Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems

Nedasadat Hosseinidehaj,[1,*] Nathan Walk,[2] and Timothy C. Ralph[1]

[1]*Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

[2]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

(Received 29 March 2020; accepted 21 December 2020; published 20 January 2021)

Free-space channels provide the possibility of establishing continuous-variable quantum key distribution in global communication networks. However, the fluctuating nature of transmissivity in these channels introduces an extra noise which reduces the achievable secret key rate. We consider two classical postprocessing strategies, postselection of high-transmissivity data and data clusterization, to reduce the fluctuation-induced noise of the channel. We undertake the investigation of such strategies utilizing a composable security proof in a realistic finite-size regime against both collective and individual attacks. We also present an efficient parameter estimation approach to estimate the effective Gaussian parameters over the postselected data or the clustered data. Although the composable finite-size effects become more significant with the postselection and clusterization both reducing the size of the data, our results show that these strategies are still able to enhance the finite-size key rate against both individual and collective attacks with a remarkable improvement against collective attacks, even moving the protocol from an insecure regime to a secure regime under certain conditions.

DOI: 10.1103/PhysRevA.103.012605

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] allows two trusted parties (traditionally called Alice and Bob) to share a secret key which is unknown to a potential eavesdropper (traditionally called Eve) by using quantum communication over an insecure quantum channel and classical communication over an authenticated classical channel. Quantum key distribution systems were first proposed for discrete-variable quantum systems [4,5], where the key information is encoded onto the degrees of freedom of single photons and detection is realized by single-photon detectors, and then extended for continuous-variable (CV) quantum systems [6–9], where the key information is encoded onto the amplitude and phase quadratures of the quantized electromagnetic field of light and detection is realized by (faster and more efficient) homodyne or heterodyne detectors. Continuous-variable QKD systems (see [2,10–12] for review) have the potential to achieve higher secret key rates, as well as the advantage of compatibility with current telecommunication optical networks.

Quantum key distribution can in general be performed using two quantum communication technologies, optical fibers and free-space channels, which are considered as complementary technologies in the emerging global QKD network. When an optical fiber exists between two points, we can perform quantum communication without being affected by external conditions such as background light, weather conditions, or other environmental obstructions. However, since optical fiber suffers from optical absorption, the maximum secure transmission distance is limited to a few hundred kilometers [13–17]. On the other hand, free-space channels offer convenient flexibility in terms of infrastructure establishment, with the possibility of implementing links to moving objects. Terrestrial free-space channels also limit the secure distance, due to the curvature of the earth, potential line-of-sight blockages, and atmospheric absorption and turbulence [18–23]. In long-distance applications, where there is no direct free-space line of sight between two ground stations, free-space channels via satellite can be used for quantum communication between satellite and the ground stations [24,25]. In satellite-based quantum communications only a small fraction of the propagation path is through the atmosphere, while most of the propagation undergoes no absorption and no turbulence.

In free-space channels (in contrast to optical fibers) the channel suffers from atmospheric turbulence (causing beam wandering, beam shape deformation, beam broadening, etc.), which results in a random variation of channel transmissivity in time. This fluctuation effect can be characterized by a probability distribution of the channel transmissivity. Depending on the atmospheric effects, advanced probability distribution models have been proposed for the channel transmissivity [26–30], which accurately describe free-space experiments [18–20].

A free-space channel can be considered as a set of subchannels, where the transmissivity of the channel is relatively stable for each subchannel [18]. In a Gaussian CV QKD protocol [10,11], Alice prepares Gaussian quantum states, which are modulated with a Gaussian distribution. Once these Gaussian states are transmitted over a free-space channel to Bob, the fluctuating transmissivity of the channel makes the received state (at Bob's station) a non-Gaussian mixture of the Gaussian states obtained for each subchannel [31]. This

*n.hosseinidehaj@uq.edu.au

non-Gaussian effect introduces an extra noise, which reduces the key rate [18,32,33]; however, the fluctuating transmissivity also provides a possibility to recover the key rate through the postselection of data from subchannels with high transmissivity [18]. The postselection decreases the amount of channel fluctuation (i.e., decreases the variance of the transmissivity distribution), which leads to a postselected state with a more Gaussian nature (i.e., with less non-Gaussian noise). This postselection has been shown to be effective for CV QKD protocols in the asymptotic regime [18,32] against Gaussian collective attacks.[1] The other classical postprocessing strategy which can also reduce the negative effect of the fluctuation-induced noise is to partition the recorded data into different clusters [35,36] and analyze the security for each cluster separately. Although both of these strategies are effective in reducing the fluctuation-induced noise, they also reduce the size of the effective data set used for parameter estimation and security analysis. Since in practice only a finite number of signals are exchanged between Alice and Bob, the composable finite-size issues become even more significant when either postselection or clusterization is applied. Thus, whether these classical postprocessing strategies are still effective in a composable finite-size regime remains an open question.

We consider the no-switching [37,38] CV QKD protocol (based on Gaussian-modulated coherent states and heterodyne detection) over a free-space channel. For the channel probability distribution we consider the elliptic-beam model [28], which accounts for the deflection and deformation of a Gaussian beam caused by turbulence in atmospheric channels. We analyze the composable finite-size security of the protocol by using the recent security proof, stating that, according to the Gaussian de Finetti reduction, for the security analysis of the no-switching protocol against general attacks, it is sufficient to consider Gaussian collective attacks in the finite-size composable regime [39,40]. We answer the question whether the postselection of high-transmissivity subchannels and data clusterization can improve the performance of the free-space CV QKD system in a composable finite-size regime against collective and individual attacks.[2]

For both postselection and clusterization, the subchannel transmissivity has to be estimated by publicly revealing a randomly chosen subset of the data obtained over the stability time. There are other proposed methods [42–44] which utilize classical auxiliary probes or the local oscillator to estimate the subchannel transmissivity. However, since these classical signals could likely be manipulated by Eve, the classical estimation of the channel may compromise the security. Note that, similar to the transmissivity, the excess noise can also be estimated for each subchannel realization separately. However, in practice, only a small number of signals can be transmitted over the stability time of the channel, which results in pessimistic error bars for the estimated excess noise, which consequently overestimates Eve's information and leads to a pessimistic bound for the key rate. Hence, to estimate Eve's information, instead of estimating the excess noise of each subchannel, we can utilize the data revealed over all subchannels (which are used for the security analysis) to estimate the effective excess noise. Our security analysis shows that the optimized postselection can improve the finite-size key rate against both individual and collective attacks. Our previous work on Gaussian postselection [45] showed a relatively modest improvement in the finite-size collective attacks in comparison with the improvement predicted by an asymptotic analysis. Surprisingly, our present work shows that the postselection of high-transmissivity subchannels provides a significant improvement against collective attacks in the composable finite-size regime, comparable to that predicted asymptotically. Further, we show that the data clusterization can also significantly improve the composable finite key rates against collective attacks, provided an optimal clusterization of subchannels is chosen.

The structure of the remainder of the paper is as follows. In Sec. II the no-switching CV QKD system is described, with the security discussed in the composable finite-size regime. In Sec. III the CV QKD system over free-space channels is discussed, with the security analyzed in Sec. IV using two approaches in the composable finite-size regime by introducing an efficient parameter estimation approach. In Sec. V the finite-size composable security is analyzed for the system with postselection of high-transmissivity subchannels and for the system with data clusterization, and the significant improvement of the composable finite key rates against collective attacks using these strategies is illustrated. Finally, concluding remarks are provided in Sec. VI.

II. SYSTEM MODEL

Continuous-variable QKD in general consists of two steps, quantum communication followed by classical postprocessing [2,10–12]. In the quantum communication step, Alice prepares a classical random variable a and encodes a onto quantum states. In Gaussian CV QKD the random variable is drawn from a Gaussian distribution and quantum states are either coherent states or squeezed states of light. In Gaussian encoding the Gaussian quantum states are modulated (i.e., displaced) according to the Gaussian random variable a. The modulated quantum states are transmitted from Alice to Bob over an insecure quantum channel, which is characterized by some transmissivity and some excess noise. At the end of the channel Bob measures the received quantum states with either homodyne or heterodyne detection to obtain a classical random variable b, which is correlated to Alice's variable a.

In this work we consider a Gaussian no-switching CV QKD protocol [37,38], where Alice prepares Gaussian-modulated coherent states and Bob uses heterodyne detection. In a prepare-and-measure scheme Alice generates two random real variables (a_q, a_p), drawn from two independent Gaussian distributions of variance V_A. Alice prepares coherent states by modulating a coherent laser source by amounts of (a_q, a_p). The variance of the beam after the modulator is $V_A + 1 = V$

[1]Note that the postselection of transmission bins with high value has also been shown effective for enhancing the squeezing properties of light transmitted through the turbulent atmosphere [19,28] and improving the fidelity of the coherent-state teleportation over the turbulent atmosphere [34].

[2]Note that when Eve has a restricted quantum memory, individual attacks can become optimal eavesdropping attacks for the no-switching CV QKD protocol [41].

(where the 1 is for the shot-noise variance); hence an average output state is thermal of variance V. The prepared coherent states are transmitted over an insecure quantum channel to Bob. For each incoming state, Bob uses heterodyne detection and measures both the $\hat{q}$ and $\hat{p}$ quadratures to obtain (b_q, b_p). Repeating this procedure many times, Alice and Bob end up with two sets of correlated data, known as the raw keys. In this protocol, sifting is not needed, since both of the random variables generated by Alice are used for the key generation. When all the incoming quantum states have been measured by Bob, classical postprocessing (including discretization, parameter estimation, error correction, and privacy amplification) over a public but authenticated classical channel is commenced to produce a shared secret key.

Each prepare-and-measure (PM) scheme can be represented by an equivalent entanglement-based (EB) scheme [10,11]. In a Gaussian EB scheme, Alice generates a two-mode Gaussian entangled state. She keeps one mode, on which she applies either homodyne or heterodyne detection, projecting the second mode onto squeezed states or coherent states, respectively. In the equivalent EB scheme of the no-switching protocol, Alice generates a pure two-mode squeezed vacuum state with the quadrature variance V. Alice keeps one mode, while sending the second mode to Bob over the insecure quantum channel. When Alice applies a heterodyne detection to her mode obtaining (x_q, x_p), she projects the other mode onto a coherent state. At the output of the channel, Bob applies a heterodyne detection to the received mode to obtain (y_q, y_p). As a result of Alice's and Bob's heterodyne detection on all the shared entangled states, they generate two sets of correlated data as the raw key, from which they can extract a shared secret key through the classical postprocessing. It is convenient to evaluate security using the equivalent EB scheme even if that actual performed protocol is a PM scheme.

The classical postprocessing starts with discretization [46], where Alice and Bob encode each measurement outcome with d bits of precision. The classical channel is assumed to be authenticated, which means Eve can monitor the classical channel, but she is not able to change the classical signals. However, the quantum channel is assumed to be in Eve's full control. This is the reason that the channel parameters (i.e., transmissivity and excess noise) have to be estimated by Alice and Bob over the parameter estimation step in order to upper bound Eve's information. The parameter estimation is usually performed by revealing a randomly chosen subset of the raw data (which should be discarded from the raw key). After the parameter estimation, error correction is performed, where Alice and Bob communicate the syndromes of the errors affecting their data. Error correction can be performed in either direct reconciliation (DR) or reverse reconciliation (RR). In the DR case Alice is the reference of reconciliation, where she sends the syndromes to Bob, who corrects his data based on the received syndrome to have the same data as Alice, while in the RR scenario Bob is the reference of reconciliation. As a result, Alice's and Bob's raw keys are transformed into the same string of bits. In the secret key rate calculation the leakage during the error correction, which is in fact the size of the syndrome, should be subtracted from the secret key length. Finally, we have privacy amplification, in which Alice and Bob generate a smaller but secret key from the raw key by reducing Eve's information of the key to a negligible amount. The amount of data to discard is given by the upper bound on Eve's information computed during the parameter estimation.

A. Composable finite-size security analysis

General attacks (or coherent attacks) are known to be the most powerful eavesdropping attacks on CV QKD protocols. In a coherent attack Eve prepares a global ancillary quantum system, interacting collectively with all quantum states transmitted through the channel, with all the output ancillae stored in a quantum memory. A collective measurement is applied over the stored ensemble to extract maximum information on the key. In a collective attack Eve prepares an ensemble of independent and identical quantum systems, each one interacting individually with a single quantum state sent through the channel, with the output ancilla stored in a quantum memory. The entire stored ensemble is collectively measured to extract the maximum information on the key, upper bounded by the Holevo information. In an individual attack, Eve interacts individually with each quantum state sent by Alice and performs an individual measurement on the output ancilla [10].

In the asymptotic regime collective attacks are as powerful as coherent attacks [47] and for Gaussian protocols, Gaussian collective attacks are asymptotically optimal [48–50]. Note also that for Gaussian protocols, among individual attacks, Gaussian individual attacks are asymptotically optimal [10].

