound and, respectively, the lower bound on the key rate in the case of collective attacks in a noisy channel can be obtained numerically and will be used in the analysis in the following sections.

4. Trusted Noise as a Threat

4.1. Preparation Noise and Reverse Reconciliation

It was previously shown that the trusted preparation noise can break the security of the coherent-state RR CV QKD protocol already for the purely lossy channel in the case of individual attacks [105], which was later extended on the noisy channels [106]. Here, we generalize the result for the arbitrary pure signal states and show that the tolerance to the preparation noise depends on the signal state squeezing. Indeed, following the calculations given in the previous section, we can derive the lower bound on the key rate for RR in the case of collective attacks on the noisy channel, which in the limit of strong modulation ($V_M \to \infty$) converges to the simple modification of the expression Equation (7):

$$K_{RR}^{V_M \to \infty} = \frac{1}{2}\left[\log_2 \frac{1}{1-\eta} - \log_2 \left(\eta[V_S + \Delta V] + 1 - \eta\right)\right] \tag{18}$$

From this follows that even in the case of a purely-attenuating channel and perfect implementation of the RR CV QKD protocol, the security against collective attacks is bounded by the condition:

$$\Delta V < \frac{2-\eta}{1-\eta} - V_S \tag{19}$$

which converges to the previously-known bound $\Delta V < 1/(1-\eta)$ for the coherent-state RR protocol [105]. Thus, in the limit of strong attenuation $\eta \to 0$, which is the region of interest for the RR protocols aimed at implementation upon strong loss compared to the DR ones, the coherent-state protocol can tolerate up to 1 SNU of excess preparation noise ΔV, while the squeezed-state protocol with infinite squeezing $V_S \to 0$ would tolerate preparation excess noise $\Delta V = 2$ SNU, which illustrates another potential advantage of the squeezed-state RR CV QKD. However, much stronger preparation noise can be tolerated either upon higher channel transmittance (in the limit $\eta \to 1$, arbitrarily-strong preparation noise is tolerable by RR CV QKD protocols) or by using the noise filtering method (originally called purification by the authors), when the signal is attenuated prior to being sent to the channel [105,106], which optimally can completely remove the negative impact of preparation noise in RR CV QKD with infinite modulation or at least strongly suppress such impact in the realistic case [106]. Furthermore, the monitoring of the source noise [119] or noiseless amplification [120] can be applied to improve the security of CV QKD with noisy coherent states. Alternatively, DR CV QKD protocols can be used, since, as it was shown and as we recapitulate further, they are in principle robust against preparation noise [107,108].

The given amount of preparation noise effectively limits the tolerable channel loss, which can be seen from the reversed security bound in terms of the channel loss $\eta > 1 - 1/\Delta V$ for the coherent-state protocol or $\eta > 1 - 1/(\Delta V - 1)$ for infinitely-squeezed states. This imposes a limitation on the channel transmittance in the otherwise perfect implementation starting from $\Delta V = 1$ SNU for the coherent-state protocol and for $\Delta V = 2$ SNU for the squeezed-state one with arbitrarily-strong squeezing.

The preparation noise also reduces the robustness of the protocol to the channel noise, as can be seen in Figure 5a, where the tolerable channel excess noise is given in the presence of preparation noise $\Delta V = 0.5$ SNU in comparison to the perfect implementation of the protocols.

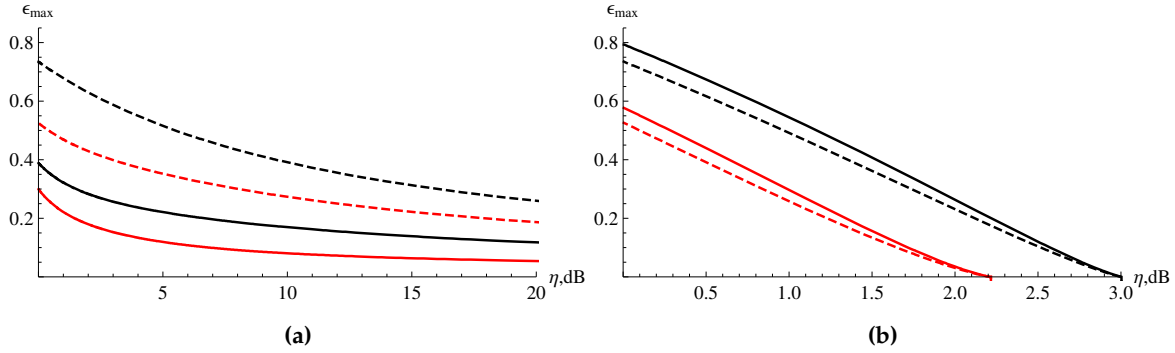

Figure 5. Maximum tolerable channel excess noise with respect to channel loss in dB for the idealized case with perfect post-processing and arbitrarily strong modulation for the coherent-state protocol (solid lines) and the squeezed-state protocol with infinite squeezing (dashed lines). (**a**) RR upon perfect implementation (black, upper lines) or in the presence of preparation noise $\Delta V = 0.5$ shot-noise units (SNU) (red, lower lines); (**b**) DR upon perfect implementation (black, upper lines) or in the presence of detection noise $N = 0.5$ SNU (red, lower lines).

