# Simple and loss-tolerant free-space quantum key distribution using a squeezed laser

Nedasadat Hosseinidehaj,* Matthew S. Winnel, and Timothy C. Ralph
*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Received 23 July 2021; accepted 14 February 2022; published 4 March 2022)

We consider a continuous-variable (CV) quantum key distribution (QKD) protocol over free-space channels, which is simpler and more robust than typical CV QKD protocols. It uses a bright laser, squeezed and modulated in the amplitude quadrature, and self-homodyne detection. We consider a scenario, where the line of sight is classically monitored to detect active eavesdroppers, so that we can assume a passive eavesdropper. Under this assumption, we analyze security of the QKD protocol in the composable finite-size regime. Proper modulation of the squeezed laser to the shot-noise level can completely eliminate information leakage to the eavesdropper and also eliminate the turbulence-induced noise of the channel in the amplitude quadrature. Under these conditions, estimation of the eavesdropper's information is no longer required. The protocol is extremely robust to modulation noise and highly loss-tolerant, which makes it a promising candidate for satellite-based continuous-variable quantum communication.

DOI: 10.1103/PhysRevA.105.032602

## I. INTRODUCTION

Current wireless communication systems are omnidirectional and so are easy to eavesdrop upon [see Fig. 1(a)]. Public-key cryptography can be used to secure such transmissions, offering security via assumptions about the computational power of malicious eavesdroppers. These assumptions are called into question by possible future advances in computational power, in particular the advent of large-scale quantum computation [1]. Given this, the security of current communications cannot be guaranteed indefinitely as they might be stored and decrypted in the future when the required level of quantum processing becomes available. Laser communications (lasercomm) can improve security in certain circumstances via its greater directionality. Nevertheless eavesdropping is still possible due to beam diffraction [see Fig. 1(b)]. Here we propose a simple extension to lasercomm using techniques from quantum key distribution [2,3] and recent observations about information leakage [4], which eliminates these eavesdroppers [see Fig. 1(c)].

Quantum key distribution (QKD) allows two trusted parties, Alice and Bob, to share a secure key, unknown to a potential eavesdropper, Eve. In contrast to current classical cryptography, QKD provides information-theoretic security [2,3,5]. Although QKD started with discrete-variable quantum systems [6,7], it has been extended to continuous-variable (CV) systems [8–11]. In the former, information is encoded in discrete degrees of freedom of a single photon, with the detection realized by single-photon detectors. While, in the latter, information is encoded in continuous degrees of freedom of light, and detection is realized by off-the-shelf homodyne detectors, offering greater compatibility with current optical telecommunication networks.

In a typical lasercomm protocol information is encoded via amplitude modulation of the laser beam and read out via direct detection, also known as self-homodyne. Similarly, in this work we propose a CV QKD protocol based on amplitude modulation of a *squeezed* laser with read out also via direct detection. In contrast, in a typical CV QKD protocol information is encoded in both amplitude and phase quadratures of the light while the detection is performed by either homodyne or heterodyne detectors, requiring the use of a separate local oscillator [3,12–14]. Our simplification comes by specifically considering free-space channels and hence limiting the eavesdropper to only gathering the lost light, i.e., a passive attack. While this is not the most general attack, we argue it is a reasonable restriction given plausible technical capabilities of Eve. Given this restriction we make a full, composable finite-key security analysis of our system and find it is robust to loss, turbulence and excess noise of the source laser.

Free-space channels are flexible in terms of infrastructure establishment and feasibility of communication with moving objects. They also provide the possibility of long-distance quantum communication via orbiting satellites. The key disadvantage of free-space quantum communications is, however, atmospheric attenuation and turbulence noise [15–17]. Atmospheric turbulence causes a random variation of channel transmissivity in time [18–22]. This transmissivity fluctuation introduces extra noise on CV QKD systems, which reduces the secret key rate, and even renders the communication insecure in the presence of strong turbulence [23–33]. It is thus of considerable significance that reasonable restrictions on Eve can lead to a far simpler and more robust system.

## II. THE MODEL

We analyze a CV QKD protocol using a squeezed laser over a free-space channel using modulation in only the amplitude quadrature and direct, self-homodyne detection [see

*nedahsn@gmail.com

 

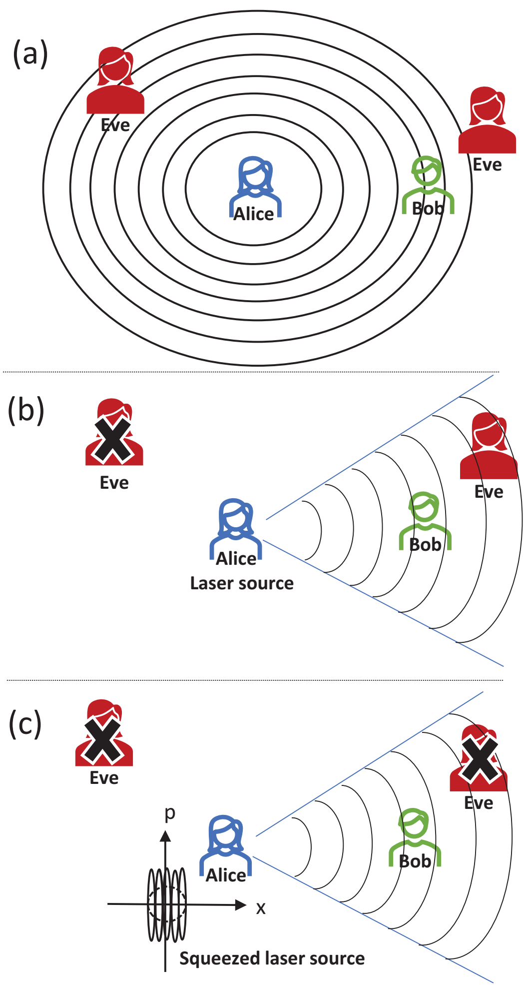


FIG. 1. A schematic representation of communication scenarios between Alice and Bob in the presence of an eavesdropper, Eve: (a) current wireless communication, which is only secure given computational limitations of Eve; (b) communication using laser-comm; and (c) the QKD protocol we consider in this paper using a squeezed laser, which can completely eliminate information leakage to Eve.

Fig. 1(c)]. A proper modulation of the squeezed states leads to zero turbulence-induced noise of the free-space channel in the amplitude quadrature as well as zero information leakage to the eavesdropper. The protocol does not require estimation of the eavesdropper's information, as information leakage is zero. It is also highly robust against modulation imperfections (i.e., modulation noise) and can tolerate high values of channel loss.

First, in our QKD protocol we assume the trusted parties, Alice and Bob, are able to classically monitor the line of sight, so that any active presence of an eavesdropper (Eve) in the line of sight can be detected, and if there is any, the protocol will be aborted. While an omnipotent eavesdropper might deceive Alice and Bob, the technologies required seem well beyond current capabilities. As a result, any active eavesdropping attacks in the line of sight will be prevented, and Eve will be limited to only passive attacks.

Second, in our QKD protocol we will exploit squeezed quantum states for information carriers, similar to the CV protocol of [4], where by properly encoding information into a Gaussian modulation of squeezed states (squeezed in a single quadrature and modulated in the squeezing direction), one can completely and deterministically eliminate information leakage to Eve in a reverse reconciliation (RR) scenario [11], if the channel is pure loss. The necessary condition for leakage elimination is that the variance of the average input state in the modulation direction has to be the shot-noise variance. Unlike [4], we consider bright squeezed states such that the modulation can be read out via direct detection of the light.