In the finite-size regime, the no-switching CV QKD protocol with N coherent states sent by Alice to Bob is ϵ-secure against Gaussian collective attacks in a reverse reconciliation scenario if $\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor}$ [46,51,52] and if the key length $\ell^{\rm col}$ is chosen such that [46,51]

$$\ell^{\rm col} \leqslant N'[\beta I(a{:}b) - \chi^{\epsilon_{\rm PE}}(b{:}E)] - \sqrt{N'}\Delta_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \tag{1}$$

where [46,51]

$$\Delta_{\rm AEP} = (d+1)^2 + 4(d+1)\sqrt{\log_2(2/\epsilon_{\rm sm}^2)} + 2\log_2(2/\epsilon^2\epsilon_{\rm sm}) + 4\epsilon_{\rm sm} d/\epsilon\sqrt{N'}, \tag{2}$$

where $N' = N - k$, with k the number of data points Alice and Bob are required to disclose during the parameter estimation, d is the discretization parameter (i.e., each symbol is encoded with d bits of precision), $\epsilon_{\rm sm}$ is the smoothing parameter, $\epsilon_{\rm cor}$ and $\epsilon_{\rm PE}$ are the maximum failure probabilities for the error correction and parameter estimation, respectively, $I(a{:}b)$ is the classical mutual information shared between Alice and Bob, and $0 \leqslant \beta \leqslant 1$ is the reconciliation efficiency. Note that in the finite-size regime the usual $\chi(b{:}E)$ (the maximum mutual information shared between Eve and Bob limited by the Holevo bound for the collective attack) has to be replaced by $\chi^{\epsilon_{\rm PE}}(b{:}E)$, taking into account the finite precision of the parameter estimation. In fact, it is now assumed that Eve's information is upper bounded by $\chi^{\epsilon_{\rm PE}}(b{:}E)$, except with probability $\epsilon_{\rm PE}$. The final key rate in bits per mode is then given by $\ell^{\rm col}/N$.

Note that for the ϵ-security analysis of the same protocol against Gaussian individual attacks we can still use Eq. (1),

where $\chi^{\epsilon_{\rm PE}}(b{:}E)$ must be replaced by the classical mutual information between Eve and Bob, maximized by $I^{\epsilon_{\rm PE}}(b{:}E)$ except with probability $\epsilon_{\rm PE}$. Note also that, based on the recent security proof in [39,40], for analyzing the composable finite-size security of the no-switching CV QKD protocol against general attacks, the security of the protocol can be first analyzed against Gaussian collective attacks with a security parameter ϵ [46] through the use of Eq. (1) and then, by using the Gaussian de Finetti reduction [39], the security can be obtained against general attacks with a polynomially larger security parameter $\tilde{\epsilon}$ [39]. Note that the security loss due to the reduction from general attacks to Gaussian collective attacks scales like $O(N'^4)$ [39]. More precisely, according to [39], ϵ-security against Gaussian collective attacks implies $\tilde{\epsilon}$-security against general attacks, where $\tilde{\epsilon}/\epsilon = K^4/50$, with $K \sim N'$.

III. FREE-SPACE CV QKD SYSTEMS

In free-space channels the atmospheric effects will cause the transmitted beam to experience fading. Hence, in contrast to a fiber link with a fixed transmissivity, the transmissivity η of a free-space channel fluctuates in time. Such fading channels can be characterized by a probability distribution $p(\eta)$ [18,53]. In fact, a fading channel can be decomposed into a set of subchannels. Each subchannel η_i is defined as a set of events for which the transmissivity is relatively stable, meaning that the fluctuations of the transmissivity are negligible. Each subchannel η_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 realizable value of transmissivity of the fading channel. Thus, the Wigner function of the output state is the sum of the Wigner functions of the states after subchannels weighted by subchannel probabilities [53]. Hence, the input Gaussian state $\rho_{\rm in}$ remains Gaussian after passing through each subchannel; however, the resulting state at the output of the channel $\rho_{\rm out} = \sum_i p_i \rho_i$ (with ρ_i the Gaussian state resulted from the transmission of the input Gaussian state $\rho_{\rm in}$ through the subchannel η_i) is a non-Gaussian state [53].

In the equivalent entanglement-based scheme of the no-switching CV QKD protocol, the initial pure two-mode Gaussian entangled state ρ_{AB_0} with the quadrature variance V is completely described by its first moment, which is zero, and its covariance matrix

$$\mathbf{M}_{AB_0} = \begin{bmatrix} V\mathbf{I} & \sqrt{V^2-1}\mathbf{Z} \\ \sqrt{V^2-1}\mathbf{Z} & V\mathbf{I} \end{bmatrix}, \tag{3}$$

with $\mathbf{I}$ a 2×2 identity matrix and $\mathbf{Z} = \mathrm{diag}(1,-1)$. Alice keeps mode A and sends mode B_0 through an insecure free-space channel. After transmission of mode B_0 through a quantum subchannel with transmissivity η and excess noise ξ_η (relative to the input of the subchannel with transmissivity η), the covariance matrix of the Gaussian state $\rho_{AB_1,\eta}$ at the output of the subchannel is given by

$$\mathbf{M}_{AB_1,\eta} = \begin{bmatrix} V\mathbf{I} & \sqrt{\eta}\sqrt{V^2-1}\mathbf{Z} \\ \sqrt{\eta}\sqrt{V^2-1}\mathbf{Z} & [\eta(V-1)+\eta\xi_\eta+1]\mathbf{I} \end{bmatrix}. \tag{4}$$

The ensemble-average state at the output of a free-space channel ρ_{AB_1} is a non-Gaussian mixture of Gaussian states obtained from individual subchannels $\rho_{AB_1,\eta}$. Thus, the Wigner function of the output state W_{AB_1} is the sum of the Wigner functions of the states obtained from individual subchannels $W_{AB_1,\eta}$ weighted by subchannel probabilities p_i, i.e., we have $W_{AB_1}(\mathbf{q},\mathbf{p}) = \sum_i p_i W_{AB_1,\eta}(\mathbf{q},\mathbf{p})$, where $\mathbf{q} = (q_A, q_{B_1})$ and $\mathbf{p} = (p_A, p_{B_1})$ indicate the vectors of amplitude and phase quadrature variables. Having the Wigner function W_{AB_1}, we can calculate the second moments of the quadratures through integration as

$$\begin{aligned}\langle \hat{X}\hat{Y}\rangle &= \int dq_A dq_{B_1} dp_A dp_{B_1} xy W_{AB_1}(q_A, q_{B_1}, p_A, p_{B_1}) \\ &= \sum_i p_i \int dq_A dq_{B_1} dp_A dp_{B_1} xy W_{AB_1,\eta}(q_A, q_{B_1}, p_A, p_{B_1}),\end{aligned} \tag{5}$$

where $\hat{X}, \hat{Y} = \hat{q}_A, \hat{q}_{B_1}, \hat{p}_A, \hat{p}_{B_1}$. Thus, the elements of the covariance matrix of the ensemble-average state ρ_{AB_1} are given by the convex sum of the moments of state $\rho_{AB_1,\eta}$, as we have $\langle \hat{X}\hat{Y}\rangle = \sum_i p_i \langle \hat{X}\hat{Y}\rangle_\eta$, or $\int_0^{\eta_{\max}} \langle \hat{X}\hat{Y}\rangle_\eta p(\eta)d\eta$ for a continuous probability distribution. The covariance matrix of the non-Gaussian state ρ_{AB_1} is then given by

$$\mathbf{M}_{AB_1} = \begin{bmatrix} V\mathbf{I} & \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\mathbf{Z} \\ \langle\sqrt{\eta}\rangle\sqrt{V^2-1}\mathbf{Z} & [\langle\eta\rangle(V-1)+\langle\eta\xi_\eta\rangle+1]\mathbf{I} \end{bmatrix}, \tag{6}$$

where $\langle\cdot\rangle$ denotes the mean value over the subchannels (or over all possible values of η), i.e.,

$$\begin{aligned}\langle\eta\rangle &= \int_0^{\eta_{\max}} \eta p(\eta)d\eta, \\ \langle\sqrt{\eta}\rangle &= \int_0^{\eta_{\max}} \sqrt{\eta} p(\eta)d\eta, \\ \langle\eta\xi_\eta\rangle &= \int_0^{\eta_{\max}} \eta\xi_\eta p(\eta)d\eta.\end{aligned} \tag{7}$$

Note that, unlike the previous theoretical works on free-space CV QKD [18,32,33,54–57] with the assumption of fixed excess noise, here we have assumed that the channel excess noise can also randomly vary in time, where the value of the excess noise depends on the the value of the channel transmissivity.

From the covariance matrix of the non-Gaussian ensemble-average state in Eq. (6), it is evident that the fluctuating channel can be considered as a nonfluctuating channel with the effective transmissivity η_f and effective excess noise ξ_f, so the covariance matrix of the ensemble-average state can be rewritten as

$$\mathbf{M}_{AB_1} = \begin{bmatrix} V\mathbf{I} & \sqrt{\eta_f}\sqrt{V^2-1}\mathbf{Z} \\ \sqrt{\eta_f}\sqrt{V^2-1}\mathbf{Z} & [\eta_f(V-1)+\eta_f\xi_f+1]\mathbf{I} \end{bmatrix}, \tag{8}$$

where $\eta_f = \langle\sqrt{\eta}\rangle^2$ and $\eta_f\xi_f = \mathrm{Var}(\sqrt{\eta})(\mathrm{V}-1) + \langle\eta\xi_\eta\rangle$, with $\mathrm{Var}(\sqrt{\eta}) = \langle\eta\rangle - \langle\sqrt{\eta}\rangle^2$. According to Eq. (8), the extra non-Gaussian noise, caused by the fluctuating nature of the channel, depends on the variance of the transmissivity fluctuations $\mathrm{Var}(\sqrt{\eta})$ and the modulation variance $V_A = V - 1$.

IV. COMPOSABLE FINITE-SIZE SECURITY ANALYSIS FOR FREE-SPACE CV QKD SYTEMS

Here we analyze the composable finite-size security of the no-switching CV QKD protocol implemented over free-space channels using two approaches, first by analyzing the security over all data and second by analyzing the security for each subchannel separately. We also analyze the security against both general attacks (i.e., memory-assisted attacks) and individual attacks (i.e., nonmemory attacks).

A. Security analysis over all data

1. General attacks

Based on the leftover hash lemma [58,59], the number of approximately secure bits ℓ 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 $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E')$ [58], i.e., we have $\ell \leqslant H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E') - 2\log_2(\frac{1}{2\bar{\epsilon}})$, where $\bar{\epsilon}$ comes from the leftover hash lemma. Note that N' indicates the length of Bob's string b after the parameter estimation. The chain rule for the smooth min-entropy [46] gives $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E') = H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|EC) \geqslant H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E) - \log_2|C|$, where $\log_2|C| = l_{\rm EC}$, with $l_{\rm EC}$ the size of data leakage during the error correction. Note that the leakage during the error correction can be given by $l_{\rm EC} = N'[H(b) - \beta I(a{:}b)]$ [46,51,60], where $H(b)$ is Bob's Shannon entropy. In order to calculate the length ℓ of the final key which is ϵ-secure ($\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor}$ [46,51]), the conditional smooth min-entropy $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E)$ 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, where every signal transmitted is attacked with the same quantum operation, the asymptotic equipartition property [46,61,62] can be utilized to lower bound the conditional smooth min-entropy with the conditional von Neumann entropy. Explicitly, we have $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E) \geqslant N'\mathcal{S}(b|E) - \sqrt{N'}\Delta_{\rm AEP}$ [46,51], where $\mathcal{S}(b|E)$ is the conditional von Neumann entropy. The conditional von Neumann entropy $\mathcal{S}(b|E)$ is given by $\mathcal{S}(b|E) = H(b) - H^{\epsilon_{\rm PE}}(b{:}E)$, where Eve's information on Bob's string b is upper bounded by $H^{\epsilon_{\rm PE}}(b{:}E)$, except with probability $\epsilon_{\rm PE}$ for a given attack [for collective attacks we have $H^{\epsilon_{\rm PE}}(b{:}E) = \chi^{\epsilon_{\rm PE}}(b{:}E)$ and for individual attacks we have $H^{\epsilon_{\rm PE}}(b{:}E) = I^{\epsilon_{\rm PE}}(b{:}E)$].

In our finite-size security analysis the assumption of collective attacks to lower bound the conditional smooth min-entropy comes with no loss of generality because, based on the Gaussian de Finetti reduction, for the security analysis of the no-switching protocol against general attacks, it is sufficient to consider Gaussian collective attacks in the composable finite-size security proof [39,40].