The mechanism of the negative effect of preparation noise in the RR CV QKD is two-fold. Firstly, it reduces the mutual information; secondly, it also increases the Holevo bound, *i.e.*, the upper bound on the information leakage, since this type of noise is added prior to the channel and contributes to Eve's information. The preparation noise thus increases both the von Neumann entropies contributing to the Holevo bound, $S(E)$, as well as $S(E|B)$; however, the first one grows faster, and the Holevo bound is increased.

In the practical situations of limited modulation and other imperfections the RR CV QKD protocol is even more sensitive to the preparation noise; we will consider the effect of imperfections jointly in the Section 6.

4.2. Detection Noise and Direct Reconciliation

While the DR CV QKD protocols are robust to the preparation noise, they are sensitive to the detection noise, which can lead to a security break, as we show here. Indeed, already in the limit of arbitrarily-strong modulation and perfect implementation of the protocol, when the key rate converges to the simple modification of Equation (6) as:

$$K_{DR}^{V_M\to\infty} = \frac{1}{2}\left[\log_2\frac{\eta}{1-\eta} - \log_2\frac{V_S\eta + 1 - \eta + N}{V_S(1-\eta)+\eta}\right] \tag{20}$$

the security is bounded by the condition:

$$N < \frac{2\eta - 1}{1-\eta} \tag{21}$$

which does not depend on the state squeezing V_S. The bound converges to zero, which means that any amount of detection noise cannot be tolerated by DR CV QKD, when the loss approaches 50% (being the loss limit for DR protocols). On the other hand, reciprocally to the preparation noise in the RR case, large amounts of detection noise can be tolerated by the protocol, when the channel approaches lossless transmission ($\eta \to 1$). In the non-ideal case, however, detection noise can be harmful and must be seriously taken into account in any implementation of the DR protocols. Moreover, such noise quickly (faster than preparation noise in the RR case) limits the tolerable channel loss already for the otherwise perfect implementation of the protocols ($\beta = 1$, $\epsilon = 0$, $V_M \to \infty$). Indeed, the bound on the detection noise can be reversed to the bound on the channel loss being $\eta > 1 - 1/(N+2)$. That means

that, e.g., for 1 SNU of detection noise, the transmittance even for the purely lossy channel should be no less than 66%.

In the presence of channel noise, similarly to the RR and preparation noise, the detection noise also reduces the robustness of the DR protocol to the channel noise, as can be seen in Figure 5b, where the tolerable channel excess noise is given in the presence of detection noise $N = 0.5$ SNU in comparison to the perfect implementation of the protocols. Moreover, it can be seen that such an amount of detection noise already reduces the tolerable channel loss even for a purely attenuating channel.

Remarkably, the Holevo bound χ_{AE} is not sensitive to the detection noise; already in the purely lossy channel case, this noise is not present in the covariance matrices γ_E and $\gamma_{E|A}$ and, thus, does not contribute to the information leakage (similarly for in the presence of the channel noise). Therefore, the security break due to detection noise in DR CV QKD is caused only by reduction of the mutual information I_{AB} between the trusted parties.

However, the trusted noise not only breaks the security, but can also improve the protocols, as we recapitulate and show in the next section.

5. Trusted Noise as a Defense

Despite the fact that trusted noise reduces the mutual information between the trusted parties, it can also, if applied at the reference side of the protocol, effectively decrease the information possessed by an eavesdropper on the data of the respective trusted party, that is decrease the Holevo quantity, upper bounding Eve's information. In the conditions of noisy channels, such a decrease can improve the key rate and extend the bounds of the tolerable channel noise, which is also known as "fighting noise with noise". Further, we describe such effects for DR and RR protocols.

5.1. Preparation Noise and Direct Reconciliation

It was already shown that the preparation noise not only can be tolerated by the coherent-state DR CV QKD protocol [107,108] (at least upon perfect implementation with $\beta = 1$), but also improves the robustness of the DR protocols to the channel noise. Here, we generalize the result for the arbitrarily signal states and show the levels and the mechanisms of such an improvement.

We demonstrate the typical effect of the preparation noise on the lower bound on the key rate in the DR CV QKD in Figure 6a for fixed channel transmittance and different amounts of the channel noise. When the channel noise is low, the preparation noise gradually reduces the key rate. As the channel noise increases, slight improvement becomes visible for low amounts of preparation noise. Close to the maximum tolerable channel noise; however, the preparation noise evidently improves the key rate and can even restore the security of the protocol. Similar behavior is observed for other channel transmittances. Interestingly, while the squeezed-state protocol is quantitatively superior to the coherent-state one already for feasible squeezing of $V_S = 0.1$ at low channel noise, the situation becomes opposite close to the maximum tolerable channel noise. The presence of the preparation noise in this case makes coherent- and squeezed-state protocols quantitatively equivalent. Evidently, the preparation noise must be optimized to maximize the key rate as the channel noise gets stronger, while close to the maximum tolerable channel noise, the effect of preparation noise saturates. It is also evident that quantitative improvement is such a regime is very small, and one could expect that the improvement would be canceled by the finite-size effects, which reduce the key rate [55,56].