Since a pure-loss channel can be considered as a passive eavesdropping attack, by the Gaussian modulation of the squeezed laser to the shot-noise level and limiting Eve to only passive attacks, we will completely and deterministically eliminate information leakage to Eve in a RR scenario (i.e., obtain zero Holevo information) over free-space channels. As a result, estimation (or upper bounding) of Eve's information is no longer required in this protocol. Such a shot-noise modulation can also eliminate the channel-fluctuation noise in the information-carrying quadrature.

Because the protocol uses squeezed bright beams, where the information is only encoded in the amplitude quadrature, self-homodyne detection at Bob's station with no need for a separate local oscillator will suffice to measure the amplitude quadrature. This will significantly simplify the experimental realization of the protocol.

We further investigate the effect of modulation imperfections. We consider the case where the variance of the average input state in the squeezing direction is not exactly the shot noise. In fact, we consider some amount of trusted preparation noise on top of the shot noise on Alice's side. We show that this type of practical imperfection leads to some information leakage to Eve, where we do the security analysis in the composable finite-size regime. However, the amount of leakage is sufficiently small, so that its effect on the secret key rate is negligible.

## III. GAUSSIAN-MODULATION SQUEEZED-STATE PROTOCOL

In a prepare-and-measure scheme, Alice generates a random real variable $a_q$, drawn from a Gaussian distribution of variance $V_{\rm sig}$ and zero mean. Alice prepares bright squeezed states with the squeezing in the amplitude $\hat{q}$ quadrature, where the variance of the squeezed quadrature is $V_{\rm sqz}$. The squeezed states are then modulated (displaced) by an amount $a_q$ in the direction of the $\hat{q}$ quadrature. The variance of the average Gaussian state after the modulator is $V_{\rm sqz} + V_{\rm sig}$ in the amplitude $\hat{q}$ quadrature and $1/V_{\rm sqz}$ in the phase $\hat{p}$ quadrature. We consider the case where the variance of the squeezed quadrature after the modulation is equal to the shot-noise variance, i.e., $V_{\rm sqz} + V_{\rm sig} = 1$ [4]. The squeezed states are then sent through a free-space channel to Bob, who directly measures the amplitude $\hat{q}$ quadrature with self-homodyne detection.

Note that in [4], in the preparation step on Alice's side, an ensemble of coherent states (modulated in only amplitude quadrature) is prepared. The ensemble is squeezed by injecting it into an optical parametric oscillator (OPO). The resulting ensemble of squeezed coherent states is sent through the quantum channel to Bob, who measures the channel output via homodyne detection using a local oscillator from the source laser.

With respect to the proposed experimental realization, we consider that Alice sends bright amplitude squeezed states. These might be produced by a squeezed laser, for example, a pumped noise-reduced semiconductor laser [34], which directly generates amplitude squeezed states. In addition, unlike [4], which uses a separate local oscillator for the homodyne detection, modulation of the squeezed amplitude can be read out via direct detection of the light, known as self-homodyne detection, with no need for a separate local oscillator.

With respect to the security analysis, Ref. [4] investigates the asymptotic regime, and calculates only Eve's information (i.e., Holevo bound and not the secret key rate) for an optical fiber with fixed transmissivity. In our work, however, we make a full, composable finite-size security analysis of the CV QKD system for a free-space channel with fluctuating transmissivity under the assumption of a passive attack. Recall that limiting the eavesdropper to passive attacks is justified by assuming Alice and Bob monitor the quantum channel for Eve's presence in a free-space channel. Further, we also investigate the impact deviation from the shot-noise modulation can have on the security of the protocol.

In contrast to a fiber link with a fixed transmissivity, the transmissivity, $\eta$, of a free-space channel fluctuates in time due to atmospheric turbulence. Such fading channels can be characterized by a probability distribution $p(\eta)$ [18–22]. A fading channel can be decomposed into a set of subchannels, for which the transmissivity is relatively stable. Each subchannel $\eta_i$ occurs with probability $p_i$ so that $\sum_i p_i = 1$ or $\int_0^{\eta_{\max}} p(\eta)\, d\eta = 1$ for a continuous probability distribution, where $\eta_{\max}$ is the maximum realisable transmissivity.

In order to analyze the security of the CV QKD protocol, we consider the equivalent entanglement-based scheme. Alice first prepares a symmetric two-mode squeezed vacuum state of quadrature variance $V$. One mode is kept by Alice (to be later measured via homodyne detection in the $\hat{q}$ quadrature), while the second mode is squeezed (on Alice's side) in the $\hat{q}$ quadrature with the squeezing parameter $r_e$. The initial entangled state, prepared on Alice's side, is given by the following covariance matrix:

$$\mathbf{M}_{\mathrm{AB}_0} = \begin{bmatrix} a_q & 0 & c_q & 0 \\ 0 & a_p & 0 & c_p \\ c_q & 0 & b_q & 0 \\ 0 & c_p & 0 & b_p \end{bmatrix}, \begin{cases} a_q = a_p = V, \\ b_q = Ve^{-2r_e}, b_p = Ve^{2r_e}, \\ c_q = e^{-r_e}\sqrt{V^2-1}, \\ c_p = -e^{r_e}\sqrt{V^2-1}. \end{cases} \tag{1}$$

Note that in order for the prepare-and-measure scheme to be equivalent with the entanglement-based scheme we need to have $V_{\mathrm{sqz}} + V_{\mathrm{sig}} = Ve^{-2r_e}$ and $1/V_{\mathrm{sqz}} = Ve^{2r_e}$.

### A. Eavesdropping assumptions

The security of CV QKD protocols is typically analyzed by assuming that a potential eavesdropper, Eve, can carry out all physically allowed operations, an assumption which grants capabilities far in excess of present technology. In our work, under the realistic assumption of Alice and Bob monitoring the line of sight, we remove the unrealistic assumption of Eve making an active attack in the line of sight without being seen. Given this restriction we make a full, composable finite-size security analysis of our system.

We assume Alice and Bob classically monitor the line of sight during the quantum communication from both directions. For Eve to make any active attacks (for instance, a quantum nondemolition (QND) or an entangling cloner attack.[1] [35]) over the line of sight, she is required to be actively present in the line of sight. Therefore, Alice and Bob will be able to detect Eve's active presence and abort the protocol. Note that we do not claim that performing an active attack is impossible for Eve. Instead, we claim that making such an attack, so that Eve can remain invisible to Alice and Bob, is an extreme technical challenge for Eve, and considered unrealistic given horizon technology.

Alternatively, Eve could perform a shine-on attack, by using an entangled state and passively adding extra noise onto Bob's detector. Again, this attack will be very challenging for Eve in a self-homodyne detection scenario with the phase of the local oscillator being random and also the line-of-sight being monitored. However, even if Eve can invisibly add extra noise, it will be identified by Alice and Bob in unexpected deviations from shot noise at Bob's station and when they estimate a signal-to-noise ratio (SNR) lower than that they expect from the light-collection attack. Thus, with no reduction in practical security, Eve's attack over free-space channels can be restricted to a passive attack, which is the same as a beam-splitter attack. In a passive collective attack, Eve collects the light lost in the transmission, and stores the quantum states in her quantum memory to be collectively measured later.