The covariance matrix of the non-Gaussian ensemble-average state $\mathbf{M}_{AB_1}$ can be described by the effective Gaussian parameters η_f and ξ_f. Therefore, a fading-channel attack can be effectively considered as a Gaussian attack with the parameters η_f and ξ_f. For the security analysis over the whole data set we can consider an optimal Gaussian collective attack with the parameters η_f and ξ_f to minimize the key rate. In this optimal attack Eve interacts individually with each transmitted signal through an optimal entangling cloner attack [63] with the parameters η_f and ξ_f, with her output ancillae stored in her quantum memory to be collectively measured later. Since this attack is independent and identically distributed over all subchannels, the conditional smooth min-entropy can be lower bounded by the conditional von Neumann entropy. Thus, the lower bound on the total finite-size key rate with security parameter ϵ against Gaussian collective attacks is given by

$$\mathrm{KR}^{\rm col} = \frac{N'}{N}[\beta I(a{:}b) - \chi^{\epsilon_{\rm PE}}(b{:}E)] - \frac{\sqrt{N'}}{N}\Delta_{\rm AEP} - \frac{2}{N}\log_2\left(\frac{1}{2\bar{\epsilon}}\right). \tag{9}$$

Note that we assume that N_s is the number of signals transmitted over each subchannel, from which k_s signals are revealed for the parameter estimation and $N_s' = N_s - k_s$ signals are used for the key generation. In total, a number of N signal states are transmitted, from which k signals are revealed over all subchannels for the parameter estimation and $N' = N - k$ signals are used for the key generation. Note that in Eq. (9), $I(a{:}b)$ is calculated based on the effective parameters η_f and ξ_f and Eve's information from a collective attack $\chi^{\epsilon_{\rm PE}}(b{:}E)$ is calculated based on the covariance matrix $\mathbf{M}_{AB_1}$ of the ensemble-average state. For this covariance matrix, the effective excess noise ξ_f can be estimated based on a relatively large number of signals k (where $k \gg k_s$) revealed over all subchannels (see Sec. IV C). Note that for the no-switching protocol, proving the security against Gaussian collective attacks with security parameter ϵ results in the security of the same protocol against general attacks with security parameter $\tilde{\epsilon} \gg \epsilon$, where we have $\tilde{\epsilon}/\epsilon = K^4/50$. Note that $K \sim N''$, where $N'' = N' - m$, with m the number of signals used for the energy test [39]. Thus, the lower bound on the total finite-size key rate with security parameter $\tilde{\epsilon}$ against general attacks is given by

$$\mathrm{KR}^{\rm gen} = \frac{N''}{N}[\beta I(a{:}b) - \chi^{\epsilon_{\rm PE}}(b{:}E)] - \frac{\sqrt{N''}}{N}\Delta_{\rm AEP} - \frac{2}{N}\log_2\left(\frac{1}{2\bar{\epsilon}}\right) - \frac{2}{N}\log_2\binom{K+4}{4}, \tag{10}$$

where $\Delta_{\rm AEP}$ is calculated using Eq. (2) with N' being replaced by N''.

2. Individual attacks

Considering the fact that in reality Eve has access to a restricted quantum memory with limited coherence time, where each state stored in her quantum memory undergoes a specific amount of decoherence over the storage time, individual attacks might be more beneficial for Eve than collective attacks [41]. In terms of the interaction with the transmitted signals, an individual attack is the same as a collective attack, while in terms of the measurement Eve performs an individual measurement instead of a collective measurement. Among

individual attacks, Gaussian attacks are also known to be optimal for the Gaussian CV QKD protocols.

For the security analysis over all data against Gaussian individual attacks, we can also consider an optimal Gaussian individual attack with the parameters η_f and ξ_f. In this attack Eve interacts individually with each signal sent from Alice to Bob with the effective parameters η_f and ξ_f,[3] with an individual measurement on her output ancillary state as soon as she obtains it. Note that in the no-switching CV QKD protocol Eve does not need a quantum memory to perform the individual measurement, since there is no basis information withheld in this protocol. This individual attack is also independent and identically distributed over all subchannels, which means the conditional smooth min-entropy can be lower bounded by the conditional von Neumann entropy. Thus, the lower bound on the total finite-size key rate with security parameter ϵ against Gaussian individual attacks can also be given by Eq. (9), where $\chi^{\epsilon_{\rm PE}}(b{:}E)$ must be replaced by $I^{\epsilon_{\rm PE}}(b{:}E)$. Note that $I^{\epsilon_{\rm PE}}(b{:}E)$ has to be calculated based on the effective parameters of the channel, i.e., η_f and ξ_f.

B. Security analysis for each subchannel separately

For the security analysis against collective attacks with the security parameter ϵ ($\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor}$), one could also write $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E) = \sum_i H_{\min}^{\epsilon_{\rm sm},i}(b^{N'_s}|E)$, where $H_{\min}^{\epsilon_{\rm sm},i}(b^{N'_s}|E)$ is the conditional smooth min-entropy for the subchannel i with the parameters η_i and ξ_{η_i}, occurring with probability p_i, and we have $\epsilon_{{\rm sm},i} = p_i\epsilon_{\rm sm}$ and $N'_s = p_i N'$. By considering an optimal Gaussian collective attack with the parameters η_i and ξ_{η_i} over the subchannel, one can lower bound $H_{\min}^{\epsilon_{\rm sm},i}(b^{N'_s}|E)$ by the conditional von Neumann entropy since the attack is independent and identically distributed over the subchannel (note that this attack is not independent and identically distributed over all subchannels). More explicitly, one can analyze the security for each subchannel separately, i.e., calculate the composable finite-size key length for each subchannel with the security parameter ϵ_i (where $\epsilon_i = p_i\epsilon$) as $\ell_i^{\rm col} = N'_s[\beta I_i(a{:}b) - \chi_i^{\epsilon_{\rm PE},i}(b{:}E)] - \sqrt{N'_s}\Delta_{\rm AEP} - 2\log_2(\frac{1}{2\bar{\epsilon}_i})$. Note that $I_i(a{:}b)$ is the classical mutual information between Alice and Bob for the subchannel and $\chi_i^{\epsilon_{\rm PE},i}(b{:}E)$ is Eve's information from the collective attack over the subchannel, which is calculated based on the covariance matrix $\mathbf{M}_{AB_1,\eta}$ with the parameter $\epsilon_{{\rm PE},i} = p_i\epsilon_{\rm PE}$. Then the lower bound on the total finite-size key rate with the security parameter ϵ against Gaussian collective attacks is obtained by averaging over all subchannels as $\frac{1}{N}\sum_i \ell_i^{\rm col}$. Note that in a realistic finite-size regime this approach might result in pessimistic key rates. This is due to the fact that in practice only a small number of signal states are transmitted over each subchannel, which results in a very pessimistic finite key length for each subchannel, due to pessimistic error bars and the finite-size correction Δ term. Note that Eve's information $\chi_i^{\epsilon_{\rm PE},i}(b{:}E)$, which should be estimated based on a small number of signals k_s (where $k_s = p_i k$), might be overestimated (because when the block size is reduced, the error bar on the estimators of channel parameters increases, which results in estimating higher information for Eve). Note that this type of security analysis can also be used against individual attacks; however, as discussed above, the resulting key rate is expected to be pessimistic.

Note that, in practice, it would be more practical to estimate the average signal-to-noise ratio (SNR) of the free-space channel based on the whole revealed data and then choose an error-correction code rate based on this average SNR for the error correction of all the remaining data. This means the mutual information should be calculated theoretically based on the effective parameters of the channel, i.e., η_f and ξ_f. Alternatively and also ideally, it could be possible to estimate the SNR for each subchannel separately and then choose an error-correction code rate based on the subchannel SNR for the error correction of the subchannel data, which means the mutual information should be calculated theoretically by averaging over the mutual information obtained from each subchannel as $\sum_i p_i I_i(a{:}b)$. However, estimation of the SNR for each subchannel based on a small number of signals revealed for each subchannel does not give a good estimation of the SNR. Note that in our numerical simulations we calculate the mutual information based on the effective parameters η_f and ξ_f, which is a lower bound on $\sum_i p_i I_i(a{:}b)$.

C. Parameter estimation for free-space CV QKD systems

Alice and Bob are able to estimate the channel transmissivity and check its stability during the transmission of data [35,66]. This is experimentally feasible, as the typical rate of free-space channel fluctuations is of the order of kilohertz, while the modulation and detection rate is typically of the order of several megahertz, i.e., at least thousands of signal states can be transmitted during the stability time of the free-space channel [18]. The proper subchannel estimation requires a large number of states to be sent through the channel during its stability. Then some of the states for each subchannel occurrence are randomly chosen for the parameter estimation.

For instance, let us consider the free-space channel fluctuation rate of 1 kHz. Then we can assume that within each millisecond the channel is relatively stable and can be modeled with a fixed-transmissivity subchannel of transmissivity η. Let us also consider the transmission and detection rate of 100 MHz. Hence, $N_s = 10^5$ signal states can be transmitted and detected at the receiver during the stability time of the channel. A fraction of these signals ($k_s = cN_s$) can be randomly chosen to be revealed for parameter estimation, with the remaining data contributing to the secret key. Finally, for instance, for 100 seconds of data transmission we will have transmitted $N = 10^{10}$ signal states (with 10^5 signal states being transmitted during each stability time of the channel), with a fraction of which, $k = cN$, revealed over all subchannels for the parameter estimation. Then a number of $N' = N - k = (1-c)N$ signals will contribute to the shared secret key. Note that the security is not analyzed for each subchannel occurrence separately as it results in pessimistic

[3]Note that different schemes have been proposed for a Gaussian interaction in an optimal individual attack against the no-switching CV QKD protocol, with the entangling cloner being one of them [64,65].

key rates (see Sec. IV B); instead the security is shown for the ensemble-average state, being obtained from the set of data of size $N-k$ upon all subchannels.

For the security analysis over all data it is sufficient to estimate the effective parameters η_f and ξ_f of an optimal Gaussian attack. Note that for both subchannel postselection and subchannel clusterization techniques, which we discuss in the following sections, Alice and Bob are required to have a prior estimation of the transmissivity of each subchannel. We can utilize the parameter estimation method introduced for a fixed-transmissivity quantum channel in [67,68] to estimate the transmissivity of each subchannel using the data of size k_s revealed for the subchannel. For a no-switching CV QKD protocol with Bob's heterodyne detector efficiency η_B and electronic noise ν_B, for a subchannel with transmissivity η, we can consider a normal linear model for Alice's and Bob's correlated variables x_A and x_B, respectively,

$$x_B = t_s x_A + x_{n,s}, \tag{11}$$

where $t_s = \sqrt{\frac{\eta_B \eta}{2}}$ and $x_{n,s}$ follows a centered normal distribution whose variance is determined from the observed data as $\sigma_s^2 = 1 + \nu_B + \frac{\eta_B}{2}\eta\xi_\eta$ (note that Alice's variable x_A has the variance V_A). Using the revealed data of size k_s for the subchannel, the maximum-likelihood estimators for the subchannel parameters t_s and σ_s^2 are given by [67,68]

$$\hat{t}_s = \frac{\sum_{i=1}^{k_s} A_i B_i}{\sum_{i=1}^{k_s} A_i^2},$$
$$\hat{\sigma}_s^2 = \frac{1}{k_s}\sum_{i=1}^{k_s}(B_i - \hat{t}_s A_i)^2, \tag{12}$$

where A_i and B_i are the realizations of x_A and x_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

$$\Delta(t_s) = z_{\epsilon_{\rm PE}/2}\sqrt{\frac{\hat{\sigma}_s^2}{k_s V_A}}. \tag{13}$$

The estimator of the square root of subchannel transmissivity and its error bar are then given by

$$\widehat{\sqrt{\eta}} = \frac{\sqrt{2}\hat{t}_s}{\sqrt{\hat{\eta}_B}},$$
$$\Delta(\sqrt{\eta}) = \widehat{\sqrt{\eta}}\sqrt{\left|\frac{\Delta(t_s)}{\hat{t}_s}\right|^2 + \left|\frac{\Delta(\eta_B)}{2\hat{\eta}_B}\right|^2}, \tag{14}$$

where $\hat{\eta}_B$ is the estimator of Bob's detector efficiency with uncertainty $\Delta(\eta_B)$. Having the estimation of $\widehat{\sqrt{\eta}}$ for each subchannel, the estimation of the effective transmissivity is given by averaging $\widehat{\sqrt{\eta}}$ over all subchannels as $\hat{\eta}_f = \widehat{\langle\sqrt{\eta}\rangle}^2$. The estimator of the subchannel transmissivity and its error bar are also given by

$$\hat{\eta} = \frac{2\hat{t}_s^2}{\hat{\eta}_B},$$
$$\Delta(\eta) = \hat{\eta}\sqrt{\left|\frac{2\Delta(t_s)}{\hat{t}_s}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2}, \tag{15}$$

Having the estimations of $\widehat{\sqrt{\eta}}$ and $\hat{\eta}$ for each subchannel, the estimation of the variance of transmissivity is given by $\widehat{\mathrm{Var}(\sqrt{\eta})} = \langle\hat{\eta}\rangle - \widehat{\langle\sqrt{\eta}\rangle}^2$.

