Optimal realistic attacks in continuous-variable quantum key distribution

Nedasadat Hosseinidehaj,[1,*] Nathan Walk,[2,3,†] 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*
[3]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom*

(Received 18 November 2018; published 23 May 2019)

Quantum cryptographic protocols are typically analyzed by assuming that potential opponents can carry out all physical operations, an assumption which grants capabilities far in excess of present technology. Adjusting this assumption to reflect more realistic capabilities is an attractive prospect, but one that can only be justified with a rigorous, quantitative framework that relates adversarial restrictions to the protocol's security and performance. We investigate the effect of limitations on the eavesdropper's (Eve's) ability to make a coherent attack on the security of continuous-variable quantum key distribution (CV-QKD). We consider a realistic attack in which the total decoherence induced during the attack is modeled by a Gaussian channel. Based on our decoherence model, we propose an optimal hybrid attack, which allows Eve to perform a combination of both coherent and individual attacks simultaneously. We evaluate the asymptotic and composable finite-size security of a heterodyne CV-QKD protocol against such hybrid attacks in terms of Eve's decoherence. We show that when the decoherence is greater than a threshold value, Eve's most effective strategy is reduced to the individual attack. Thus, if we are willing to assume that the decoherence caused by the memory and the collective measurement is large enough, it is sufficient to analyze the security of the protocol only against individual attacks, which significantly improves the CV-QKD performance in terms of both the key rate and maximum secure transmission distance.

DOI: 10.1103/PhysRevA.99.052336

I. INTRODUCTION

Coherent attacks are known to be the most powerful eavesdropping attacks on quantum key distribution (QKD) protocols. The eavesdropper, Eve, prepares a global ancillary system, interacting collectively with all the quantum states sent through the channel, with the entire output ancillae stored into a quantum memory and a collective measurement applied over the stored ensemble [1,2] to extract the maximum information on the key. Making such an attack, particularly on a continuous-variable (CV) QKD system [1–3], represents an extreme technical challenge for Eve.

For a no-switching CV-QKD protocol [4,5], based on Gaussian-modulated coherent states and heterodyne detection, the finite-size composable security against coherent attacks can be analyzed by considering Gaussian collective attacks [6]. In a collective attack Eve prepares an ensemble of independent and identical quantum systems, each one interacting individually with a single quantum state transmitted through the channel, with the output ancilla stored into a quantum memory [1,2]. In a collective attack on Gaussian-modulated coherent-state CV-QKD protocol the ancillae stored in Eve's quantum memory is a tensor product of n coherent states, i.e., an n-symbol codeword. In order for Eve to extract the maximum information upper bounded by the Holevo information [7–9], a sequence of projective binary-outcome collective quantum measurements has to be applied to the n-symbol codeword [10]. In [11] a quantum optical realization of the sequential decoding strategy has been provided, which in a large number of 2^{nR} steps determines which codeword was sent (with R the rate in bits/symbol being bounded by the Holevo information). In [12] a more efficient (in terms of scaling) sequential decoding strategy (but with no evidence of quantum optical implementation) has been proposed, consisting of a sequence of complex adaptive collective quantum measurements performed in a series of nR concatenated steps to determine which codeword was sent. Thus, in a realistic collective attack a significant amount of time and/or coherent operations are required for Eve to collectively decode the stored ensemble to approach the Holevo information.

In this work we investigate Eve's optimal attack in a no-switching CV-QKD protocol, given practical restrictions on her storage and processing ability. The realistic assumption of restricted quantum memories has been studied in the context of quantum data-locking protocols [13–16] and two-party cryptographic tasks of oblivious transfer and bit commitment [17–21]. In a no-switching CV-QKD protocol, Eve can avoid the decoherence induced over the storage and processing time of the collective attack by performing individual attacks where she interacts individually with each quantum state sent by Alice, and she immediately performs an individual measurement on the output ancilla. This is an optimal individual attack strategy, because there is no basis information withheld in the no-switching protocol. With the aim of allowing Eve to