## IV. FINITE-SIZE SECURITY ANALYSIS

The Wigner function of Alice and Bob's ensemble-average state (over all subchannels) at the output of a free-space channel with fluctuating transmissivity $\eta$ is the sum of the Wigner functions of the states after individual subchannels weighted by subchannel probabilities [33]. Alice and Bob's state is Gaussian after the realization of each subchannel; however, Alice and Bob's ensemble-average state is a non-Gaussian mixture of Gaussian states obtained from individual subchannels.

In an RR scenario, Eve's information, upper bounded by the Holevo information in a collective attack, is given by $\chi(b{:}E) = \mathcal{S}(\rho_E) - \mathcal{S}(\rho_{E|b})$, where $\mathcal{S}(\rho)$ is the von Neumann entropy of the quantum state $\rho$. The security is analyzed based on the purification assumption, i.e., the assumption that Alice and Bob's quantum state $\rho_{AB}$ is purified by Eve's quantum state $\rho_E$. This results in $\mathcal{S}(\rho_E) = \mathcal{S}(\rho_{AB})$, and $\mathcal{S}(\rho_{E|b}) = \mathcal{S}(\rho_{A|b})$. Thus, Eve's Holevo information is given by $\chi(b{:}E) = \mathcal{S}(\rho_{AB}) - \mathcal{S}(\rho_{A|b})$. Note that $\rho_{AB}$ is non-Gaussian for a free-space channel however, according to the

[1] In addition to entangling cloner attack, modulation of only amplitude quadrature can provide Eve with the possibility of an active intercept and resend attack. However, such an attack needs an active presence of Eve in the line of sight, which will be prevented under the assumption of Alice and Bob monitoring the line of sight.

optimality of Gaussian attacks [36–38], $\chi(b{:}E)$ can be maximized if calculated based on the covariance matrix of $\rho_{AB}$. The covariance matrix of Alice and Bob's ensemble-average state is given by

$$\mathbf{M}_{AB} = \begin{bmatrix} a_q & 0 & c'_q & 0 \\ 0 & a_p & 0 & c'_p \\ c'_q & 0 & b'_q & 0 \\ 0 & c'_p & 0 & b'_p \end{bmatrix}, \text{ where}$$
$$b'_q = \eta_f b_q + 1 - \eta_f + \mathrm{Var}(\sqrt{\eta})(b_q - 1)$$
$$b'_p = \eta_f b_p + 1 - \eta_f + \mathrm{Var}(\sqrt{\eta})(b_p - 1)$$
$$c'_q = \sqrt{\eta_f}\, c_q, \quad c'_p = \sqrt{\eta_f}\, c_p, \text{ where}$$
$$\eta_f = \langle\sqrt{\eta}\rangle^2, \quad \mathrm{Var}(\sqrt{\eta}) = \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2, \tag{2}$$

where $\langle\eta\rangle = \int_0^{\eta_{\max}} \eta p(\eta)\, d\eta$, and $\langle\sqrt{\eta}\rangle = \int_0^{\eta_{\max}} \sqrt{\eta} p(\eta)\, d\eta$. Thus, Eve's effective passive attack can be considered as a beam-splitter attack with the beam-splitter transmissivity $\eta_f$.

According to Eq. (2), a fading channel is equivalent with a fixed-transmissivity channel with transmissivity $\eta_f$ and an extra non-Gaussian noise of $\mathrm{Var}(\sqrt{\eta})(b_{q(p)} - 1)$ [24,32,33]. This noise depends on the channel fluctuation variance $\mathrm{Var}(\sqrt{\eta})$ and the input variance to the channel $b_{q(p)}$. When Eve's attack is considered passive, it means that the channel fluctuation is not under Eve's control. This means that the fluctuation noise $\mathrm{Var}(\sqrt{\eta})(b_{q(p)} - 1)$ is not accessible to Eve for the purification, and hence the fluctuation noise should be considered as a trusted noise on Bob's side. On the other hand, having a trusted noise on Bob's side in a RR scenario decreases Eve's information [39]. Hence, in calculating Eve's information from the passive attack we consider the (trusted) fluctuation noise to be zero as this can only overestimate Eve's information.

Note that we can also use Eve and Bob's covariance matrix to calculate Eve's Holevo information from the passive attack, and obtain the same result as that from the purification assumption as discussed above (see Appendix A for more details on the purification assumption). As a result of Eve's passive attack, the covariance matrix of Eve's ensemble-average state is given by

$$\mathbf{M}_E = \begin{bmatrix} (1-\eta_f)b_q+\eta_f & 0 \\ 0 & (1-\eta_f)b_p+\eta_f \end{bmatrix}. \tag{3}$$

The covariance matrix of Eve's system conditioned on Bob's homodyne detection (with efficiency $\eta_B$ and electronic noise $\nu_B$) is given by $\mathbf{M}_{E|B'}=\mathbf{M}_E-\mathbf{M}_{EB'}(\mathbf{X}\mathbf{M}_{B'}\mathbf{X})^{\mathrm{MP}}\mathbf{M}_{EB'}^T$, where $\mathbf{X} = \mathrm{diag}(1, 0)$, MP stands for the Moore-Penrose pseudoinverse of a matrix, and we have

$$\mathbf{M}_{B'} = \mathrm{diag}(V_{Bq}, V_{Bp}), \text{ where}$$
$$V_{Bq} = \eta_B[\eta_f b_q+1-\eta_f]+(1-\eta_B)\upsilon,$$
$$V_{Bp} = \eta_B[\eta_f b_p+1-\eta_f]+(1-\eta_B)\upsilon, \text{ where}$$
$$\upsilon = 1 + \frac{\nu_B}{1-\eta_B}, \text{ and}$$
$$\mathbf{M}_{EB'} = \mathrm{diag}(C_{EBq}, C_{EBp}), \text{ where}$$
$$C_{EBq} = \sqrt{\eta_B}\sqrt{\eta_f(1-\eta_f)}[1-b_q],$$
$$C_{EBp} = \sqrt{\eta_B}\sqrt{\eta_f(1-\eta_f)}[1-b_p]. \tag{4}$$

Note that in reality for Bob's quadrature variance (after the detection) we have $V_{Bq} = \eta_B b'_q+(1-\eta_B)\upsilon$ and $V_{Bp} = \eta_B b'_p+(1-\eta_B)\upsilon$. But, since as noted earlier, the (trusted) fluctuation noise $\mathrm{Var}(\sqrt{\eta})(b_{q(p)} - 1)$ on Bob's side decreases Eve's information, we assume the fluctuation noise is zero in $V_{Bq}$ and $V_{Bp}$ of Eq. (4) for the security analysis.

According to the protocol, Alice has to make sure that the beam leaving her laboratory in the prepare-and-measure scheme has exactly the shot-noise variance in the $\hat{q}$ quadrature. It means that the beam leaving Alice's laboratory in the entanglement-based scheme also needs to have the shot-noise variance in the $\hat{q}$ quadrature, i.e., $b_q = 1$. As a result, according to $\mathbf{M}_{EB}$ in Eq. (4), there is no correlation between Eve and Bob in the $\hat{q}$ quadrature ($C_{EBq} = 0$), i.e, the quadrature that contains the key information. Hence, there is no information leakage to Eve during the quantum communication part in a RR scenario, i.e., we have the Holevo information $\chi(b{:}E) = \mathcal{S}(\mathbf{M}_E)-\mathcal{S}(\mathbf{M}_{E|B'}) = 0$.