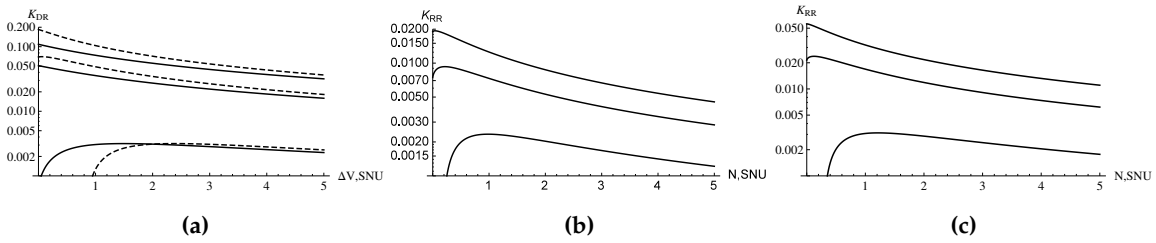

Figure 6. Lower bound on the key rate in the case of collective attacks in a noisy channel on the protocols with arbitrarily-strong modulation $V_M \to \infty$ and perfect post-processing $\beta = 1$. (**a**) Key rate for the DR coherent-state (solid lines) and squeezed-state with $V_S = 0.1$ (dashed lines) CV QKD protocols *versus* preparation noise (in SNU) in the presence of channel noise $\epsilon = 0.2, 0.15, 0.1$ (from bottom to top); the channel transmittance is $\eta = 0.6$; (**b**) key rate for RR coherent-state CV QKD protocol *versus* detection noise (in SNU) in the presence of channel noise $\epsilon = 0.18, 0.15, 0.12$ (from bottom to top); channel transmittance is $\eta = 0.1$; (**c**) key rate for the RR squeezed-state CV QKD protocol with $V_S = 0.1$ *versus* detection noise (in SNU) in the presence of channel noise $\epsilon = 0.4, 0.3, 0.2$ (from bottom to top); channel transmittance is $\eta = 0.1$.

The improvement of the robustness to the channel noise by the preparation noise for DR CV QKD is evident from Figure 7a. When the optimal amount of preparation noise is added, the difference between the coherent- and squeezed-state protocols vanishes. However, the improvement gets less as the channel loss increases.

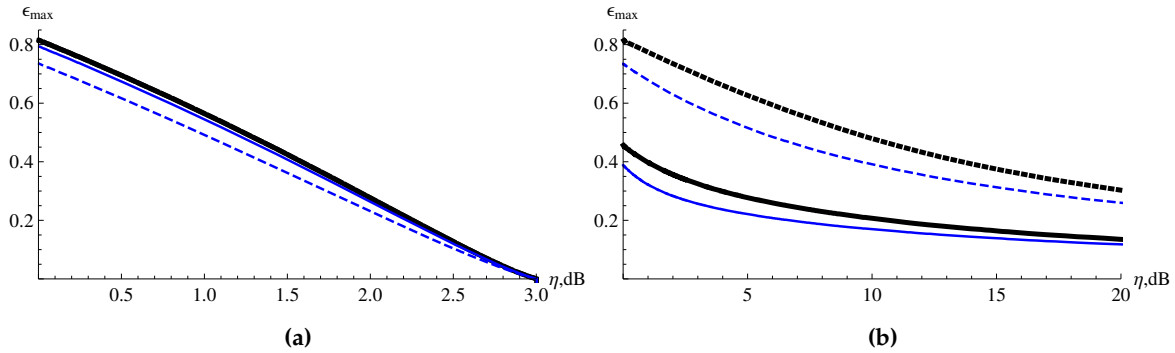

Figure 7. Maximum tolerable channel excess noise *versus* channel transmittance (in dB scale) for the coherent-state (solid lines) and squeezed-state with $V_S = 0.1$ (dashed lines) CV QKD protocols with arbitrarily-strong modulation $V_M \to \infty$ and perfect post-processing $\beta = 1$. (**a**) DR with no preparation noise (regular blue lines) and with optimal preparation noise added (thick black lines, overlapping for squeezed- and coherent-state protocols); (**b**) RR with no preparation noise (regular blue lines) and with optimal detection noise added (thick black lines).

The reason for the improvement is concerned with the fact that the noise, added on the reference side of the protocol (the preparation noise in DR in this case), reduces the Holevo bound. Such noise, in fact, increases the both von Neumann entropies $S(E)$ and $S(E|A)$, but the latter one grows faster, thus contributing to the decrease of χ_{EA}. Therefore, despite the simultaneous decrease of the mutual information I_{AB}, the lower bound on the key rate can be slightly improved and even turned positive by the preparation noise for strong channel noise. This also explains, why in the perfect conditions of noiseless implementation, the coherent-state protocol shows slightly better robustness to the channel noise compared to the squeezed-state protocol, which provides higher mutual information, but also offers more information leakage upon high channel noise. The shot noise of the coherent signal states in this case already reduces the Holevo bound compared to the squeezed signal state.

5.2. Detection Noise and Reverse Reconciliation

Similarly to the previous case, the detection noise can improve the robustness of the RR CV QKD protocols to the channel noise. This effect was already shown for the squeezed-state protocol [103], while here, we generalize it for the arbitrary pure signal states and discuss the mechanism of such an improvement.