*n.hosseinidehaj@uq.edu.au
†nwalk@zedat.fu-berlin.de
‡ralph@physics.uq.edu.au

simultaneously benefit from both the collective decoding and avoiding the decoherence induced over the decoding, we propose realistic optimal attacks, hybrid attacks, that lie in between the coherent and individual attacks. In the hybrid attack we model the total decoherence induced on each quantum system stored into the quantum memory with a thermal, lossy Gaussian channel. We will evaluate the asymptotic and composable finite-size security of a no-switching CV-QKD protocol in terms of Eve's attack decoherence, thereby demonstrating that if the decoherence is higher than a threshold value, Eve's best strategy is the individual attack; thus the security of the CV-QKD protocol can be analyzed by considering only the individual attack, which remarkably improves both the key rate and the maximum secure transmission distance of the protocol. Note that our realistic assumption of decoherence over the storage time of a collective (or coherent) attack is fully future proof in the sense that if a perfect quantum memory becomes possible in the future, the key which is secure now will remain secure.

The outline of the paper is as follows: In Sec. II we briefly describe the no-switching CV-QKD protocol in both the prepare-and-measure and equivalent entanglement-based scheme. In Sec. III we discuss the security of the no-switching protocol in the composable finite-size regime. In Sec. IV we propose an optimal realistic eavesdropping attack in a hybrid scheme and analyze the security of the protocol against such attacks. In Sec. V we show the numerical results for the performance of the CV-QKD system against the optimal realistic attacks. Finally, we discuss and conclude this work in Secs. VI and VII, respectively.

II. CV-QKD SYSTEM

We consider a Gaussian no-switching CV-QKD protocol [4,5], where Alice generates a pair of random real numbers, chosen from two independent Gaussian distributions of variance V_A, to prepare coherent states. The prepared states are then transmitted over an insecure quantum channel with transmissivity T and excess noise ξ (relative to the input of the quantum channel) to Bob. For each incoming state, Bob uses heterodyne detection to measure both the $\hat{q}$ and $\hat{p}$ quadratures. In this protocol, sifting is not needed, since both of the random variables generated by Alice are used for the generation of the key. When the quantum communication is finished and all the incoming quantum states are 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.

This Gaussian CV-QKD system can also be represented by an equivalent entanglement-based scheme [1,2], where Alice generates a two-mode squeezed vacuum (TMSV) state ρ_{AB} with the quadrature variance $V = V_A+1$. Alice retains mode A while sending mode B to Bob over the quantum channel. In the entanglement-based scheme, Alice applies a heterodyne detection to mode A, which results in projecting mode B onto a coherent state. At the output of the channel, Bob applies a heterodyne detection to the received mode B_1, with his detector having an efficiency of η and electronic noise variance of $\upsilon_{\rm el}$ [22,23].

III. COMPOSABLE FINITE-SIZE SECURITY ANALYSIS

We exploit the approach introduced in [6,24] to analyze the composable finite-size security of the no-switching CV-QKD protocol (acting on a $2N$-mode state shared between Alice and Bob) against coherent attacks. This approach consists of two steps: first proving the security of the protocol against Gaussian collective attacks with a security parameter ϵ [24], and then applying the Gaussian de Finetti reduction [6] to obtain the security against coherent attacks with a polynomially larger security parameter $\tilde{\epsilon}$ [6], where the security loss due to the reduction from coherent attacks to collective attacks scales like $O(N^4)$ (see Appendix A for more details). There exists another approach to prove the security against coherent attacks which is based on an entropic uncertainty relation [25–27], but the relevant CV-QKD protocol requires the preparation of squeezed states. Furthermore, due to the looseness of the current best entropic uncertainty relations, this approach predicts key rates that are pessimistic as a function of loss.

The no-switching CV-QKD protocol with the number of $2n$ coherent states sent by Alice is ϵ-secure against collective attacks in a reverse reconciliation (RR) scenario if [24,28]

$$\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor} \tag{1}$$

and if the key length ℓ is chosen such that [24,28]

$$\ell \leqslant N[\beta I(A{:}B) - \chi(B{:}E)] - \Delta_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \tag{2}$$

where $I(A{:}B)$ is the Shannon mutual information between Alice and Bob (calculated and provided in Appendix B), $\chi(B{:}E)$ is the Holevo information between Eve and Bob, β is the reconciliation efficiency, $N = 2n$, and the finite-size correction term is given by [24,28]