The shot-noise modulation in the $\hat{q}$ quadrature has another advantage of eliminating the fluctuation-induced noise of a free-space channel. Bob's variance in the $\hat{q}$ quadrature (before the detection) is given by $b'_q=\eta_f b_q + 1 - \eta_f + \mathrm{Var}(\sqrt{\eta})(b_q - 1)$. When we have $b_q = 1$, the fluctuation-induced noise of the channel in the $\hat{q}$ quadrature, i.e., $\mathrm{Var}(\sqrt{\eta})(b_q - 1)$, will become zero, and Bob's variance will also be the shot noise, $b'_q=1$.

Since having $b_q = 1$ results in no information leakage to Eve during the quantum communication, i.e., $\chi(b{:}E)=0$, we do not need to estimate (or upper bound) Eve's information. However, the transmissivity of the channel needs to be estimated in order to estimate the SNR of the channel, which will be used to choose the most efficient error-correcting code rate for the error-correction step. This means we are still required to reveal a subset of data for SNR estimation.

Note that in this protocol, $\chi(b{:}E) = 0$ does not mean that Eve and Bob's quantum systems are not correlated because Eve and Bob still remain correlated in the phase $\hat{p}$ quadrature ($C_{EBp} \neq 0$). However, this correlation is irrelevant to the security of the protocol because the key information is only encoded in the $\hat{q}$ quadrature. In fact, $\chi(b{:}E) = 0$ means that Bob's measurement outcomes are uncorrelated with Eve's quantum system $E$ before the error correction. However, in the error-correction procedure, classical information $C$ of size $l_{\mathrm{EC}}$ (i.e., the size of the syndrome of Bob's string sent to Alice in a RR scenario) will be revealed by the trusted parties. In the privacy amplification step, Alice and Bob have to discard the leakage during the error correction.

Based on the leftover hash lemma [40,41], the number of approximately secure bits, $\ell$, that can be extracted from the raw key should be slightly smaller than the smooth min-entropy of Bob's string $b$ conditioned on Eve's system $E'$ (which characterizes Eve's quantum state $E$, as well as the public classical variable $C$ leaked during the QKD protocol), denoted by $H_{\min}^{\epsilon_{\mathrm{sm}}}(b^{N'}|E')$ [40], i.e., we have $\ell \leqslant H_{\min}^{\epsilon_{\mathrm{sm}}}(b^{N'}|E')-2\log_2(\frac{1}{2\bar{\epsilon}})$, where $\bar{\epsilon}$ comes from the leftover hash lemma. Note that $N'$ indicates the length of Bob's string $b$ after the SNR estimation. The chain rule for the smooth min-entropy [42] gives $H_{\min}^{\epsilon_{\mathrm{sm}}}(b^{N'}|E') = H_{\min}^{\epsilon_{\mathrm{sm}}}(b^{N'}|EC) \geqslant H_{\min}^{\epsilon_{\mathrm{sm}}}(b^{N'}|E) - \log_2|C|$, where $\log_2|C| = l_{\mathrm{EC}}$, with $l_{\mathrm{EC}}$ the size of data leakage during the error correction, which can be given by $l_{\rm EC}=N'[H(b)-\beta I(a{:}b)]$ [42–44], where $H(b)$ is Bob's Shannon entropy and $\beta$ is the reconciliation efficiency. In order to calculate the length $\ell$ of the final key which is $\epsilon$-secure ($\epsilon{=}2\epsilon_{\rm sm}{+}\bar{\epsilon}{+}\epsilon_{\rm PE}{+}\epsilon_{\rm cor}$ [42,43]), the conditional smooth min-entropy $H^{\epsilon_{\rm sm}}_{\rm min}(b^{N'}|E)$ has to be lower bounded when the protocol did not abort. Under the assumption of independent and identically distributed attacks such as collective or individual attacks, the asymptotic equipartition property [42,45,46] can be utilized to lower bound the conditional smooth min-entropy with the conditional von Neumann entropy. Explicitly, we have $H^{\epsilon_{\rm sm}}_{\rm min}(b^{N'}|E)\geqslant N'\mathcal{S}(b|E)-\sqrt{N'}\Delta_{\rm AEP}$ [42,43], where $\Delta_{\rm AEP}=(d{+}1)^2{+}4(d{+}1)\sqrt{\log_2(2/\epsilon^2_{\rm sm})}+2\log_2[2/(\epsilon^2\epsilon_{\rm sm})]{+}4\epsilon_{\rm sm}d/(\epsilon\sqrt{N'})$ with $d$ the discretization parameter, and $\mathcal{S}(b|E)$ the conditional von Neumann entropy, which is given by $\mathcal{S}(b|E)=H(b)-H^{\epsilon_{\rm PE}}(b{:}E)$. Eve's information $H^{\epsilon_{\rm PE}}(b{:}E)$ from a collective (an individual) attack on Bob's string $b$ is upper bounded by Holevo information $\chi^{\epsilon_{\rm PE}}(b{:}E)$ (mutual information between Eve and Bob $I^{\epsilon_{\rm PE}}(b{:}E)$), except with probability $\epsilon_{\rm PE}$. Recall again that having $b_q=1$, we do not need to estimate $\chi^{\epsilon_{\rm PE}}(b{:}E)$, as it is exactly zero. Therefore, the secret key length is given by $\ell{=}N'\beta I(a{:}b){-}\sqrt{N'}\Delta_{\rm AEP}{-}2\log_2(\frac{1}{2\bar{\epsilon}})$, and the secret key rate is given by $K=\ell/N$. Note that the mutual information is given by $I(a{:}b)=\frac{1}{2}\log_2\frac{a_q}{a_q-[\eta_B c_q'^2]/[\eta_B b_q'+(1-\eta_B)\upsilon]}$.

### A. Modulation noise

Now we investigate the discrepancies between the ideal protocol and its practical implementations in terms of the modulation. We consider the case where the prepared state on Alice's side does not have the exact shot-noise variance in the modulation direction. More precisely, we assume some preparation noise $\xi$ on Alice's side, which is assumed to be trusted in the case of a passive eavesdropper. For the aim of numerical simulation, we assume $b_q=1$ and $\xi=0.02$. Eve's information can still be calculated using Eve and Bob's covariance matrices in Eqs. (3) and (4), where the term $b_{q(p)}$ in Eqs. (3) and (4) should now be replaced by $b_{q(p)}+\xi$. In this nonideal modulation case, we have $C_{EBq}\neq 0$ in Eq. (4) due to $b_q+\xi>1$, which means the preparation noise on top of the shot noise leads to information leakage [i.e., $\chi^{\epsilon_{\rm PE}}(b{:}E)\neq 0$], and the secret key length for collective attacks is given by $\ell{=}N'\beta I(a{:}b){-}N'\chi^{\epsilon_{\rm PE}}(b{:}E){-}\sqrt{N'}\Delta_{\rm AEP}{-}2\log_2(\frac{1}{2\bar{\epsilon}})$. Note that in the presence of modulation noise, Eve's information can also be calculated from the purification assumption, i.e., using Alice and Bob's covariance matrix while assuming the (trusted) fluctuation noise is zero (see Appendix A).