The next step is to estimate the effective excess noise ξ_f, which according to Eq. (8) requires the estimation of both $\mathrm{Var}(\sqrt{\eta})$ and $\langle\eta\xi_\eta\rangle$. Here we generalize the above-discussed parameter estimation method to the data of size k revealed over all subchannels to estimate $\langle\eta\xi_\eta\rangle$. Considering Eq. (11) over all subchannels, we can still have a normal linear model for Alice's and Bob's correlated variables as

$$x_B = t x_A + x_n, \tag{16}$$

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

$$\hat{t} = \frac{\sum_{i=1}^{k} A_i B_i}{\sum_{i=1}^{k} A_i^2},$$
$$\hat{\sigma}^2 = \frac{1}{k}\sum_{i=1}^{k}(B_i - \hat{t}A_i)^2. \tag{17}$$

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

$$\Delta(t) = z_{\epsilon_{\rm PE}/2}\sqrt{\frac{\hat{\sigma}^2}{kV_A}},$$
$$\Delta(\sigma^2) = z_{\epsilon_{\rm PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{k}}. \tag{18}$$

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 $\sigma_0^2 = 1 + \nu_B$, which is Bob's shot-noise variance. The maximum-likelihood estimator for σ_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 $\Delta(\sigma_0^2) = z_{\epsilon_{\rm PE}/2}\frac{\hat{\sigma}_0^2\sqrt{2}}{\sqrt{N}}$.[4] Now we can estimate $\langle\eta\rangle$ and $\langle\eta\xi_\eta\rangle$, which are given by

$$\widehat{\langle\eta\rangle} = \frac{2\hat{t}^2}{\hat{\eta}_B},$$
$$\Delta(\langle\eta\rangle) = \widehat{\langle\eta\rangle}\sqrt{\left|\frac{2\Delta(t)}{\hat{t}}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2},$$
$$\widehat{\langle\eta\xi_\eta\rangle} = 2\frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{\eta}_B},$$
$$\Delta(\langle\eta\xi_\eta\rangle) = \widehat{\langle\eta\xi_\eta\rangle}\sqrt{\left|\frac{\Delta(\sigma^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\sigma_0^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2}. \tag{19}$$

[4]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.

Note that in order to maximize Eve's information from collective and individual attacks, the worst-case estimators of the effective parameters η_f and ξ_f should be used to evaluate Eve's information. Now, having Eqs. (14), (15), and (19), the worst-case estimators of the effective parameters η_f and ξ_f are given by

$$\begin{aligned}\hat{\eta}_f &= \langle \min[\sqrt{\eta}]\rangle^2 = \langle \widehat{\sqrt{\eta}} - \Delta(\sqrt{\eta})\rangle^2,\\ \widehat{\eta_f\xi_f} &= \max[\mathrm{Var}(\sqrt{\eta})]V_A + \max[\langle \eta\xi_\eta\rangle]\\ &= [\langle \hat{\eta} + \Delta(\eta)\rangle - \langle \widehat{\sqrt{\eta}} - \Delta(\sqrt{\eta})\rangle^2]V_A\\ &\quad + \widehat{\langle \eta\xi_\eta\rangle} + \Delta(\langle \eta\xi_\eta\rangle). \end{aligned} \tag{20}$$

V. CLASSICAL POSTPROCESSING STRATEGIES TO IMPROVE FREE-SPACE CV QKD SYSTEMS

If we compare a fluctuating channel with an equivalent fixed-transmissivity channel with transmissivity $\eta_f = \langle\sqrt{\eta}\rangle^2$ and excess noise $\langle\eta\xi_\eta\rangle$, the fluctuating channel has an extra non-Gaussian noise of $\mathrm{Var}(\sqrt{\eta})(V-1)$ [see Eq. (8)], which reduces the key rate. Although fluctuating transmissivity of a free-space channel reduces the key rate, it also provides the possibility to improve or even recover it through the postselection of subchannels with high transmissivity [18] or the clusterization of subchannels [35,36].

In the postselection technique as introduced in [18], the data collected for each subchannel is kept, conditioned on the estimated subchannel transmissivity being larger than a postselection threshold η_{th}, and discarded otherwise. In this technique, the security should be analyzed over the postselected data. With such a postselection, the postselected data become more Gaussian and more strongly correlated, since the postselection reduces the fluctuation variance of the channel, while increases the average transmissivity of the channel.

In the clusterization technique as introduced in [35], for the classical postprocessing, Alice and Bob partition their data into n different clusters and perform classical postprocessing (including reconciliation and privacy amplification) over each cluster separately. The clusterization we consider here is such that the jth cluster ($j = 1, 2, \ldots, n$) corresponds to the jth channel transmissivity bin $(j-1)\delta < \eta < j\delta$, with the bin size $\delta = \frac{\eta_{\max}}{n}$. Note that the clusterization we consider here is the uniform binning of the probability distribution; however, in principle, the width of each cluster can be optimized depending on the probability distribution. With such a technique, the data within each cluster become more Gaussian, since the fluctuation variance of the channel is reduced within each cluster.

The postselection has been shown to improve the free-space CV QKD performance in terms of the key rate in the asymptotic regime against Gaussian collective attacks [18,32] and the clusterization has been shown to improve the key rate in the asymptotic and finite-size regime against Gaussian collective attacks [35,36], but none of them has been analyzed in a composable finite-size security regime. However, both postselection and clusterization reduce the size of the data set used for the security analysis and the size of the data set used for the parameter estimation. Hence, the composable finite-size effects become more significant in these scenarios. In the following sections we investigate the effectiveness of the postselection and clusterization in the composable finite-size regime against both individual and collective attacks (where the security against general attacks can be obtained by the security against collective attacks with a larger security parameter).

A. Composable finite-size security analysis for the postselection

In the finite-size regime, the size of the postselected data set is $N_{\mathrm{ps}} = P_s N$, where P_s is the postselection success probability, i.e., the total probability for the channel transmissivity to fall within the postselected region $\eta \geqslant \eta_{\mathrm{th}}$, and is given by $P_s = \int_{\eta_{\mathrm{th}}}^{\eta_{\max}} p(\eta)d\eta$. Note that since in the postselection protocol Eve's information should be estimated based on the postselected data, Alice and Bob can only use the revealed data over the postselected subchannels to estimate the covariance matrix of the postselected ensemble-average state, which means a data set of size $k_{\mathrm{ps}} = P_s k$ is used for the parameter estimation. Recall that k is the amount of revealed data over all subchannels. Hence, the data set of size $N'_{\mathrm{ps}} = N_{\mathrm{ps}} - k_{\mathrm{ps}}$ contributes to the postselected key. Explicitly, the finite-size key length of the postselection protocol which is ϵ-secure against Gaussian collective attacks in the reverse reconciliation scenario is given by

$$\begin{aligned}\ell^{\mathrm{col}}_{\mathrm{ps}} \leqslant N'_{\mathrm{ps}}[\beta I_{\mathrm{ps}}(a{:}b) - \chi^{\epsilon_{\mathrm{PE}}}_{\mathrm{ps}}(b{:}E)]\\ - \sqrt{N'_{\mathrm{ps}}}\Delta_{\mathrm{AEP}} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right).\end{aligned} \tag{21}$$

Eve's information from the Gaussian collective attack in the postselection protocol is calculated based on the covariance matrix of the postselected ensemble-average state $\rho^{\mathrm{ps}}_{AB_1}$, which is given by

$$\begin{aligned}\mathbf{M}^{\mathrm{ps}}_{AB_1} &= \begin{bmatrix} V\mathbf{I} & \sqrt{\eta^{\mathrm{ps}}_f}\sqrt{V^2-1}\mathbf{Z}\\ \sqrt{\eta^{\mathrm{ps}}_f}\sqrt{V^2-1}\mathbf{Z} & \left[\eta^{\mathrm{ps}}_f(V-1)+\eta^{\mathrm{ps}}_f\xi^{\mathrm{ps}}_f+1\right]\mathbf{I}\end{bmatrix},\\ \eta^{\mathrm{ps}}_f &= \langle\sqrt{\eta}\rangle^2_{\mathrm{ps}},\\ \eta^{\mathrm{ps}}_f\xi^{\mathrm{ps}}_f &= \mathrm{Var}_{\mathrm{ps}}(\sqrt{\eta})(\mathrm{V}-1) + \langle\eta\xi_\eta\rangle_{\mathrm{ps}},\\ \mathrm{Var}_{\mathrm{ps}}(\sqrt{\eta}) &= \langle\eta\rangle_{\mathrm{ps}} - \langle\sqrt{\eta}\rangle^2_{\mathrm{ps}},\end{aligned} \tag{22}$$

where $\langle\cdot\rangle_{\mathrm{ps}}$ denotes the mean value over the postselected subchannels, i.e.,

$$\begin{aligned}\langle\eta\rangle_{\mathrm{ps}} &= \frac{1}{P_s}\int_{\eta_{\mathrm{th}}}^{\eta_{\max}} \eta p(\eta)d\eta,\\ \langle\sqrt{\eta}\rangle_{\mathrm{ps}} &= \frac{1}{P_s}\int_{\eta_{\mathrm{th}}}^{\eta_{\max}} \sqrt{\eta}p(\eta)d\eta,\\ \langle\eta\xi_\eta\rangle_{\mathrm{ps}} &= \frac{1}{P_s}\int_{\eta_{\mathrm{th}}}^{\eta_{\max}} \eta\xi_\eta p(\eta)d\eta.\end{aligned} \tag{23}$$

Similarly, the finite-size key length of the postselection protocol which is ϵ-secure against Gaussian individual attacks in the reverse reconciliation scenario is given by

$$\begin{aligned}\ell^{\mathrm{ind}}_{\mathrm{ps}} \leqslant N'_{\mathrm{ps}}[\beta I_{\mathrm{ps}}(a{:}b) - I^{\epsilon_{\mathrm{PE}}}_{\mathrm{ps}}(b{:}E)]\\ - \sqrt{N'_{\mathrm{ps}}}\Delta_{\mathrm{AEP}} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right),\end{aligned} \tag{24}$$

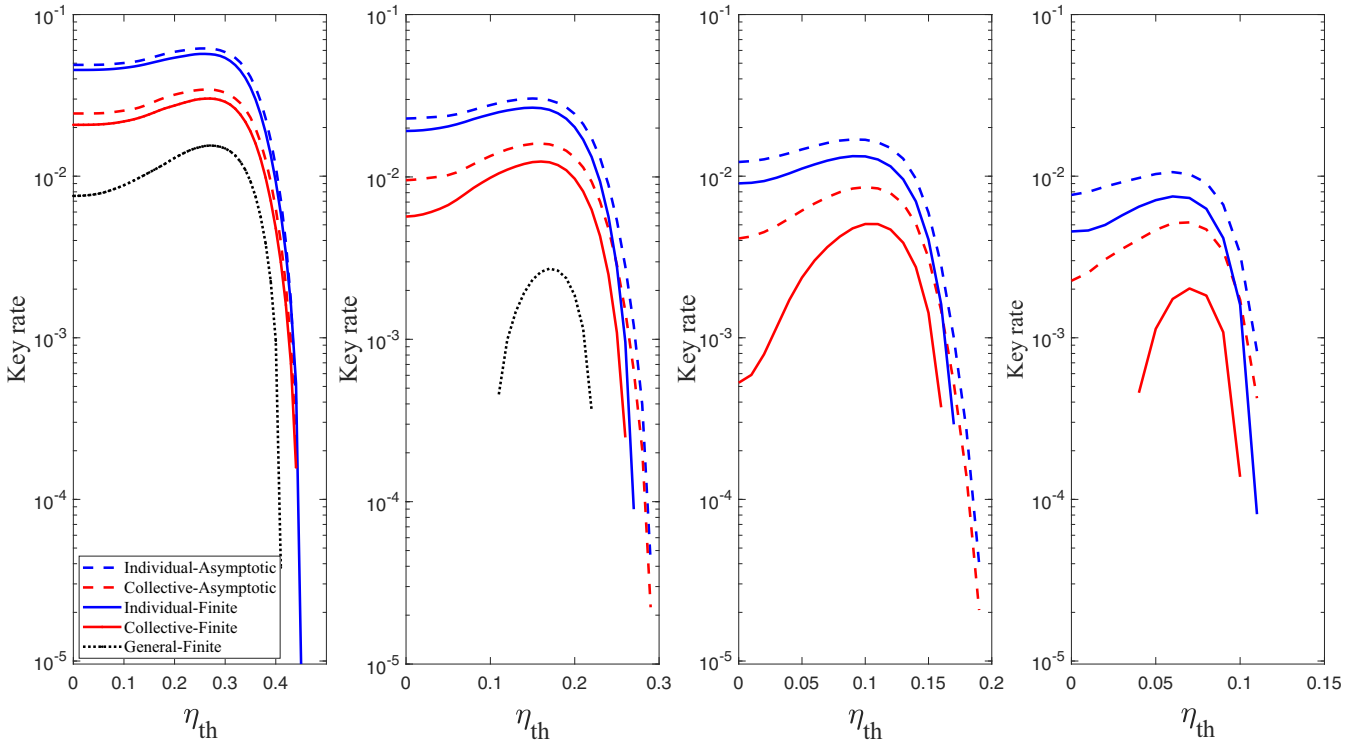

FIG. 1. Postselected key rate (in bits per mode) in the asymptotic (dashed lines) and composable finite-size (solid and dotted lines) regime as a function of the postselection threshold $\eta_{\rm th}$, secure against individual (blue top lines), collective (red middle lines), and general (black dotted bottom lines) attacks. Note that in the asymptotic regime collective attacks are as powerful as general attacks. Note also that for the free-space channels in the two right plots the protocol is not secure against general attacks in the composable finite-size regime. The numerical values for the finite-size regime are the security parameter $\epsilon = 10^{-9}$ ($\bar{\epsilon} = 10^{-9}$ for general attacks) and the discretization parameter $d = 5$. The other parameters are chosen from the most recent CV QKD experiment [17] as follows. Bob's detector has efficiency $\eta_B = 0.6$ and electronic noise $\nu_B = 0.25$. The reconciliation efficiency is considered to be $\beta = 0.98$. The expected excess noise of each subchannel is assumed to be fixed as $\xi = 0.01$. (Note that, although in our numerical simulations we have assumed a fixed excess noise for each subchannel, our parameter estimation presented in Sec. IV C also works for the case of fluctuating excess noise.) The block size is chosen to be $N = 10^{10}$, half of which (i.e., $k = 0.5N$) is used in total for parameter estimation with $\epsilon_{\rm PE} = 10^{-10}$ ($\epsilon_{\rm PE} = 10^{-50}$ for general attacks). Note that we also use a subset of data of size $m = 0.1N$ for the energy test required for security analysis against general attacks. Since the non-Gaussian noise [i.e., the term $\mathrm{Var}(\sqrt{\eta})(\mathrm{V}-1)$ in Eq. (8)] depends on the modulation variance, the modulation variance is optimized for each postselection threshold to maximize the key rate against a given attack. We consider a probability distribution for the free-space channel given by the elliptic-beam model (see Appendix C for more details on the model). From left to right we have the average $\langle\eta\rangle = 0.32, 0.19, 0.12, 0.08$, $\langle\sqrt{\eta}\rangle = 0.56, 0.43, 0.34, 0.27$, the variance $\mathrm{Var}(\sqrt{\eta}) = 0.005, 0.004, 0.003, 0.002$, and the maximum transmissivity $\eta_{\max} = 0.46, 0.30, 0.20, 0.13$ [see Fig. 3 in Appendix C for the corresponding probability distributions $p(\eta)$].