First, we show in Figure 6b,c how the key rate can be improved by detection noise in the RR case for both the coherent- and squeezed-state protocols. Similarly to the case of DR and preparation noise, the detection noise decreases the key rate when the channel noise is relatively low, but can optimally improve the key rate and even restore the security of the protocols when the channel noise is close to the threshold. Therefore, the detection noise must be optimized and can shift the bounds on the tolerable channel excess noise, as can be seen in Figure 7b. In this case, however, the squeezed- and coherent-state protocols are both improved in their robustness to noise and do not overlap, *i.e.*, the squeezed-state protocol remains to be more robust against noise, contrary to the DR case. This effect also explains why the RR protocols with the heterodyne detection at Bob's side are more stable against the channel noise, because an additional half SNU added at the detection stage in this case serves as the detection noise, improving the robustness of the protocol. However, typically, more noise must be added to achieve optimal performance in the noisy channels, at least in the asymptotic regime.

The reason for the improvement, similarly to DR and preparation noise, lays in the decrease of the Holevo bound, *i.e.*, of the information leakage. While the von Neumann entropy $S(E)$ remains unchanged by the detection noise, the conditional entropy $S(E|B)$ increases (as Eve becomes effectively decoupled from Bob's data upon the addition of the uncorrelated noise) and χ_{BE} decreases. In particular, for the coherent-state protocol $V_S = 1$, already in the purely-attenuating channel $\epsilon = 0$ the derivative of $S(E|B)$ by N at $N = 0$ in the limit of large modulation $V_M \to \infty$ analytically simplifies to $(1-\eta)/(2\log 2)$, which is always non-negative. Such an increase of $S(E|B)$ improves the key rate when the channel noise is strong enough despite the decrease of the mutual information I_{AB}.

Note that the quantitative improvement of the key rate in the noisy channels is also minor as in the case of DR and preparation noise. Therefore, one could also expect that the positive effect of the detection noise would be canceled by the reduction of the key rate in the finite-size regime [55,56].

6. Combined Trusted Noise Effects on Security

In the previous sections, we described the effects of trusted noise in the idealized DR and RR CV QKD protocols independently. However, the implementation of the protocols is never perfect, other different realistic effects may take place, and the types of trusted noise can be combined, which can amplify the negative and compensate the positive effects described above. Therefore, in the current section, we briefly study how the imperfect post-processing affects the performance of the protocols in the presence of trusted noise and what impact do combined sources of noise have on the security and robustness of the protocols.

6.1. Trusted Noise and Imperfect Post-Processing

First, we confirm the positive effect of the trusted noise on the reference side of the protocols in the regime of limited post-processing efficiency. Therefore, upon the realistic post-processing, the preparation noise in DR and the detection noise in RR (the latter effect previously shown in [121]) still improve the robustness of the protocols to the channel noise when the modulation variance V_M is properly optimized for the given post-processing efficiency β (values discussed above).

On the other hand, the imperfect post-processing leads to a decrease of robustness to the trusted noise on the remote side of the protocols (that is to the detection noise in DR and preparation noise in RR). We illustrate the effect by the plots in Figure 8 (blue lines), where it is evident for both DR and RR protocols that the key rate becomes lower, and the security bound in terms of the noise on the remote side is reduced.

This effect is more significant for RR and is minor in the case of DR protocols, since the post-processing in the DR regime is typically higher, as well as the channel transmittance.

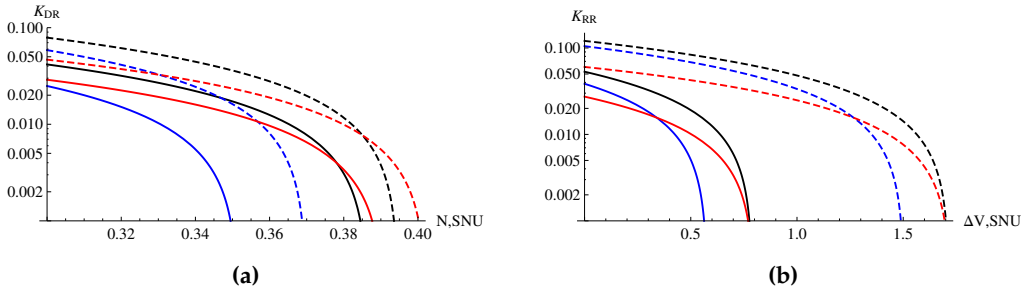

Figure 8. Lower bound on the key rate secure against collective attacks in a noisy channel on the protocols with limited modulation for coherent-state (solid lines) and squeezed-state with $V_S = 0.1$ (dashed lines) CV QKD protocols. (**a**) Key rate for DR *versus* detection noise (in SNU) upon modulation variance $V_M = 20$ in the perfect implementation ($\beta = 1$, $\Delta V = 0$), black lines; upon limited post-processing efficiency ($\beta = 0.99$, $\Delta V = 0$) blue lines; and in the presence of additional preparation noise $\Delta V = 1$ SNU (red lines). Channel transmittance is $\eta = 0.6$, channel noise is 1% SNU. (**b**) Key rate for RR *versus* preparation noise (in SNU) upon modulation variance $V_M = 5$ in the perfect implementation ($\beta = 1$, $N = 0$); black lines, upon limited post-processing efficiency ($\beta = 0.95$, $N = 0$); blue lines; and in the presence of additional detection noise $N = 1$ SNU (red lines). Channel transmittance is $\eta = 0.1$; channel noise is 1% SNU.