In Fig. 2 the finite-size key rate of the squeezed-state protocol is shown as a function of channel loss under the assumption of passive collective attacks. For the sake of comparison, we also show the finite-size key rate of a CV QKD protocol using coherent states, under the assumption of passive attacks. Similar to the squeezed-state protocol, it uses Gaussian modulation in only the amplitude quadrature, and direct detection of the amplitude quadrature [47]. For this protocol, the Holevo information can still be calculated using

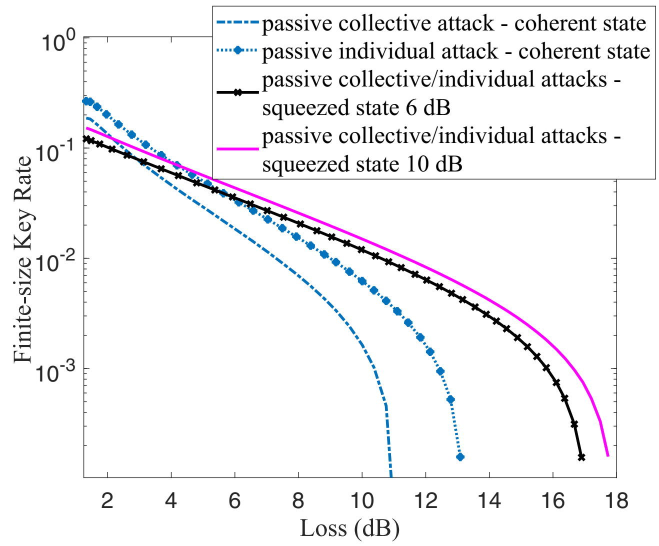


FIG. 2. Finite-size key rate as a function of channel loss (dB), where $\text{Loss(dB)}=-10\log_{10}\eta_f$, for the coherent-state protocol and the squeezed-state protocol secure against passive individual and collective attacks, with 6 dB and 10 dB squeezing, where $\text{Squeezing(dB)}=-10\log_{10}V_{\rm sqz}$. The numerical values for the finite-size regime are the security parameter $\epsilon=10^{-9}$ and the discretization parameter $d=5$. The other parameters are Bob's detector efficiency $\eta_B=0.61$, electronic noise $\nu_B=0.12$, reconciliation efficiency $\beta=0.98$, and excess noise $\xi=0.02$ (note that in a passive attack this noise is assumed to be a trusted preparation noise). The block size is chosen to be $N=10^{10}$, half of which is used in total for the parameter estimation. The modulation variance in the coherent-state protocol is optimized to maximise the key rate. We consider a probability distribution for the free-space channel given by the elliptic-beam model [20], where the model parameters have been chosen according to [33].

the same method as discussed for the squeezed-state protocol, where now we should set $r_e=-\ln(\sqrt{V})$ and $V_{\rm sqz}=1$. As can be seen from Fig. 2, for losses above 4 dB, the squeezed-state protocol outperforms the coherent-state protocol under the assumption of passive collective attacks. The squeezed-state protocol can achieve reasonable key rates for losses more than 4 times that of the coherent-state protocol.

Note that for both the squeezed-state and coherent-state protocols, (passive) Eve's information from an individual attack can be upper bounded using the classical mutual information between Eve and Bob $I^{\epsilon_{\rm PE}}(b{:}E)$ (except with probability $\epsilon_{\rm PE}$), where $I(b{:}E)=\frac{1}{2}\log_2\frac{V_{Bq}}{V_{Bq}-C^2_{EBq}/[(1-\eta_f)b_q+\eta_f]}$, where $r_e$ and $V_{\rm sqz}$ should be set differently for each protocol as mentioned earlier. Note that for the squeezed-state protocol, Eve's individual information is only slightly less than the Holevo information, so that the finite-size key rate for passive individual attacks is almost the same as the key rate for passive collective attacks. According to Fig. 2, for losses above 6 dB, the squeezed-state protocol outperforms the coherent-state protocol under the assumption of passive individual attacks. Further, while the coherent-state protocol is not secure for losses above 13 dB, the squeezed-state protocol can achieve reasonable key rates for losses up to 18 dB.

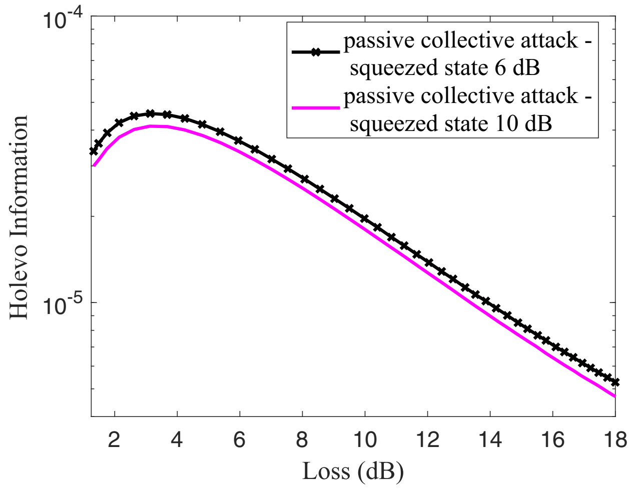


FIG. 3. Holevo information $\chi^{\epsilon_{\mathrm{PE}}}(b{:}E)$ resulting from the passive collective attack as a function of channel loss (dB) for the nonideal squeezed-state protocol with preparation noise $\xi$ (on top of the shot-noise variance) for 6 dB and 10 dB squeezing. The other parameters are the same as Fig. 2.

Note that the amount of modulation, $V_{\mathrm{sig}}$, is related to the amount of squeezing, $V_{\mathrm{sqz}}$, because the variance of the amplitude quadrature after the modulation has to be equal to the shot-noise variance, $V_{\mathrm{sqz}} + V_{\mathrm{sig}} = 1$. In fact, the more squeezing (lower $V_{\mathrm{sqz}}$), the higher modulation we can use (higher $V_{\mathrm{sig}}$), which means a larger number of squeezed states can be modulated within the shot-noise variance (more information can be encoded).

As can be seen from Fig. 3, showing Holevo information $\chi^{\epsilon_{\mathrm{PE}}}(b{:}E)$ as a function of channel loss for the squeezed-state protocol of Fig. 2, the amount of leakage due to the preparation noise is sufficiently small such that it only has a negligible effect on the secret key rate shown in Fig. 2. For instance, even for a large preparation noise of $\xi = 0.02$, we have $\chi^{\epsilon_{\mathrm{PE}}}(b{:}E) < 5 \times 10^{-5}$ for the given values of squeezing (very small compared to the secret key rate shown in Fig. 2). Also, Fig. 3 shows that Eve's information is maximized for the channel loss of around 3 dB and then reduced with increasing loss. Note that in the case of modulation noise, where there is some information leakage to Eve, parameter estimation of channel transmissivity and preparation noise is required to upper bound Eve's information $\chi^{\epsilon_{\mathrm{PE}}}(b{:}E)$ (see Appendix B for more details). Note that the squeezed-state protocol is very robust to error bars of estimators, such that the difference between $\chi^{\epsilon_{\mathrm{PE}}}(b{:}E)$ (i.e., Holevo information considering the error bars due to the finite-size effects) and Holevo information given the perfect estimation of channel parameters (i.e, the asymptotic case) is negligible. Note that this is not the case for the coherent-state protocol shown in Fig. 2.