where Eve's information from the Gaussian individual attack in the postselection protocol has to also be calculated based on the effective parameters $\eta_f^{\rm ps}$ and $\xi_f^{\rm ps}$. Note that Eve's information $\chi_{\rm ps}^{\epsilon_{\rm PE}}(b{:}E)$ and $I_{\rm ps}^{\epsilon_{\rm PE}}(b{:}E)$ should be calculated based on the worst-case estimators of the effective parameters $\eta_f^{\rm ps}$ and $\xi_f^{\rm ps}$. These worst-case estimators can be calculated using Eq. (20), where the average has to be taken over the postselected subchannels and the estimations in Eqs. (17) and (18) have to be calculated based on the revealed data over the postselected subchannels of size $k_{\rm ps}$. Note also that the classical mutual information between Alice and Bob obtained from the postselection $I_{\rm ps}(a{:}b)$ is calculated based on the effective parameters $\eta_f^{\rm ps}$ and $\xi_f^{\rm ps}$, and $\Delta_{\rm AEP}$ is calculated using Eq. (2) with N' being replaced by $N'_{\rm ps}$. Finally, the finite-size key rate of the postselection protocol is given by $\ell_{\rm ps}^{\rm col}/N$ against collective attacks and by $\ell_{\rm ps}^{\rm ind}/N$ against individual attacks. See Appendix A for the detailed calculation of Eve's information and Alice and Bob's mutual information.

Note that the postselection of high-transmissivity subchannels has two different effects on the finite-size key rate. On the positive side the postselection makes the ensemble-average state more Gaussian and more strongly correlated, while on the negative side the postselection reduces the key block size and also makes the error bars larger in the parameter estimation.

As discussed earlier in Sec. IV C, Alice and Bob can estimate the transmissivity of each subchannel by revealing a fraction of the data allocated to each subchannel. In the postselection protocol, based on such an estimation of subchannel transmissivity, they decide to keep or discard the subchannel data. Note that the subchannel transmissivity can be estimated using different schemes, e.g., by transmitting auxiliary coherent (classical) light probe signals that are intertwined

with the quantum information [42,43] or by monitoring the local oscillator at the receiver, where the signal and the local oscillator have been sent in two orthogonally polarized modes through the free-space channel [44]. However, in all these scenarios Eve can manipulate the classical probe signal or the local oscillator in such a way as to gain an advantage. For instance, Eve can make Alice and Bob think the transmissivity is good and within the postselection region, when it is actually bad and not in the postselection region. In fact, Eve can make Alice and Bob postselect a particular subchannel which is not actually within their postselection region. Such a likely manipulation by Eve can result in underestimating Eve's information and overestimating the secret key rate.

Figure 1 shows the postselected key rate in both the asymptotic and composable finite-size regimes as a function of the postselection threshold $\eta_{\rm th}$, where the security is analyzed against individual, collective, and general attacks. Note that the black dotted lines in Fig. 1 show the finite-size key rate secure against general attacks. In fact, for the black dotted lines we have analyzed the security against collective attacks with the security parameter $\epsilon = 10^{-49}$ and block size $N = 10^{10}$, which according to [39] leads to the security of the protocol against general attacks with $\tilde{\epsilon} = 10^{-9}$. In this case, for the parameter estimation we use $\epsilon_{\rm PE} = 10^{-50}$, which makes $z_{\epsilon_{\rm PE}/2} \to \infty$. Because of this divergence, for general attacks we use the parameter estimation discussed in Appendix B. Note that for the free-space channels with $\langle\eta\rangle = 0.12, 0.08$ (the two right plots of Fig. 1) the protocol is not secure against general attacks in the composable finite-size regime even with a strong postselection. As can be seen for both asymptotic and finite-size regimes, the key rate resulting from all types of attacks first improves up to an optimized value, as the threshold value increases, and then the key rate decreases. As the threshold value increases, the variance of the channel fluctuations $\mathrm{Var}(\sqrt{\eta})$ decreases, while the effective channel transmission coefficient $\langle\sqrt{\eta}\rangle$ increases. As a result, the postselected state becomes more Gaussian (i.e., with less non-Gaussian noise) and more strongly correlated, which increases the mutual information between Alice and Bob. However, this increase in the mutual information happens at the cost of lower success probability P_s and larger error bars for the estimated parameters. Hence, there is an optimal threshold value which maximizes the postselected key rate. As can be seen, from left to right, the postselection becomes more effective. In fact, this type of postselection is more useful for recovering the key rate in cases where it was strongly diminished by the free-space channel. Figure 1 also shows the significant improvement of the finite-size key rate from collective attacks due to the postselection compared to the asymptotic regime. While without the postselection positive finite key rates cannot be generated against collective attacks (general attacks) for $\langle\eta\rangle = 0.08$ (for $\langle\eta\rangle = 0.19$), by performing the postselection beyond $\eta_{\rm th} = 0.04$ ($\eta_{\rm th} = 0.11$), Alice and Bob are able to move from an insecure regime to a secure regime and generate nontrivial positive finite key rates.

B. Composable finite-size security analysis for the clusterization

For the clusterization technique, in order to compute the key rate with security parameter ϵ (where $\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor}$), the conditional smooth min-entropy $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E)$ can be written as the sum of the conditional smooth min-entropy of n different clusters of data, i.e., $H_{\min}^{\epsilon_{\rm sm}}(b^{N'}|E) = \sum_{j=1}^{n} H_{\min}^{\epsilon_{{\rm sm},j}}(b^{N'_j}|E)$, where $N'_j = P_j N'$, with $P_j = \int_{\frac{(j-1)\eta_{\max}}{n}}^{\frac{j\eta_{\max}}{n}} p(\eta)d\eta$ the probability for the channel transmissivity to fall within the jth cluster, and $\epsilon_{{\rm sm},j} = P_j\epsilon_{\rm sm}$. Note that for each cluster Eve's optimal attack can be considered as an independent and identically distributed Gaussian attack with the effective parameters η_f^j and ξ_f^j given by

$$\begin{aligned}\eta_f^j &= \langle\sqrt{\eta}\rangle_j^2,\\ \eta_f^j\xi_f^j &= \mathrm{Var}_j(\sqrt{\eta})(V-1) + \langle\eta\xi_\eta\rangle_j,\\ \mathrm{Var}_j(\sqrt{\eta}) &= \langle\eta\rangle_j - \langle\sqrt{\eta}\rangle_j^2,\end{aligned} \tag{25}$$

where $\langle\cdot\rangle_j$ denotes the mean value over all subchannels within the jth cluster, i.e.,

$$\begin{aligned}\langle\eta\rangle_j &= \frac{1}{P_j}\int_{\frac{(j-1)\eta_{\max}}{n}}^{\frac{j\eta_{\max}}{n}} \eta p(\eta)d\eta,\\ \langle\sqrt{\eta}\rangle_j &= \frac{1}{P_j}\int_{\frac{(j-1)\eta_{\max}}{n}}^{\frac{j\eta_{\max}}{n}} \sqrt{\eta}p(\eta)d\eta,\\ \langle\eta\xi_\eta\rangle_j &= \frac{1}{P_j}\int_{\frac{(j-1)\eta_{\max}}{n}}^{\frac{j\eta_{\max}}{n}} \eta\xi_\eta p(\eta)d\eta.\end{aligned} \tag{26}$$

Since the attack can be considered independent and identically distributed over each cluster, we can lower bound $H_{\min}^{\epsilon_{{\rm sm},j}}(b^{N'_j}|E)$ with the conditional von Neumann entropy and compute the key length with security parameter $\epsilon_j = P_j\epsilon$ for the jth cluster as $\ell_j^{\rm col} = P_jN'[\beta I_j(a{:}b) - \chi_j^{\epsilon_{{\rm PE},j}}(b{:}E)] - \sqrt{P_jN'}\Delta_{\rm AEP} - 2\log_2(\frac{1}{2\bar{\epsilon}_j})$ against collective attacks and $\ell_j^{\rm ind} = P_jN'[\beta I_j(a{:}b) - I_j^{\epsilon_{{\rm PE},j}}(b{:}E)] - \sqrt{P_jN'}\Delta_{\rm AEP} - 2\log_2(\frac{1}{2\bar{\epsilon}_j})$ against individual attacks, where $I_j(a{:}b)$ is the classical mutual information between Alice and Bob for the jth cluster calculated based on the effective parameters η_f^j and ξ_f^j; $\chi_j^{\epsilon_{{\rm PE},j}}(b{:}E)$ is Eve's information from the collective attack over the jth cluster, which is calculated based on the covariance matrix $\mathbf{M}_{AB_1}^j$,

$$\mathbf{M}_{AB_1}^j = \begin{bmatrix} V\mathbf{I} & \sqrt{\eta_f^j}\sqrt{V^2-1}\mathbf{Z} \\ \sqrt{\eta_f^j}\sqrt{V^2-1}\mathbf{Z} & \left[\eta_f^j(V-1) + \eta_f^j\xi_f^j + 1\right]\mathbf{I}\end{bmatrix}; \tag{27}$$

and $I_j^{\epsilon_{{\rm PE},j}}(b{:}E)$ is Eve's information from individual attack over the jth cluster, which is calculated based on the effective parameters η_f^j and ξ_f^j. Note that Eve's information $\chi_j^{\epsilon_{{\rm PE},j}}(b{:}E)$ and $I_j^{\epsilon_{{\rm PE},j}}(b{:}E)$ is now estimated based on the worst-case estimators of the effective parameters η_f^j and ξ_f^j. These worst-case estimators can be calculated using Eq. (20), where the average has to be taken over the subchannels within cluster j and the estimations in Eqs. (17) and (18) have to be calculated based on the revealed data over cluster j of size P_jk, with the maximum failure probability $\epsilon_{{\rm PE},j} = P_j\epsilon_{\rm PE}$. Note also that $\Delta_{\rm AEP}$ is calculated using Eq. (2) with N' being replaced by P_jN', and $\Delta_{\rm AEP}$ is now calculated based on the parameters ϵ_j, $\epsilon_{{\rm sm},j}$, and $\bar{\epsilon}_j = P_j\bar{\epsilon}$. The total key rate with security parameter

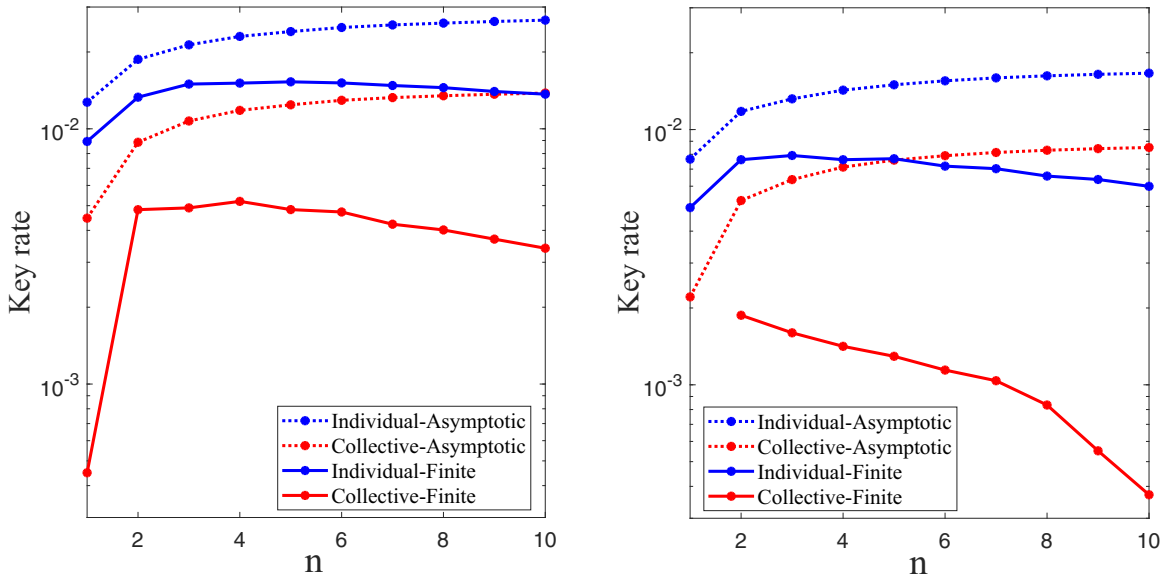

FIG. 2. Key rate (in bits per mode) in the asymptotic regime (circular points on dotted lines) secure against individual (blue top lines) and collective (red bottom lines) attacks and composable finite-size regime (circular points on solid lines) secure against individual (blue top lines) and collective (red bottom lines) attacks, as a function of the number of clusters n. The numerical values are the same as in Fig. 1. From left to right we have the average $\langle\eta\rangle = 0.12, 0.08$, $\langle\sqrt{\eta}\rangle = 0.34, 0.27$, the variance $\mathrm{Var}(\sqrt{\eta}) = 0.003, 0.002$, and the maximum transmissivity $\eta_{\max} = 0.20, 0.13$.