6.2. Combination of Preparation and Detection Noise

Finally, we consider the combined effect of the trusted detection and preparation noise on the security of DR and RR CV QKD protocols.

Interestingly, in this regime, the noise added on the reference side of the protocols can improve the robustness to the noise added on the remote side, *i.e.*, the effects similar to "fighting noise with noise" take place, when one type of trusted noise improves the robustness against another.

In the case of DR protocols, the addition of trusted preparation noise slightly improves the robustness to the detection noise (typically in the amount of fractions of a percent of SNU). The mechanism for such an improvement of robustness is similar to using noise on the reference side of the protocol against the channel noise: it leads to the decrease of the Holevo bound due to simultaneous increase of $S(E)$ and $S(E|A)$ entropies in the DR case with the latter one increasing faster. The effect gets less for the lower channel transmittance and upon the imperfect post-processing. This is shown in Figure 8a (red lines): it is evident that the security region in terms of the detection noise is improved when additional preparation noise is present. We also confirm the positive effect of the preparation noise in the DR scheme in the presence of the detection noise, as shown in Figure 9a, where the graphs for the key rate upon the same parameters as in Figure 6 are given in the presence of detection noise $N = 8\%$ SNU (note that the lower graph corresponding to $\epsilon = 0.2$ vanished in the presence of such detection noise).

In the case of RR protocols, the addition of trusted detection can result in improvement of the robustness to the trusted preparation noise, which gets less for the lower channel transmittance. For the low transmittance, the effect is negligible, as we demonstrate in Figure 8b,c (red lines), where the security bounds in terms of the preparation noise are not changed by the presence of the detection noise. At the same time, we confirm the positive role of the detection noise in the presence of the preparation noise, as can be seen from Figure 9b,c, where the key rate is plotted upon the same settings as in Figure 6, but with additional preparation noise $\Delta V = 0.1$. Note that, similarly to the DR case, the lines corresponding to the highest considered channel noise vanished in this case. Nevertheless, the positive effect of the detection noise is evident from the plots. Therefore, the positive role of the

trusted noise at the reference side of the protocols can be still observed in the presence of the trusted noise on the remote side.

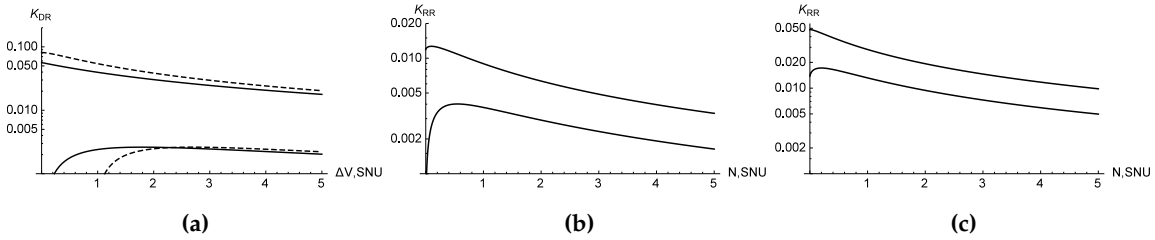

Figure 9. Lower bound on the key rate in the case of collective attacks in a noisy channel on the protocols with arbitrarily-strong modulation $V_M \to \infty$ and perfect post-processing $\beta = 1$. (**a**) Key rate for DR coherent-state (solid lines) and squeezed-state with $V_S = 0.1$ (dashed lines) CV QKD protocols *versus* preparation noise (in SNU) in the presence of channel noise $\epsilon = 0.15, 0.1$ (from bottom to top) and detection noise $N = 8\%$ SNU, channel transmittance is $\eta = 0.6$; (**b**) key rate for RR coherent-state CV QKD protocol *versus* detection noise (in SNU) in the presence of channel noise $\epsilon = 0.12, 0.06$ (from bottom to top) and preparation noise $\Delta V = 0.1$; channel transmittance is $\eta = 0.1$; (**c**) key rate for RR squeezed-state CV QKD protocol with $V_S = 0.1$ *versus* detection noise (in SNU) in the presence of channel noise $\epsilon = 0.25, 0.1$ (from bottom to top) and preparation noise $\Delta V = 0.1$; channel transmittance is $\eta = 0.1$.

7. Summary and Discussion

We have recapitulated the known and shown the previously undisclosed effects of the phase-insensitive trusted preparation and detection noise in CV QKD. In particular, we have shown the overlapping saturation of the positive effect of the trusted preparation noise on the robustness of the DR protocols to the channel noise in the case of coherent and squeezed signal states. We have also shown the negative effect (up to security break in the purely attenuating channels) of the trusted detection noise in the DR scenario. We have confirmed the positive effect of the noise on the reference side of the protocols in the regime of imperfect post-processing. Finally we have shown that the combination of two types of trusted noise has practically no influence (and even slight improvement) on the security bounds on the harmful type of noise. We have discussed the mechanisms of the positive and negative influences of the trusted noise, which mainly concern the impact on the mutual information between the trusted parties, as well as on the quantum entropies, defining the information leakage for an imperfect quantum channel.