## V. CONCLUSIONS

We performed composable finite-size security analysis for a CV QKD protocol using an amplitude squeezed laser for free-space channels. Amplitude squeezing can be produced by compact semiconductor lasers [34]. The information is encoded into the amplitude quadrature such that the Gaussian-modulated beam has the shot-noise variance, and detection is performed by the self-homodyne detection of the amplitude quadrature. Under the realistic assumption of classical monitoring of the line of sight, we limited the eavesdropper (Eve) to only passive attacks, where she can only collect the light lost in the communication. Under such an assumption, the shot-noise modulation eliminates information leakage to Eve (and also eliminates the channel-fluctuation noise in the amplitude quadrature). As a result, the parameter estimation of Eve's information is no longer required. We investigated nonideal modulation with some extra noise on top of the shot noise, which results in sufficiently small information leakage having negligible effect on the finite key rate. The protocol is highly robust to modulation noise, and can tolerate high values of channel loss. While our analysis shows the effectiveness of the protocol for losses up to 18 dB (given practical squeezing) for the block size of $10^{10}$, the performance can be improved by increasing the block size. For instance, for the block size of $10^{11}$, the protocol can tolerate losses up to 23 dB, expected in downlink channels from low-earth-orbit satellites. While our analysis focuses on Gaussian modulation, a remaining question would be how the performance is affected by (non-Gaussian) discrete modulation of squeezed states to the shot-noise level.

## ACKNOWLEDGMENTS

The authors gratefully acknowledge valuable discussions with Nathan Walk, Andrew Lance, and Thomas Symul. This research was supported by funding from the Australian Department of Defence. This research is also supported by the Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE170100012).

## APPENDIX A: CALCULATE EVE'S HOLEVO INFORMATION FROM THE PURIFICATION ASSUMPTION

Let us consider a case where there is some preparation noise $\xi$ on top of the shot noise on Alice's side. In this case, the noise $\xi$ should be considered trusted in a passive attack scenario. This trusted noise is not attributed to Eve, so it can be modeled by placing a beam splitter of transmissivity $\eta_p \to 1$ on Alice's side before the channel. The preparation noise can be modeled by a two-mode squeezed vacuum state, $\rho_{F_0'G'}$, of quadrature variance $\upsilon' = \xi/(1-\eta_p)$. One input port of the beam splitter is the initial entangled mode $B_0$ with the $\hat{q}$ ($\hat{p}$) quadrature variance $b_q$ ($b_p$), and the second input port is fed by one half of the entangled state $\rho_{F_0'G'}$, mode $F_0'$, while the output ports are mode $B_0'$ (which is sent to Bob through the channel) and mode $F'$.

At the output of the channel Bob applies homodyne detection to the received mode $B$. Bob's homodyne detector with efficiency $\eta_B$ and electronic noise variance of $\nu_B$ can be modeled by placing a beam splitter of transmissivity $\eta_B$ before an ideal homodyne detector. The homodyne detector's electronic noise can be modeled by a two-mode squeezed vacuum state, $\rho_{F_0G}$, of quadrature variance $\upsilon$, where $\upsilon = 1 + \nu_B/(1-\eta_B)$.

One input port of the beam splitter is the received mode $B$, and the second input port is fed by one half of the entangled state $\rho_{F_0G}$, mode $F_0$, while the output ports are mode $B'$ (which is measured by the ideal homodyne detector) and mode $F$.

In a collective attack, Eve's information, $\chi(b{:}E)$, is given by $\chi(b{:}E) = \mathcal{S}(\rho_E) - \mathcal{S}(\rho_{E|B'})$. Here we assume Alice's preparation noise and Bob's detection noise are not accessible to Eve. In this case, the assumption that Alice and Bob's quantum state is purified by Eve's quantum state results in $\mathcal{S}(\rho_E) = \mathcal{S}(\rho_{AF'G'B})$, where the entropy $\mathcal{S}(\rho_{AF'G'B})$ can be calculated through the symplectic eigenvalues of covariance matrix $\mathbf{M}_{AF'G'B}$. The second entropy we require in order to determine $\chi(b{:}E)$ can be written as $\mathcal{S}(\rho_{E|B'}) = \mathcal{S}(\rho_{AF'G'FG|B'})$. The covariance matrix of the conditional state $\rho_{AF'G'FG|B'}$ is given by $\mathbf{M}_{AF'G'FG|B'} = \mathbf{M}_{AF'G'FG} - \sigma_{AF'G'FG,B'}\,(\mathbf{X}\mathbf{M}_{B'}\mathbf{X})^{\mathrm{MP}}\,\boldsymbol{\sigma}^T_{AF'G'FG,B'}$. Note that the matrices $\mathbf{M}_{AF'G'FG}$, $\boldsymbol{\sigma}_{AF'G'FG,B'}$, and $\mathbf{M}_{B'}$ can be derived from the decomposition of the covariance matrix

$$\mathbf{M}_{AF'G'FGB'} = \begin{bmatrix} \mathbf{M}_{AF'G'FG} & \boldsymbol{\sigma}_{AF'G'FG,B'} \\ \boldsymbol{\sigma}^T_{AF'G'FG,B'} & \mathbf{M}_{B'} \end{bmatrix}. \tag{A1}$$

Note that the covariance matrix $\mathbf{M}_{AF'G'FGB'}$ is given by the rearrangement of the following matrix:

$$\mathbf{M}_{AF'G'B'FG} = (\mathbf{I}_A \oplus \mathbf{I}_{F'} \oplus \mathbf{I}_{G'} \oplus \mathbf{S}_{\mathrm{bs}} \oplus \mathbf{I}_G)^T \times (\mathbf{M}_{AF'G'B} \oplus \mathbf{M}_{F_0G})(\mathbf{I}_A \oplus \mathbf{I}_{F'} \oplus \mathbf{I}_{G'} \oplus \mathbf{S}_{\mathrm{bs}} \oplus \mathbf{I}_G), \tag{A2}$$

where $\mathbf{S}_{\mathrm{bs}}$ is the matrix for the beam splitter transformation (applied on modes $B$ and $F_0$), given by

$$\mathbf{S}_{\mathrm{bs}} = \begin{bmatrix} \sqrt{\eta_B}\,\mathbf{I} & \sqrt{1-\eta_B}\,\mathbf{I} \\ -\sqrt{1-\eta_B}\,\mathbf{I} & \sqrt{\eta_B}\,\mathbf{I} \end{bmatrix}, \tag{A3}$$

and the covariance matrix of the entangled state $\rho_{F_0G}$ is given by

$$\mathbf{M}_{F_0G} = \begin{bmatrix} \upsilon\,\mathbf{I} & \sqrt{\upsilon^2-1}\,\mathbf{Z} \\ \sqrt{\upsilon^2-1}\,\mathbf{Z} & \upsilon\,\mathbf{I} \end{bmatrix}. \tag{A4}$$