ϵ is then given by $\frac{1}{N}\sum_{j=1}^{n} \ell_j^{\mathrm{col}}$ against collective attacks and by $\frac{1}{N}\sum_{j=1}^{n} \ell_j^{\mathrm{ind}}$ against individual attacks.

Figure 2 shows the key rate in both the asymptotic and composable finite-size regimes secure against collective and individual attacks as a function of the number of clusters n. Note that $n = 1$ indicates no clusterization, where security is analyzed over all data. As can be seen, clusterization always increases the asymptotic key rate against collective and individual attacks. However, by considering composable finite-size effects in the security analysis, there is an optimal number of clusters which maximizes the key rate. In fact, as the number of clusters increases, the variance of channel fluctuation within each cluster decreases. As a result, the non-Gaussian noise becomes smaller for each cluster, which makes the state obtained over each cluster more Gaussian. However, as the number of clusters increases, the number of signals for each cluster decreases. As a result, the composable finite-size effects (i.e., the effect of the Δ term and the effect of parameter estimation, which is now performed based on $P_j k$ signals with $\epsilon_{\mathrm{PE},j}$) become more significant, which reduces the key rate. Figure 2 shows that while for $\langle\eta\rangle = 0.08$, without clusterization (i.e., $n = 1$), the protocol is not secure against collective attacks in the composable finite-size regime, if Alice and Bob perform clusterization as described above, the protocol becomes secure against collective attacks and the finite key rate is maximized for $n = 2$. Note that when the number of clusters n becomes sufficiently large, the security analysis is performed as if the security is analyzed over each subchannel separately (as described in Sec. IV B).

Note that the postselection (or clusterization) is performed based on the estimated subchannel transmissivity $\hat{\eta}$, given in Eq. (15), not the true value of transmissivity. Crucially, however, once the data are postselected (or partitioned), the key rate is calculated based upon a worst-case value of the subchannel transmissivity, as presented in the first of Eqs. (20), which takes into account the possibility that the true transmissivity is below the estimated transmissivity except with some probability ϵ_{PE}.

VI. CONCLUSION

We have analyzed the security of the no-switching CV QKD protocol over free-space channels with fluctuating transmissivity in the composable finite-size regime against both collective and individual attacks. We introduced a parameter estimation approach, where Alice and Bob can efficiently estimate the effective excess noise of an optimal Gaussian attack using the data revealed over all subchannels used for the security analysis. We analyzed two classical postprocessing strategies, the postselection of high-transmissivity subchannels and partitioning subchannels into different clusters, in the composable finite-size regime, showing that these strategies can improve the finite-size key rate against both individual and collective attacks. The most remarkable improvement is for the finite-size collective attacks, which are the most practically relevant, where we see these classical postprocessing allow significant key rates in situations that would otherwise be completely insecure.

ACKNOWLEDGMENTS

The authors gratefully acknowledge valuable discussions with Andrew Lance and Thomas Symul. This research was supported by the Australian Research Council under the Centre of Excellence for Quantum Computation and

Communication Technology (Project No. CE170100012). N.W. acknowledges funding support from the European Unions Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 750905 and Q.Link.X from the BMBF in Germany.

APPENDIX A: KEY RATE CALCULATION

1. Eve's information from a collective attack

At the output of the channel Bob applies heterodyne detection to mode B_1. Bob's heterodyne detector with efficiency η_B and electronic noise variance of ν_B can be modeled by placing a beam splitter of transmissivity η_B before an ideal heterodyne detector [69,70]. The heterodyne detector's electronic noise can be modeled by a two-mode squeezed vacuum state ρ_{F_0G} of quadrature variance υ, where $\upsilon = 1 + 2\nu_B/(1-\eta_B)$. One input port of the beam splitter is the received mode B_1, and the second input port is fed by one half of the entangled state ρ_{F_0G}, mode F_0, while the output ports are mode B_2 (which is measured by the ideal heterodyne detector) and mode F.

In a collective attack, Eve's information $\chi(b{:}E)$ is given by $\chi(b{:}E) = \mathcal{S}(\rho_E) - \mathcal{S}(\rho_{E|B})$, where $\mathcal{S}(\rho)$ is the von Neumann entropy of the state ρ. Here we assume Bob's detection noise is not accessible to Eve. In this case $\mathcal{S}(\rho_E) = \mathcal{S}(\rho_{AB_1})$, where the entropy $\mathcal{S}(\rho_{AB_1})$ can be calculated through the symplectic eigenvalues $\nu_{1,2}$ of covariance matrix[5] $\mathbf{M}_{AB_1}$ in Eq. (8). The second entropy we require in order to determine $\chi(b{:}E)$ can be written as $\mathcal{S}(\rho_{E|B}) = \mathcal{S}(\rho_{E|B_2}) = \mathcal{S}(\rho_{AFG|B_2})$. The covariance matrix of the conditional state $\rho_{AFG|B_2}$ is given by $\mathbf{M}_{AFG|B_2} = \mathbf{M}_{AFG} - \boldsymbol{\sigma}_{AFG,B_2}\mathbf{H}_{\text{het}}\boldsymbol{\sigma}^T_{AFG,B_2}$, where $\mathbf{H}_{\text{het}} = (\mathbf{M}_{B_2} + \mathbf{I})^{-1}$, with $\mathbf{M}_{B_2} = V_{B2}\mathbf{I}$, where

$$V_{B2} = \eta_B[\eta_f(V-1) + \eta_f\xi_f + 1] + (1-\eta_B)\upsilon. \tag{A1}$$

Note that the matrices $\mathbf{M}_{AFG}$, $\boldsymbol{\sigma}_{AFG,B_2}$, and $\mathbf{M}_{B_2}$ can be derived from the decomposition of the covariance matrix

$$\mathbf{M}_{AFGB_2} = \begin{bmatrix} \mathbf{M}_{AFG} & \boldsymbol{\sigma}_{AFG,B_2} \\ \boldsymbol{\sigma}^T_{AFG,B_2} & \mathbf{M}_{B_2} \end{bmatrix}. \tag{A2}$$

Note that the covariance matrix $\mathbf{M}_{AFGB_2}$ is given by $\mathbf{M}_{AFGB_2} = (\mathbf{I}_A \oplus \mathbf{S}_{\text{bs}} \oplus \mathbf{I}_G)^T[\mathbf{M}_{AB_1} \oplus \mathbf{M}_{F_0G}](\mathbf{I}_A \oplus \mathbf{S}_{\text{bs}} \oplus \mathbf{I}_G)$, where $\mathbf{S}_{\text{bs}}$ is the matrix for the beam-splitter transformation (applied on modes B_1 and F_0), given by

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

and the covariance matrix of the entangled state ρ_{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 in the finite-size regime, $\chi^{\epsilon_{\text{PE}}}(b{:}E)$ should be calculated based on the worst-case estimators of η_f and ξ_f. Note also that for the postselection protocol, the parameters η_f and ξ_f have to be replaced by the postselection parameters η_f^{ps} and ξ_f^{ps} from Eq. (22), and for the clusterization, the parameters η_f and ξ_f have to be replaced by the cluster parameters η_f^j and ξ_f^j from Eq. (25).

[5]The von Neumann entropy of an n-mode Gaussian state ρ with the covariance matrix $\mathbf{M}$ is given by $\mathcal{S}(\rho) = \sum_{i=1}^{n} G(\frac{\nu_i - 1}{2})$, where ν_i are the symplectic eigenvalues of the covariance matrix $\mathbf{M}$ and $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$.

2. Eve's information from an individual attack

Considering a free-space channel with effective parameters η_f and ξ_f, defined in Eq. (8), in the individual attack, Eve's information $I(b{:}E)$ is given by $I(b{:}E) = \log_2 \frac{V_{B_2^{\text{het}}}}{V_{B_2^{\text{het}}|E}}$ [64,65], where $V_{B_2^{\text{het}}}$ is the variance of heterodyne-detected mode B_2 and is given by $V_{B_2^{\text{het}}} = (V_{B2}+1)/2$, where V_{B2} is given in Eq. (A1). Note that $V_{B_2^{\text{het}}|E}$ in the case of Bob's detection noise not being accessible to Eve is given by $V_{B_2^{\text{het}}|E} = \eta_B[\frac{V x_E + 1}{V + x_E} + \chi_{\text{het}}]/2$, where $x_E = \eta_f(2 - \xi_f)^2/(\sqrt{2 - 2\eta_f + \eta_f\xi_f} + \sqrt{\xi_f})^2 + 1$ and $\chi_{\text{het}} = [1 + (1 - \eta_B) + 2\nu_B]/\eta_B$. Note that in the finite-size regime, $I^{\epsilon_{\text{PE}}}(b{:}E)$ should be calculated based on the worst-case estimators of η_f and ξ_f. Note also that the parameters η_f and ξ_f have to be replaced by the parameters η_f^{ps} and ξ_f^{ps} from Eq. (22) for the postselection protocol and by the parameters η_f^j and ξ_f^j from Eq. (25) for cluster j.

3. Mutual information between Alice and Bob

The classical mutual information between Alice and Bob is given by $I(a{:}b) = \log_2 \frac{V_{B_2^{\text{het}}}}{V_{B_2^{\text{het}}|A^{\text{het}}}}$. The conditional variance $V_{B_2^{\text{het}}|A^{\text{het}}}$ is the variance of heterodyne-detected mode B_2 conditioned on Alice's heterodyne detection of mode A, which is given by $V_{B_2^{\text{het}}|A^{\text{het}}} = \eta_B\eta_f(1 + \chi_{\text{tot}})/2$, where $\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{\eta_f}$, with $\chi_{\text{line}} = \xi_f - 1 + \frac{1}{\eta_f}$. Note that for the postselected protocol, the parameters η_f and ξ_f have to be replaced by the postselection parameters η_f^{ps} and ξ_f^{ps}, and for the clusterization, the parameters η_f and ξ_f have to be replaced by the cluster parameters η_f^j and ξ_f^j.