We have studied the P & M schemes using the equivalent entanglement-based representation only to analyze the security in the case of the channel excess noise. The research, however, can be extended on the entangled-based protocols, which are promising for possible networking configurations and were recently studied in the alternative topology of entanglement in the middle by Weedbrook [122]. Such protocols were shown feasible on a proof-of-principle level by Su *et al.* [123] without the additional modulation, and by Madsen *et al.* [121] with additional optimal modulation of the entangled states. They were also studied concerning the possible multi-mode effects [124,125], which can affect the security of the CV QKD protocols with bright multimode (macroscopic) states of light [126,127].

Another promising direction of the study of the role of trusted noise in CV QKD is the two-way protocols suggested by Pirandola *et al.* [128], which are aimed at tolerating higher channel noise compared to the one-way CV QKD protocols discussed here. The trusted noise can have an impact on such protocols, and the role of trusted preparation noise on the two-way coherent-state CV QKD was recently discussed by Weedbrook *et al.* [129] and by Wang *et al.* [130], who had shown that the preparation noise tightens the bounds on the key rate, but preserves the advantage in terms of the tolerable channel noise of the two-way protocol over the one-way counterpart.

The physical discussion of the role of trusted preparation and detection noise in CV QKD is relevant not only for existing optical implementation of the protocols. The original motivation of the proposal of the DR CV QKD protocol with a noisy source [107] was to address the possibility of a short distance implementation of the protocol with noisy microwave sources. However, also the homodyne/heterodyne detection of the microwave states is typically noisy, and therefore, our analysis completes the description of the practical specific issues in the possible future implementations of CV QKD with microwave technology, which is rapidly developing [131–133].

Acknowledgments: The research leading to these results has received funding from the EU FP7 under Grant Agreement No. 308803 (Project BRISQ2), co-financed by the Ministry of Education, Youth and Sports of the Czech Republic (7E13032). Vladyslav C. Usenko acknowledges Project No. 13-27533J of the Czech Science Foundation .

Author Contributions: Vladyslav C. Usenko and Radim Filip performed the theoretical calculations, discussed the results, prepared the manuscript, and commented on the manuscript at all stages. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350.
3. Vernam, G.S. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *J. AIEE* **1926**, *45*, 109–115.
4. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
5. Bennett, C.H.; Brassard, G. Quantum cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–19 December 1984.
6. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124.
7. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901.
8. Brendel, J.; Gisin, N.; Tittel, W.; Zbinden, H. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **1999**, *82*, 2594–2597.
9. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504.
10. Einstein, A.; Podolsky, B.; Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **1935**, *47*, 777–780.
11. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663.
12. Bell, J.S. On the Einstein Podolsky Rosen paradox. *Physics* **1964**, *1*, 195–200.
13. Clauser, J.F.; Horne, M.A.; Shimony, A.; Holt, R.A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **1969**, *23*, 880–884.
14. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559.
15. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **2005**, *461*, 207–235.
16. Kraus, B.; Gisin, N.; Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **2005**, *95*, 080501.
17. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New J. Phys.* **2009**, *11*, 085006.
18. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.* **2007**, *3*, 645–649.
19. Christandl, M.; König, R.; Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 020504.
20. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634, doi:10.1038/ncomms1631.

21. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577, doi:10.1103/RevModPhys.77.513.
22. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, doi:10.1103/RevModPhys.84.621.
23. Lorenz, S.; Korolkova, N.; Leuchs, G. Continuous-variable quantum key distribution using polarization encoding and post selection. *Appl. Phys. B* **2004**, *79*, 273–277.
24. Funk, A.; Raymer, M. Quantum key distribution using nonclassical photon-number correlations in macroscopic light pulses. *Phys. Rev. A* **2002**, *65*, 042307.
25. Zhang, Y.; Kasai, K.; Hayasaka, K. Quantum channel using photon number correlated twin beams. *Opt. Express* **2003**, *11*, 3592–3597.
26. Usenko, V.C.; Lev, B.I. Large-alphabet quantum key distribution with two-mode coherently correlated beams. *Phys. Lett. A* **2005**, *348*, 17–23.
27. Usenko, V.C.; Paris, M.G. Multiphoton communication in lossy channels with photon-number entangled states. *Phys. Rev. A* **2007**, *75*, 043812.
28. Usenko, V.C.; Paris, M.G. Quantum communication with photon-number entangled states and realistic photodetection. *Phys. Lett. A* **2010**, *374*, 1342–1345.
29. Ralph, T.C. Continuous variable quantum cryptography. *Phys. Rev. A* **1999**, *61*, 010303.
30. Ralph, T.C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **2000**, *62*, 062306.
31. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **2000**, *61*, 022309.
32. Gottesman, D.; Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Rev. A* **2001**, *63*, 022309.
33. Reid, M.D. Quantum cryptography with a predetermined key, using continuous-variable Einstein–Podolsky–Rosen correlations. *Phys. Rev. A* **2000**, *62*, 062308.
34. Silberhorn, C.; Korolkova, N.; Leuchs, G. Quantum key distribution with bright entangled beams. *Phys. Rev. Lett.* **2002**, *88*, 167902.
35. Cerf, N.J.; Levy, M.; van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311.
36. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902.
37. Silberhorn, C.; Ralph, T.C.; Lütkenhaus, N.; Leuchs, G. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.* **2002**, *89*, 167901.
38. Grosshans, F.; van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241.
39. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504.
40. Usenko, V.C.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *92*, 062337.
41. Grosshans, F.; Cerf, N.J. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Phys. Rev. Lett.* **2004**, *92*, 047905.
42. Navascués, M.; Grosshans, F.; Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.
43. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.
44. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **2006**, *96*, 080502.
45. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504.
46. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503.
47. Renner, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504.
48. Braunstein, S.L.; Kimble, H.J. Teleportation of continuous quantum variables. *Phys. Rev. Lett.* **1998**, *80*, 869–872, doi:10.1103/PhysRevLett.80.869.