Note that the covariance matrix $\mathbf{M}_{AF'G'B}$ is obtained by tracing out Eve's mode $E$ from the covariance matrix $\mathbf{M}_{AF'G'BE}$, given by

$$\mathbf{M}_{AF'G'BE} = (\mathbf{I}_A \oplus \mathbf{I}_{F'} \oplus \mathbf{I}_{G'} \oplus \mathbf{S}^c_{\mathrm{bs}})^T \times (\mathbf{M}_{AF'G'B'_0} \oplus \mathbf{M}_{E_0})(\mathbf{I}_A \oplus \mathbf{I}_{F'} \oplus \mathbf{I}_{G'} \oplus \mathbf{S}^c_{\mathrm{bs}}), \tag{A5}$$

where $\mathbf{S}^c_{\mathrm{bs}}$ is the matrix for the beam splitter (i.e., channel) transformation (applied on modes $B'_0$ and $E_0$), given by

$$\mathbf{S}^c_{\mathrm{bs}} = \begin{bmatrix} \sqrt{\eta_f}\,\mathbf{I} & \sqrt{1-\eta_f}\,\mathbf{I} \\ -\sqrt{1-\eta_f}\,\mathbf{I} & \sqrt{\eta_f}\,\mathbf{I} \end{bmatrix}, \tag{A6}$$

where $\eta_f$ is the effective transmissivity of the free-space channel, and $\mathbf{M}_{E_0}$ is the covariance matrix of the vacuum state. Note that the covariance matrix $\mathbf{M}_{AF'G'B'_0}$ is given by the rearrangement of the following covariance matrix:

$$\mathbf{M}_{AB'_0F'G'} = (\mathbf{I}_A \oplus \mathbf{S}'_{\mathrm{bs}} \oplus \mathbf{I}_{G'})^T \times (\mathbf{M}_{AB_0} \oplus \mathbf{M}_{F'_0G'})(\mathbf{I}_A \oplus \mathbf{S}'_{\mathrm{bs}} \oplus \mathbf{I}_{G'}), \tag{A7}$$

where $\mathbf{S}'_{\mathrm{bs}}$ is the matrix for the beam splitter transformation (applied on modes $B_0$ and $F'_0$), which is given by

$$\mathbf{S}'_{\mathrm{bs}} = \begin{bmatrix} \sqrt{\eta_p}\,\mathbf{I} & \sqrt{1-\eta_p}\,\mathbf{I} \\ -\sqrt{1-\eta_p}\,\mathbf{I} & \sqrt{\eta_p}\,\mathbf{I} \end{bmatrix}. \tag{A8}$$

Note that the covariance matrix of the entangled state $\rho_{F'_0G'}$ is given by

$$\mathbf{M}_{F'_0G'} = \begin{bmatrix} \upsilon'\,\mathbf{I} & \sqrt{\upsilon'^2-1}\,\mathbf{Z} \\ \sqrt{\upsilon'^2-1}\,\mathbf{Z} & \upsilon'\,\mathbf{I} \end{bmatrix}, \tag{A9}$$

and the covariance matrix $\mathbf{M}_{AB_0}$ is given by Eq. (1). Note that with the assumption of zero (trusted) fluctuation noise, the purification of Alice and Bob's state by Eve's state results in $\mathbf{M}_E = \mathbf{M}_{AF'G'B}$, and $\mathbf{M}_{E|B'} = \mathbf{M}_{AF'G'FG|B'}$. Therefore, Eve's information, $\chi(b{:}E)$, calculated from Eve and Bob's covariance matrix (discussed in the main text) is the same as that calculated based on the purification assumption (discussed above).

## APPENDIX B: PARAMETER ESTIMATION FOR SQUEEZED-STATE PROTOCOL

In the prepare-and-measure scheme, for a subchannel with transmissivity $\eta$, we can consider a normal linear model for Alice and Bob's correlated $q$ quadrature variables, $q_A$ and $q_B$, respectively,

$$q_B = t_s q_A + q_{n,s}, \tag{B1}$$

where $t_s = \sqrt{\eta_B \eta}$, and $q_{n,s}$ follows a centered normal distribution whose variance is determined from the observed data as follows, $\sigma_s^2 = 1 + \nu_B + \eta_B\eta(V_{\mathrm{sqz}} + \xi) - \eta_B\eta$ (note that Alice's variable $q_A$ has the variance $V_{\mathrm{sig}}$). Using the revealed data of size $k_s$ for the subchannel (note in our numerical simulation we assumed $10^5$ subchannels), the maximum-likelihood estimators for the subchannel parameters, $t_s$ and $\sigma_s^2$, are given by [48,49]

$$\hat{t}_s = \frac{\sum_{i=1}^{k_s} A_i B_i}{\sum_{i=1}^{k_s} A_i^2}, \qquad \hat{\sigma}_s^2 = \frac{1}{k_s}\sum_{i=1}^{k_s} (B_i - \hat{t}_s A_i)^2, \tag{B2}$$

where $A_i$ and $B_i$ are the realizations of $q_A$ and $q_B$ for the subchannel, respectively. The confidence interval for $t_s$ is given by $t_s \in [\hat{t}_s - \Delta(t_s), \hat{t}_s + \Delta(t_s)]$, where

$$\Delta(t_s) = z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}_s^2}{k_s V_{\mathrm{sig}}}}. \tag{B3}$$

The estimator of the square root of subchannel transmissivity, and its error bar is given by

$$\widehat{\sqrt{\eta}} = \frac{\hat{t}_s}{\sqrt{\hat{\eta}_B}},$$

$$\Delta(\sqrt{\eta}) = \widehat{\sqrt{\eta}}\sqrt{\left|\frac{\Delta(t_s)}{\hat{t}_s}\right|^2 + \left|\frac{\Delta(\eta_B)}{2\hat{\eta}_B}\right|^2}. \tag{B4}$$

Here we generalize the above discussed parameter estimation method to the data of size $k$ revealed over all subchannels to estimate $\xi$. Considering Eq. (B1) over all subchannels we can still have a normal linear model for Alice and Bob's correlated $q$ quadrature variables as

$$q_B = t q_A + q_n, \tag{B5}$$

where $t = \sqrt{\eta_B \langle\eta\rangle}$, and $q_n$ follows a centered normal distribution whose variance is determined from the observed data as $\sigma^2 = 1 + \nu_B + \eta_B\langle\eta\rangle(V_{\rm sqz} + \xi) - \eta_B\langle\eta\rangle$. Using the total data revealed over all subchannels of size $k$, we can calculate the maximum-likelihood estimators for $t$ and $\sigma^2$, which are given by

$$\hat{t} = \frac{\sum_{i=1}^k A_i B_i}{\sum_{i=1}^k A_i^2},$$

$$\hat{\sigma}^2 = \frac{1}{k}\sum_{i=1}^k (B_i - \hat{t}A_i)^2. \tag{B6}$$

The confidence intervals for these parameters are given by $t \in [\hat{t} - \Delta(t), \hat{t} + \Delta(t)]$, and $\sigma^2 \in [\hat{\sigma}^2 - \Delta(\sigma^2), \hat{\sigma}^2 + \Delta(\sigma^2)]$ where

$$\Delta(t) = z_{\epsilon_{\rm PE}/2}\sqrt{\frac{\hat{\sigma}^2}{k V_{\rm sig}}},$$

$$\Delta(\sigma^2) = z_{\epsilon_{\rm PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{k}}. \tag{B7}$$