APPENDIX B: PARAMETER ESTIMATION FOR THE SECURITY ANALYSIS AGAINST GENERAL ATTACKS

The distributions of independent estimators $\hat{t}_s$ and $\hat{\sigma}_s^2$ in Eq. (12) are

$$\hat{t}_s \sim \mathcal{N}\left(t_s, \frac{\sigma_s^2}{\sum_{i=1}^{k_s} A_i^2}\right), \quad \frac{k_s\hat{\sigma}_s^2}{\sigma_s^2} \sim \chi^2(k_s - 1). \tag{B1}$$

Now let us consider $T_s = \frac{\eta_B}{2}\eta$. Having the variance of x_A as V_A, the estimator of T_s is given by

$$\hat{T}_s = \frac{(\widehat{C_{AB}})^2}{V_A^2}, \tag{B2}$$

where we use the maximum-likelihood estimator of $\widehat{C_{AB}} = \frac{1}{k_s}\sum_{i=1}^{k_s} A_iB_i$. The variance of this estimator is given by $\text{Var}(\widehat{C_{AB}}) = \frac{T_sV_A^2}{k_s}(2 + \frac{\sigma_s^2}{T_sV_A})$ (proof in Appendix A of [71]). The next step is to calculate the variance of the estimator $\hat{T}_s$. For this reason we write $(\widehat{C_{AB}})^2 = V_{\text{cov}}\frac{(\widehat{C_{AB}})^2}{V_{\text{cov}}}$, where $V_{\text{cov}} = \text{Var}(\widehat{C_{AB}})$. Since $\frac{(\widehat{C_{AB}})^2}{V_{\text{cov}}}$ has a noncentral χ^2 distribution of

$\frac{(\widehat{C_{AB}})^2}{V_{\rm cov}} \sim \chi^2(1, \frac{C_{AB}^2}{V_{\rm cov}})$, the mean value and the variance of the estimator $\hat{T}_s$ is given by [71]

$$\begin{aligned}\mathbb{E}(\hat{T}_s) &= \frac{C_{AB}^2}{V_A^2} + \frac{V_{\rm cov}}{V_A^2} = T_s + O(1/k_s),\\ \mathrm{Var}(\hat{T}_s) &= \frac{2V_{\rm cov}^2}{V_A^4}\left(1 + 2\frac{C_{AB}^2}{V_{\rm cov}}\right)\\ &= \frac{4T_s^2}{k_s}\left(2 + \frac{\sigma_s^2}{T_s V_A}\right) + O\big(1/k_s^2\big). \end{aligned} \tag{B3}$$

According to Lemma 8 in the Appendix of [72], we have a tail bound for a noncentral χ^2 random variable $X \sim \chi^2(d, \nu)$ with d degrees of freedom and noncentrality parameter ν as, for all $x > 0$,

$$\mathrm{Prob}[X \leqslant (d+\nu) - 2\sqrt{(d+2\nu)x}] \leqslant e^{-x}. \tag{B4}$$

Based on Eq. (B4), for the noncentral χ^2 variable $\frac{(\widehat{C_{AB}})^2}{V_{\rm cov}} \sim \chi^2(1, \frac{C_{AB}^2}{V_{\rm cov}})$ we have

$$\mathrm{Prob}\left[\frac{(\widehat{C_{AB}})^2}{V_{\rm cov}} \leqslant \left(1 + \frac{C_{AB}^2}{V_{\rm cov}}\right) - 2\sqrt{\left(1 + 2\frac{C_{AB}^2}{V_{\rm cov}}\right)x}\right] \leqslant e^{-x}. \tag{B5}$$

Using Eq. (B2), we can rewrite Eq. (B5) as

$$\mathrm{Prob}\left[\hat{T}_s \leqslant \left(\frac{V_{\rm cov}}{V_A^2} + \frac{C_{AB}^2}{V_A^2}\right) - 2\frac{V_{\rm cov}}{V_A^2}\sqrt{\left(1 + 2\frac{C_{AB}^2}{V_{\rm cov}}\right)x}\right] \leqslant e^{-x}. \tag{B6}$$

Now using Eq. (B3) and assuming sufficiently large k_s, we can rewrite Eq. (B6) as

$$\mathrm{Prob}[\hat{T}_s \leqslant T_s - \sqrt{\mathrm{Var}(\hat{T}_s)}\sqrt{2x}] \leqslant e^{-x}. \tag{B7}$$

Setting $e^{-x} = \epsilon_{\rm PE}$, we have

$$\mathrm{Prob}\left[T_s \geqslant \hat{T}_s + \sqrt{\mathrm{Var}(\hat{T}_s)}\sqrt{2\ln\left(\frac{1}{\epsilon_{\rm PE}}\right)}\right] \leqslant \epsilon_{\rm PE}. \tag{B8}$$

Thus, the confidence interval for T_s is given by

$$\Delta(T_s) = \sqrt{2\ln\left(\frac{1}{\epsilon_{\rm PE}}\right)}\sqrt{\frac{4T_s^2}{k_s}\left(2 + \frac{\sigma_s^2}{T_s V_A}\right)}. \tag{B9}$$

The estimator of the square root of subchannel transmissivity and its error bar are then given by

$$\begin{aligned}\widehat{\sqrt{\eta}} &= \frac{\sqrt{2}\sqrt{\hat{T}_s}}{\sqrt{\hat{\eta}_B}},\\ \Delta(\sqrt{\eta}) &= \widehat{\sqrt{\eta}}\sqrt{\left|\frac{\Delta(T_s)}{2\hat{T}_s}\right|^2 + \left|\frac{\Delta(\eta_B)}{2\hat{\eta}_B}\right|^2}. \end{aligned} \tag{B10}$$

The estimation of the effective transmissivity is then given by averaging $\widehat{\sqrt{\eta}}$ over all subchannels as $\hat{\eta}_f = \widehat{\sqrt{\eta}}^{\,2}$. The estimator of the subchannel transmissivity and its error bar are also given by

$$\hat{\eta} = \frac{2\hat{T}_s}{\hat{\eta}_B},$$

$$\Delta(\eta) = \hat{\eta}\sqrt{\left|\frac{\Delta(T_s)}{\hat{T}_s}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2}. \tag{B11}$$

The estimation of the variance of transmissivity is then given by $\widehat{\mathrm{Var}(\sqrt{\eta})} = \langle\hat{\eta}\rangle - \langle\widehat{\sqrt{\eta}}\rangle^2$.

We now generalize the above-discussed parameter estimation method to the data of size k revealed over all subchannels to estimate $\langle\eta\xi_\eta\rangle$. The distributions of independent estimators $\hat{t}$ and $\hat{\sigma}^2$ in Eq. (16) are

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^k A_i^2}\right), \quad \frac{k\hat{\sigma}^2}{\sigma^2} \sim \chi^2(k-1). \tag{B12}$$

According to Lemma 6 in the Appendix of [72], we have a tail bound for a central χ^2 random variable $Y \sim \chi^2(d)$ with d degrees of freedom as, for all $x \geqslant 0$,

$$\mathrm{Prob}[Y \leqslant d - 2\sqrt{dx}] \leqslant e^{-x}. \tag{B13}$$

Based on Eq. (B13), for the central χ^2 variable $\frac{k\hat{\sigma}^2}{\sigma^2} \sim \chi^2(k-1)$ we have

$$\mathrm{Prob}\left[\frac{k\hat{\sigma}^2}{\sigma^2} \leqslant (k-1) - 2\sqrt{(k-1)x}\right] \leqslant e^{-x}. \tag{B14}$$

For sufficiently large k, we can rewrite Eq. (B14) as

$$\mathrm{Prob}\left[\hat{\sigma}^2 \leqslant \sigma^2 - \frac{\sqrt{2}\sigma^2}{\sqrt{k}}\sqrt{2x}\right] \leqslant e^{-x}. \tag{B15}$$

Having $\mathrm{Var}(\hat{\sigma}^2) = \frac{2\sigma^4}{k}$ and setting $e^{-x} = \epsilon_{\rm PE}$, we can rewrite Eq. (B15) as

$$\mathrm{Prob}\left[\sigma^2 \geqslant \hat{\sigma}^2 + \sqrt{\mathrm{Var}(\hat{\sigma}^2)}\sqrt{2\ln\left(\frac{1}{\epsilon_{\rm PE}}\right)}\right] \leqslant \epsilon_{\rm PE}. \tag{B16}$$

Thus, the confidence interval for σ^2 is given by

$$\Delta(\sigma^2) = \sqrt{2\ln\left(\frac{1}{\epsilon_{\rm PE}}\right)}\frac{\sqrt{2}\sigma^2}{\sqrt{k}}. \tag{B17}$$

Note that the above-mentioned method of calculating error bars for the output noise has been used in [73]. 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 $\sigma_0^2 = 1 + \nu_B$, which is Bob's shot-noise variance. The maximum-likelihood estimator for σ_0^2 is given by $\hat{\sigma}_0^2 = \frac{1}{N}\sum_{i=1}^N B_{0i}^2$. For $\hat{\sigma}_0^2$ we have the distribution of $\frac{N\hat{\sigma}_0^2}{\sigma_0^2} \sim \chi^2(N-1)$. The confidence interval for this parameter is given by $\Delta(\sigma_0^2) = \sqrt{2\ln(\frac{1}{\epsilon_{\rm PE}})}\frac{\sqrt{2}\sigma_0^2}{\sqrt{N}}$. Now we can estimate $\langle\eta\xi_\eta\rangle$, which is given by

$$\begin{aligned}\widehat{\langle\eta\xi_\eta\rangle} &= 2\frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{\eta}_B},\\ \Delta(\langle\eta\xi_\eta\rangle) &= \widehat{\langle\eta\xi_\eta\rangle}\sqrt{\left|\frac{\Delta(\sigma^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\sigma_0^2)}{\hat{\sigma}^2 - \hat{\sigma}_0^2}\right|^2 + \left|\frac{\Delta(\eta_B)}{\hat{\eta}_B}\right|^2}. \end{aligned} \tag{B18}$$

In order to maximize Eve's information from general attacks, the worst-case estimators of the effective parameters η_f and

ξ_f [through the use of Eq. (20)] should be utilized to evaluate Eve's information. Note that for security analysis against general attacks with security parameter $\tilde{\epsilon} = 10^{-9}$ for a block size of $N = 10^{10}$, we need to analyze security against collective attacks with security parameters $\epsilon = 10^{-49}$ and $\epsilon_{\rm PE} = 10^{-50}$. For this very small $\epsilon_{\rm PE}$, we cannot use the parameter estimation method in Sec. IV C because $z_{\epsilon_{\rm PE}/2}$ diverges. Instead we use the parameter estimation method discussed in this Appendix where $\sqrt{2\ln(\frac{1}{\epsilon_{\rm PE}})} = 15.1743$.

APPENDIX C: ELLIPTIC-BEAM MODEL

We have considered a free-space channel where the probability distribution for the channel transmissivity is given by the elliptic-beam model [28]. This model can be used for an atmospheric channel including beam wandering, beam broadening, and beam shape deformation [28]. However, for this model, referred to as the elliptic-beam approximation, there is not an explicit form for the probability distribution. Here we briefly discuss how to apply the model of the elliptic-beam approximation for calculation of the key rate. Further details on the model can be found in [28]. Within this model, it is assumed that turbulent disturbances along the propagation path result in beam wandering and deformation of the Gaussian beam profile into an elliptic form. The elliptic beam at the aperture plane is characterized by the beam-centroid position $\mathbf{r}_0 = (x_0, y_0)^T = (r_0\cos\psi_0, r_0\sin\psi_0)^T$ and W_1 and W_2 as semiaxes of the elliptic spot, where the semiaxis W_1 has an angle $\psi \in [0, \pi/2)$ relative to the x axis. Defining $\phi = \psi - \psi_0$, the aperture transmissivity η_a is a function of real parameters $[x_0, y_0, \Theta_1, \Theta_2, \phi]$ [29], which are randomly changed by the atmosphere. Note that Θ_1 and Θ_2 are related to the semiaxes, as $W_j^2 = W_0^2\exp(\Theta_j)$ [28] for $j = 1, 2$ with W_0 the initial beam-spot radius. Note also that random fluctuations of the beam-centroid position $\mathbf{r}_0$, i.e., the parameters x_0 and y_0, cause the effect of beam wandering. For the parameters $[x_0, y_0, \Theta_1, \Theta_2]$, we can assume a four-dimensional Gaussian distribution, and for the parameter ϕ, by assuming isotropic turbulence, we can assume a uniform distribution in the interval $[0, \pi/2]$ [29]. Under the assumption of isotropic turbulence, there is no correlation between ϕ with other linear parameters [28]. We also assume that $\langle\mathbf{r}_0\rangle = 0$, i.e., beam wandering fluctuations are placed around the reference-frame origin. Under this assumption, correlations between x_0, y_0, and Θ_j vanish [28]. Hence, we first generate n independent Gaussian random vectors $\mathbf{v}_i = (x_{0i}, y_{0i}, \Theta_{1i}, \Theta_{2i})$, $i = 1, \ldots, n$, and n random uniformly distributed angles $\phi_i \in [0, \pi/2)$. The Gaussian random parameters $(x_{0i}, y_{0i}, \Theta_{1i}, \Theta_{2i})$ can be characterized by the covariance matrix

$$\mathbf{M} = \begin{pmatrix} \langle\Delta x_0^2\rangle & 0 & 0 & 0 \\ 0 & \langle\Delta y_0^2\rangle & 0 & 0 \\ 0 & 0 & \langle\Delta\Theta_1^2\rangle & \langle\Delta\Theta_1\Delta\Theta_2\rangle \\ 0 & 0 & \langle\Delta\Theta_1\Delta\Theta_2\rangle & \langle\Delta\Theta_2^2\rangle \end{pmatrix} \tag{C1}$$

and the mean value $(0, 0, \langle\Theta_1\rangle, \langle\Theta_2\rangle)$. The elements of the covariance matrix and the mean values for weak turbulence are given by [28]

$$\begin{aligned} \langle\Delta x_0^2\rangle &= \langle\Delta y_0^2\rangle = 0.33W_0^2\sigma_R^2\Omega^{-7/6}, \\ \langle\Delta\Theta_1^2\rangle &= \ln\left[1 + \frac{1.2\sigma_R^2\Omega^{5/6}}{\left(1 + 2.96\sigma_R^2\Omega^{5/6}\right)^2}\right], \\ \langle\Delta\Theta_1\Delta\Theta_2\rangle &= \ln\left[1 - \frac{0.8\sigma_R^2\Omega^{5/6}}{\left(1 + 2.96\sigma_R^2\Omega^{5/6}\right)^2}\right], \\ \langle\Theta_1\rangle &= \langle\Theta_2\rangle = \ln\left[\frac{\left(1 + 2.96\sigma_R^2\Omega^{5/6}\right)^2}{\Omega^2\sqrt{\left(1 + 2.96\sigma_R^2\Omega^{5/6}\right)^2 + 1.2\sigma_R^2\Omega^{5/6}}}\right], \end{aligned} \tag{C2}$$