49. Chizhov, A.; Knöll, L.; Welsch, D.G. Continuous-variable quantum teleportation through lossy channels. *Phys. Rev. A* **2002**, *65*, 022310.
50. Fiurášek, J. Improving the fidelity of continuous-variable teleportation via local operations. *Phys. Rev. A* **2002**, *66*, 012304.
51. Pirandola, S.; Mancini, S. Quantum teleportation with continuous variables: A survey. *Laser Phys.* **2006**, *16*, 1418–1438.
52. Cerf, N.J.; Iblisdir, S. Optimal *N*-to-*M* cloning of conjugate quantum variables. *Phys. Rev. A* **2000**, *62*, 040301.
53. Braunstein, S.L.; Cerf, N.J.; Iblisdir, S.; van Loock, P.; Massar, S. Optimal cloning of coherent states with a linear amplifier and beam splitters. *Phys. Rev. Lett.* **2001**, *86*, 4938–4941.
54. Fiurášek, J. Optical implementation of continuous-variable quantum cloning machines. *Phys. Rev. Lett.* **2001**, *86*, 4942–4945.
55. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343.
56. Ruppert, L.; Usenko, V.C.; Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **2014**, *90*, 062310.
57. Leverrier, A.; Grangier, P. Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2010**, *81*, 062314.
58. Walk, N.; Ralph, T.C.; Symul, T.; Lam, P.K. Security of continuous-variable quantum cryptography with Gaussian postselection. *Phys. Rev. A* **2013**, *87*, 020303.
59. Fiurášek, J.; Cerf, N.J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302.
60. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502.
61. Furrer, F. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A* **2014**, *90*, 042325.
62. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502.
63. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501.
64. Heid, M.; Lütkenhaus, N. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A* **2006**, *73*, 052316.
65. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; *et al*. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305.
66. Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R.; Grangier, P. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **2009**, *11*, 045023.
67. Leverrier, A.; Alléaume, R.; Boutros, J.; Zémor, G.; Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **2008**, *77*, 042325.
68. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317.
69. Jouguet, P.; Kunz-Jacques, S. High performance error correction for quantum key distribution using polar codes. *Quantum Inf. Comput.* **2014**, *14*, 329–338.
70. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381.
71. Usenko, V.C.; Filip, R. Squeezed-state quantum key distribution upon imperfect reconciliation. *New J. Phys.* **2011**, *13*, 113007.
72. Grosshans, F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 020504.
73. Grosshans, F.; Cerf, N.J.; Wenger, J.; Tualle-Brouri, R.; Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf. Comput.* **2003**, *3*, 535–552.
74. Navascués, M.; Acín, A. Security bounds for continuous variables quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 020505.

75. Heid, M.; Lütkenhaus, N. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Phys. Rev. A* **2007**, *76*, 022313.
76. Blandino, R.; Leverrier, A.; Barbieri, M.; Etesse, J.; Grangier, P.; Tualle-Brouri, R. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2012**, *86*, 012327.
77. Mayers, D.; Yao, A. Quantum Cryptography with Imperfect Apparatus. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS '98), Palo Alto, CA, USA, 8–11 November 1998.
78. Barrett, J.; Hardy, L.; Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **2005**, *95*, 010503.
79. Acín, A.; Gisin, N.; Masanes, L. From Bell's Theorem to Secure Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 120405.
80. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.
81. Gisin, N.; Pironio, S.; Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **2010**, *105*, 070501.
82. Vazirani, U.; Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **2014**, *113*, 140501.
83. Grangier, P.; Potasek, M.; Yurke, B. Probing the phase coherence of parametrically generated photon pairs: A new test of Bell's inequalities. *Phys. Rev. A* **1988**, *38*, 3132.
84. Banaszek, K.; Wódkiewicz, K. Nonlocality of the Einstein–Podolsky–Rosen state in the Wigner representation. *Phys. Rev. A* **1998**, *58*, 4345–4347.
85. Banaszek, K.; Wódkiewicz, K. Testing quantum nonlocality in phase space. *Phys. Rev. Lett.* **1999**, *82*, 2009–2013.
86. Marshall, K.; Weedbrook, C. Device-independent quantum cryptography for continuous variables. *Phys. Rev. A* **2014**, *90*, 042311.
87. Gottesman, D.; Kitaev, A.; Preskill, J. Encoding a qubit in an oscillator. *Phys. Rev. A* **2001**, *64*, 012310.
88. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.
89. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503.
90. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate quantum cryptography in untrusted networks. **2014**, arXiv:1312.4104.
91. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402.
92. Zhang, Y.C.; Li, Z.; Yu, S.; Gu, W.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325.
93. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301.
94. Pirandola, S. Quantum discord as a resource for quantum cryptography. *Sci. Rep.* **2014**, *4*, doi:10.1038/srep06956.
95. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348.
96. Holevo, A.S.; Werner, R.F. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A* **2001**, *63*, 032312.
97. Serafini, A.; Paris, M.G.A.; Illuminati, F.; de Siena, S. Quantifying decoherence in continuous variable systems. *J. Opt. B: Quantum Semiclass. Opt.* **2005**, *7*, doi:10.1088/1464-4266/7/4/R01.
98. Penrose, R. A Generalized Inverse for Matrices. In *Mathematical Proceedings of the Cambridge Philosophical Society*; Cambridge University Press: Cambridge, UK, 1955; pp. 406–413.
99. Serafini, A.; Illuminati, F.; de Siena, S. Symplectic invariants, entropic measures and correlations of Gaussian states. *J. Phys. B* **2004**, *37*, L21–L28.
100. Araki, H.; Lieb, E.H. Entropy Inequalities. In *Inequalities*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 47–57.
101. Lance, A.M.; Symul, T.; Sharma, V.; Weedbrook, C.; Ralph, T.C.; Lam, P.K. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **2005**, *95*, 180503.