Note that when no signal is exchanged, Bob's variable with realization $B_{0i}$ follows a centered normal distribution whose variance is determined from the observed data as follows, $\sigma_0^2 = 1 + \nu_B$, which is Bob's shot noise variance. The maximum-likelihood estimator for $\sigma_0^2$ is given by $\hat{\sigma}_0^2 = \frac{1}{N}\sum_{i=1}^N B_{0i}^2$. The confidence interval for this parameter is given by $\sigma_0^2 \in [\hat{\sigma}_0^2 - \Delta(\sigma_0^2), \hat{\sigma}_0^2 + \Delta(\sigma_0^2)]$, where $\Delta(\sigma_0^2) = z_{\epsilon_{\rm PE}/2}\frac{\hat{\sigma}_0^2\sqrt{2}}{\sqrt{N}}$.[2] Now we can estimate $\langle\eta\rangle$ and $\xi$, which are given by

$$\widehat{\langle\eta\rangle} = \frac{\hat{t}^2}{\hat{\eta}_B},$$

$$\Delta(\langle\eta\rangle) = \widehat{\langle\eta\rangle}\sqrt{\left|\frac{2\Delta(t)}{\hat{t}}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2},$$

$$\hat{\xi} = \frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{\eta}_B\widehat{\langle\eta\rangle}} - \hat{V}_{\rm sqz} + 1,$$

$$\Delta(\xi) = \hat{\xi}\sqrt{\left|\frac{\Delta(\sigma^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\sigma_0^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2 + \left|\frac{\Delta(\langle\eta\rangle)}{\widehat{\langle\eta\rangle}}\right|^2} + \Delta(V_{\rm sqz}). \tag{B8}$$

Note that in order to maximize Eve's information, $\chi^{\epsilon_{\rm PE}}(b{:}E)$, from passive collective attacks, the worst-case estimators of $\eta$ and $\xi$ should be used to evaluate Eve's information. Now, having Eqs. (B4) and (B8), the worst-case estimators of parameters $\sqrt{\eta}$ (for channel losses above 3 dB) to calculate $\eta_f$ and $\xi$ are given by $\widehat{\sqrt{\eta}} + \Delta(\sqrt{\eta})$ and $\hat{\xi} + \Delta(\xi)$. Note also that for the parameter estimation of the coherent-state protocol, we can still use the equations provided in this section, but we should set $V_{\rm sqz} = 1$ due to the use of coherent states.

Note that here we estimated the noise $\xi$ by first estimating the channel transmissivity and revealing a subset of data. However, since the preparation noise $\xi$ is trusted and not under Eve's control, it can be estimated using the whole data block with a very good precision. This estimation can be performed in only Alice's laboratory without revealing any data.

[2]Note that $z_{\epsilon_{\rm PE}/2}$ is such that $1 - \mathrm{erf}(\frac{z_{\epsilon_{\rm PE}/2}}{\sqrt{2}})/2 = \epsilon_{\rm PE}/2$, where erf is the error function.


[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[4] C. S. Jacobsen, L. S. Madsen, V. C. Usenko, R. Filip, and U. L. Andersen, Complete elimination of information leakage in continuous-variable quantum communication channels, npj Quantum Inf. **4**, 32 (2018).

[5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[6] C. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[7] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[8] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[9] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[10] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[11] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[12] R. Garcia-Patron, Ph.D. thesis, Université Libre de Bruxelles, 2007.

[13] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[14] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).

[15] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook, IEEE Commun. Surv. Tutor. **21**, 881 (2019).

[16] S.-K. Liao *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[17] J. Yin *et al.*, Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. **119**, 200501 (2017).

[18] A. A. Semenov and W. Vogel, Quantum light in the turbulent atmosphere, Phys. Rev. A **80**, 021802(R) (2009).

[19] D. Yu. Vasylyev, A. A. Semenov, and W. Vogel, Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality, Phys. Rev. Lett. **108**, 220501 (2012).

[20] D. Yu. Vasylyev, A. A. Semenov, and W. Vogel, Atmospheric Quantum Channels with Weak and Strong Turbulence, Phys. Rev. Lett. **117**, 090501 (2016).

[21] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, Free-space quantum links under diverse weather conditions, Phys. Rev. A. **96**, 043856 (2017).

[22] D. Vasylyev, W. Vogel, and A. A. Semenov, Theory of atmospheric quantum channels based on the law of total probability, Phys. Rev. A **97**, 063852 (2018).

[23] R. Dong, M. Lassen, J. Heersink, C. Marquardt, R. Filip, G. Leuchs, and U. L. Andersen, Continuous-variable entanglement distillation of non-Gaussian mixed states, Phys. Rev. A **82**, 012312 (2010).

[24] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels, New J. Phys. **14**, 093048 (2012).

[25] N. Hosseinidehaj and R. Malaney, Gaussian entanglement distribution via satellite, Phys. Rev. A **91**, 022304 (2015).

[26] N. Hosseinidehaj and R. Malaney, Quantum key distribution over combined atmospheric fading channels, in *Proceedings of the IEEE International Conference on Communications (ICC), London, UK* (IEEE, Piscataway, NJ, 2015), pp. 7413–7419.

[27] N. Hosseinidehaj and R. Malaney, Entanglement generation via non-Gaussian transfer over atmospheric fading channels, Phys. Rev. A **92**, 062336 (2015).

[28] N. Hosseinidehaj and R. Malaney, CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels, in *Proceedings of IEEE Global Communications Conference (GLOBECOM), Washington, DC* (IEEE, Piscataway, NJ, 2016), pp. 1–7.

[29] N. Hosseinidehaj and R. Malaney, CV-MDI quantum key distribution via satellite, Quantum Inf. Comput. **17**, 361 (2017).

[30] P. Papanastasiou, C. Weedbrook, and S. Pirandola, Continuous-variable quantum key distribution in uniform fast-fading channels, Phys. Rev. A **97**, 032311 (2018).

[31] S. Wang, P. Huang, T. Wang, and G. Zeng, Atmospheric effects on continuous-variable quantum key distribution, New J. Phys. **20**, 083037 (2018).

[32] L. Ruppert, C. Peuntinger, B. Heim, K. Günthner, V. C. Usenko, D. Elser, G. Leuchs, R. Filip, and C. Marquardt, Fading channel estimation for free-space continuous-variable secure quantum communication, New J. Phys. **21**, 123036 (2019).

[33] N. Hosseinidehaj, N. Walk, and T. C. Ralph, Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems, Phys. Rev. A **103**, 012605 (2021).

[34] Y. Yamamoto, S. Machida, and W. H. Richardson, Photon number squeezed states in semiconductor lasers, Science **255**, 1219 (1992).

[35] S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[36] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).

[37] M. Navascues, F. Grosshans, and A. Acin, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[38] R. Garcia-Patron and N. J. Cerf, Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[39] V. C. Usenko and R. Filip, Trusted Noise in continuous-variable quantum key distribution: A threat and a defense, Entropy **18**, 20 (2016).

[40] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).

[41] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[42] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (2015).

[43] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Phys. Rev. A **97**, 052327 (2018).

[44] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks, Phys. Rev. Lett. **109**, 100502 (2012).

[45] M. Tomamichel, Ph.D. thesis, Swiss Federal Institute of Technology (ETH), Zurich, 2012, arXiv:1203.2142.

[46] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[47] V. C. Usenko and F. Grosshans, Unidimensional continuous-variable quantum key distribution, Phys. Rev. A **92**, 062337 (2015).

[48] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[49] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, Phys. Rev. A **86**, 032309 (2012).