where σ_R^2 is the Rytov parameter, $\Omega = \frac{kW_0^2}{2L}$ is the Fresnel parameter, k is the wave number, and L is the propagation distance. After generating n random vectors $\mathbf{v}_i = (x_{0i}, y_{0i}, \Theta_{1i}, \Theta_{2i})$ and n random angles $\phi_i \in [0, \pi/2)$, we can generate n random transmissivity $\eta_{a,i} = \eta_a(\mathbf{v}_i, \phi_i)$ as [28]

$$\eta_a(\mathbf{v}, \phi) = \eta_0\exp\left\{-\left[\frac{r_0/a}{R\left(\frac{2}{W_{\rm eff}(\phi)}\right)}\right]^{\lambda[2/W_{\rm eff}(\phi)]}\right\}, \tag{C3}$$

where $r_0 = \sqrt{x_0^2 + y_0^2}$ is the distance between the beam and the aperture center and a is the radius of the circular receiver aperture. The transmissivity for the centered beam, i.e., for $r_0 = 0$, is given by [28]

$$\begin{aligned} \eta_0 = 1 - I_0\left(a^2\left[\frac{1}{W_1^2} - \frac{1}{W_2^2}\right]\right)\exp\left\{-a^2\left[\frac{1}{W_1^2} + \frac{1}{W_2^2}\right]\right\} - 2\left(1 - \exp\left\{-\frac{a^2}{2}\left[\frac{1}{W_1} - \frac{1}{W_2}\right]^2\right\}\right) \\ \times\exp\left\{-\left[\frac{\frac{(W_1+W_2)^2}{|W_1^2 - W_2^2|}}{R\left(\frac{1}{W_1} - \frac{1}{W_2}\right)}\right]^{\lambda(1/W_1 - 1/W_2)}\right\}. \end{aligned} \tag{C4}$$

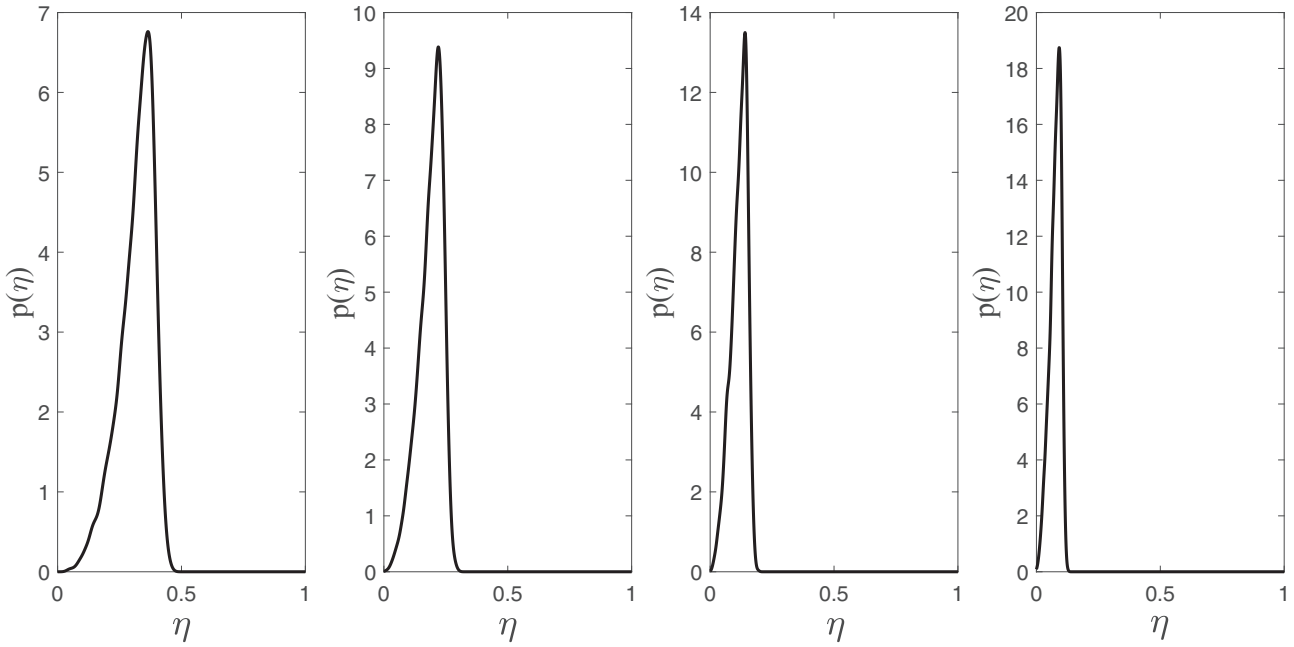

FIG. 3. Probability distribution function $p(\eta)$ obtained for the generated sampled data η_i, $n = 10^4$. For the sample generations the parameters are chosen based on an experimentally implemented free-space experiment [18]. The elliptic-beam model [28] shows good agreement with the experimental distribution of the transmissivity [28]. The following parameter values are used: the wavelength $\lambda = 809$ nm, the initial beam-spot radius $W_0 = 20$ mm, the deterministic attenuation 1.25 dB, and the radius of the receiver aperture $a = 40$ mm. The Rytov parameter is given by $\sigma_R^2 = 1.23 C_n^2 k^{7/6} L^{11/6}$, where we choose $C_n^2 = 1.5 \times 10^{-14}$ m$^{-2/3}$, and the propagation distance $L = 2, 2.5, 3, 3.5$ km from left to right.

The additional parameters, that is, the effective squared spot radius $W_{\text{eff}}^2(\phi)$ and the scale $R(\zeta)$ and shape $\lambda(\zeta)$ functions, are given by [28]

$$
\begin{aligned}
W_{\text{eff}}^2(\phi) &= 4a^2\left[\mathcal{W}\left(\frac{4a^2}{W_1 W_2}\exp\left\{\frac{a^2}{W_1^2}(1+2\cos^2\phi)\right\}\exp\left\{\frac{a^2}{W_2^2}(1+2\sin^2\phi)\right\}\right)\right]^{-1},\\
R(\zeta) &= \left(\ln\left[2\frac{1-\exp\{-\frac{1}{2}a^2\zeta^2\}}{1-\exp\{-a^2\zeta^2\}I_0(a^2\zeta^2)}\right]\right)^{-1/\lambda(\zeta)},\\
\lambda(\zeta) &= 2a^2\zeta^2\frac{\exp\{-a^2\zeta^2\}I_1(a^2\zeta^2)}{1-\exp\{-a^2\zeta^2\}I_0(a^2\zeta^2)}\left(\ln\left[2\frac{1-\exp\{-\frac{1}{2}a^2\zeta^2\}}{1-\exp\{-a^2\zeta^2\}I_0(a^2\zeta^2)}\right]\right)^{-1},
\end{aligned}
\tag{C5}
$$

where $\mathcal{W}(\zeta)$ is the Lambert W function and $I_j(\zeta)$ is the modified Bessel function of the jth order.

We also consider a deterministic (constant) transmissivity $\eta_m \in [0, 1]$, which means the total transmissivity of the channel would be $\eta_i = \eta_m \eta_{a,i}$. Note that η_m can be considered as the extinction factor of the atmospheric channel describing the absorption and scattering losses [29]. Based on the generated sampling data, one can estimate the mean value of any function of the transmissivity $f(\eta)$ as $\langle f(\eta)\rangle = \frac{1}{n}\sum_{i=1}^{n} f(\eta_i)$. For instance, Eq. (7) can be modified as

$$
\langle\eta\rangle = \frac{1}{n}\sum_{i=1}^{n}\eta_i, \quad \langle\sqrt{\eta}\rangle = \frac{1}{n}\sum_{i=1}^{n}\sqrt{\eta_i}, \quad \langle\eta\xi_\eta\rangle = \frac{1}{n}\sum_{i=1}^{n}\eta_i\xi_{\eta_i}. \tag{C6}
$$

In our numerical analysis we have first fitted a probability distribution to the generated sampled data η_i (shown in Fig. 3), which gives us a numerical form for $p(\eta_i)$. Note that since no closed-form solution for $p(\eta)$ could be used, the integrals required to be computed for the security analysis [provided in Eqs. (23) and (26)] should be numerically evaluated.

[1] 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).

[2] S. Pirandola *et al.*, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[3] 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).

[4] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Sig-*

nal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

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

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

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

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

[9] 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).

[10] R. Garcia-Patron, Ph.D. thesis, Universite Libre de Bruxelles, 2007.

[11] 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).

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

[13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photon. **7**, 378 (2013).

[14] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[15] G. Zhang, J. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photon. **13**, 839 (2019).

[16] Y. Zhang *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[17] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[18] 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).

[19] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Distribution of Squeezed States through an Atmospheric Channel, Phys. Rev. Lett. **113**, 060502 (2014).

[20] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, Atmospheric continuous-variable quantum communication, New J. Phys. **16**, 113018 (2014).

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

[22] 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. Tut. **21**, 881 (2019).

[23] S.-Y. Shen, M.-W. Dai, X.-T. Zheng, Q.-Y. Sun, G.-C. Guo, and Z.-F. Han, Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment, Phys. Rev. A **100**, 012325 (2019).

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

[25] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. **119**, 200501 (2017).

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

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

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

[29] 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).

[30] 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).

[31] M. Bohmann, A. A. Semenov, J. Sperling, and W. Vogel, Gaussian entanglement in the turbulent atmosphere, Phys. Rev. A **94**, 010302(R) (2016).

[32] N. Hosseinidehaj and R. Malaney, in *Proceedings of the IEEE International Conference on Communications (ICC), London, 2015* (IEEE, Piscataway, 2015), pp. 7413–7419.

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

[34] K. Hofmann, A. A. Semenov, W. Vogel, and M. Bohmann, Quantum teleportation through atmospheric channels, Phys. Scr. **94**, 125104 (2019).

[35] 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).

[36] D. Dequal, L. T. Vidarte, V. R. Rodriquez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of satellite-to-ground continuous-variable quantum key distribution, npj Quantum Information **7**,3 (2021).

[37] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography Without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[38] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light, Phys. Rev. Lett. **95**, 180503 (2005).

[39] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution Via a Gaussian De Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[40] S. Ghorai, E. Diamanti, and A. Leverrier, Composable security of two-way continuous-variable quantum key distribution without active symmetrization, Phys. Rev. A **99**, 012311 (2019).

[41] N. Hosseinidehaj, N. Walk, and T. C. Ralph, Optimal realistic attacks in continuous-variable quantum key distribution, Phys. Rev. A **99**, 052336 (2019).

[42] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Impact of Turbulence in Long Range Quantum and Classical Communications, Phys. Rev. Lett. **109**, 200502 (2012).

[43] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels, Phys. Rev. A **91**, 042320 (2015).

[44] A. A. Semenov, F. Töppel, D. Y. Vasylyev, H. V. Gomonay, and W. Vogel, Homodyne detection for atmosphere channels, Phys. Rev. A **85**, 013826 (2012).

[45] N. Hosseinidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection, Phys. Rev. A **101**, 052335 (2020).

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

[47] R. Renner and J. I. Cirac, de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

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

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

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

[51] 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).

[52] P. Papanastasiou and S. Pirandola, Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks, Phys. Rev. Research **3**, 013047 (2021).

[53] 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).

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

[55] N. Hosseinidehaj and R. Malaney, in *Proceedings of the IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016* (IEEE, 2016), pp. 1–7.

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

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

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

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

[60] 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).

[61] M. Tomamichel, Ph.D. thesis, Swiss Federal Institute of Technology, 2012.

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

[63] 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).

[64] J. Lodewyck and P. Grangier, Tight bound on the coherent-state quantum key distribution with heterodyne detection, Phys. Rev. A **76**, 022332 (2007).

[65] J. Sudjana, L. Magnin, R. Garcia-Patron, and N. J. Cerf, Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching, Phys. Rev. A **76**, 052301 (2007).

[66] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, Parameter estimation of atmospheric continuous-variable quantum key distribution, Phys. Rev. A **99**, 032326 (2019).

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

[68] 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).

[69] R. Garcia-Patron and N. J. Cerf, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Phys. Rev. Lett. **102**, 130501 (2009).

[70] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B **42**, 114014 (2009).

[71] L. Ruppert, V. C. Usenko, and R. Filip, Long-distance continuous-variable quantum key distribution with efficient channel estimation, Phys. Rev. A **90**, 062310 (2014).

[72] M. Kolar and H. Liu, Marginal regression for multitask learning, in *Proceedings of the Fifteenth International Conference on Artificial Intelligence and Statistics*, Vol. 22 (PMLR, 2012), pp. 647–655.

[73] S. Pirandola, Limits and security of free-space quantum communications, arXiv:2010.04168.