102. Usenko, V.C.; Heim, B.; Peuntinger, C.; Wittmann, C.; Marquardt, C.; Leuchs, G.; Filip, R. Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels. *New J. Phys.* **2012**, *14*, 093048.
103. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 130501.
104. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B* **2009**, *42*, 114014.
105. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2008**, *77*, 022310.
106. Usenko, V.C.; Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2010**, *81*, 022318.
107. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501.
108. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **2012**, *86*, 022318.
109. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E.; Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 032309.
110. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329.
111. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309.
112. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304.
113. Kunz-Jacques, S.; Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *91*, 022307.
114. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313.
115. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339.
116. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Zhou, Y.L.; Liang, L.M. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Phys. Rev. A* **2014**, *89*, 032310.
117. Shen, Y.; Peng, X.; Yang, J.; Guo, H. Continuous-variable quantum key distribution with Gaussian source noise. *Phys. Rev. A* **2011**, *83*, 052304.
118. Huang, P.; He, G.Q.; Zeng, G.H. Bound on Noise of Coherent Source for Secure Continuous-Variable Quantum Key Distribution. *Int. J. Theor. Phys.* **2013**, *52*, 1572–1582.
119. Yang, J.; Xu, B.; Guo, H. Source monitoring for continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 042314.
120. Wang, T.; Yu, S.; Zhang, Y.C.; Gu, W.; Guo, H. Improving the maximum transmission distance of continuous-variable quantum key distribution with noisy coherent states using a noiseless amplifier. *Phys. Lett. A* **2014**, *378*, 2808–2812.
121. Madsen, L.S.; Usenko, V.C.; Lassen, M.; Filip, R.; Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **2012**, *3*, doi:10.1038/ncomms2097.
122. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308.
123. Su, X.; Wang, W.; Wang, Y.; Jia, X.; Xie, C.; Peng, K. Continuous variable quantum key distribution based on optical entangled states without signal modulation. *Europhys. Lett.* **2009**, *87*, 20005.
124. Usenko, V.C.; Ruppert, L.; Filip, R. Entanglement-based continuous-variable quantum key distribution with multimode states and detectors. *Phys. Rev. A* **2014**, *90*, 062326.
125. Usenko, V.C.; Ruppert, L.; Filip, R. Quantum communication with macroscopically bright nonclassical states. *Opt. Express* **2015**, *23*, 31534–31543.

126. Peřina, J.; Křepelka, J.; Peřina, J.; Bondani, M.; Allevi, A.; Andreoni, A. Experimental joint signal-idler quasidistributions and photon-number statistics for mesoscopic twin beams. *Phys. Rev. A* **2007**, *76*, 043806.
127. Iskhakov, T.; Chekhova, M.V.; Leuchs, G. Generation and direct detection of broadband mesoscopic polarization-squeezed vacuum. *Phys. Rev. Lett.* **2009**, *102*, 183602.
128. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726–730.
129. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309.
130. Wang, T.; Yu, S.; Zhang, Y.C.; Gu, W.; Guo, H. Security of two-way continuous-variable quantum key distribution with source noise. *J. Phys. B* **2014**, *47*, 215504.
131. Da Silva, M.P.; Bozyigit, D.; Wallraff, A.; Blais, A. Schemes for the observation of photon correlation functions in circuit QED with linear detectors. *Phys. Rev. A* **2010**, *82*, 043804.
132. Bozyigit, D.; Lang, C.; Steffen, L.; Fink, J.; Eichler, C.; Baur, M.; Bianchetti, R.; Leek, P.; Filipp, S.; da Silva, M.; *et al*. Antibunching of microwave-frequency photons observed in correlation measurements using linear detectors. *Nat. Phys.* **2011**, *7*, 154–158.
133. Eichler, C.; Bozyigit, D.; Lang, C.; Baur, M.; Steffen, L.; Fink, J.; Filipp, S.; Wallraff, A. Observation of two-mode squeezing in the microwave frequency domain. *Phys. Rev. Lett.* **2011**, *107*, 113601.