$$\Delta_{\rm AEP} = \sqrt{N}\Bigg[(d+1)^2+4(d+1)\sqrt{\log_2\left(\frac{2}{\epsilon_{\rm sm}^2}\right)} + 2\log_2\left(\frac{2}{\epsilon^2\epsilon_{\rm sm}}\right)\Bigg] + 4\frac{\epsilon_{\rm sm} d}{\epsilon}, \tag{3}$$

where d is the discretization parameter, and $\epsilon_{\rm cor}$ and $\epsilon_{\rm PE}$ are the maximum failure probabilities for the error correction and parameter estimation, respectively (see Appendix A for more details). We have considered the same scenario as [24,28,29], where almost all the raw data can be utilized to distill the secret key. Note that for the ϵ-security analysis of the same protocol against individual attacks we can still use Eq. (2), where $\chi(B{:}E)$ must be replaced by the Shannon mutual information between Eve and Bob, $I(B{:}E)$.

IV. OPTIMAL REALISTIC ATTACK

Now we investigate the optimal eavesdropping attack on a no-switching CV-QKD protocol, given Eve's storage and processing limitations. We propose an optimal realistic hybrid attack, where Eve performs a combination of both the coherent and individual attacks. Note that Eve does not need a quantum memory for the individual attack, since she does not need to wait for any basis information to be disclosed in the no-switching CV-QKD protocol. This hybrid attack

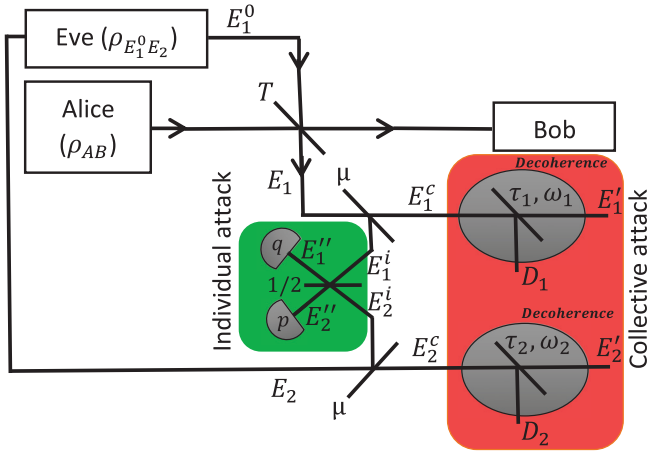

FIG. 1. Eve's optimal hybrid attack for the no-switching CV-QKD protocol.

allows Eve to benefit from the advantage of both the collective decoding, as well as the individual measurement of the nondecohered ancillae.

We model the coherent-attack part of the hybrid attack with a Gaussian collective attack and the individual-attack part of the hybrid attack with a Gaussian individual attack. Gaussian collective (individual) attacks are known to be asymptotically optimal [1,2,30–33]. Furthermore, according to the Gaussian de Finetti reduction, for the no-switching protocol it is also sufficient to consider Gaussian collective attacks in the finite-size, composable security proof [6]. These results are crucial, since they allow us to explicitly model Eve's attack and her decoherence. Both the optimal Gaussian collective attack [34] and the optimal Gaussian individual attack [35] can be modeled using an entangling cloner attack (shown in Fig. 1), where Eve replaces the Gaussian channel with transmissivity T and excess noise ξ by a TMSV state $\rho_{E_1^0E2}$ of the quadrature variance $\omega_E = 1+T\xi/(1-T)$, and a beam splitter of transmissivity T. Half of the TMSV state, mode E_1^0, is mixed with the state sent by Alice in the beam splitter, outputting mode B_1 (which is sent to Bob through a perfect quantum channel) and Eve's ancillary, mode E_1.

In order to combine both the Gaussian collective attack and the Gaussian individual attack in a hybrid attack, we exploit two beam splitters with identical transmissivities μ to split each of Eve's ancillary modes into two output modes, one for the collective attack and the other one for the individual attack. In fact, the output mode E_1 (E_2) is split in a beam splitter of transmissivity μ into two output modes E_1^c (E_2^c) for the collective attack and E_1^i (E_2^i) for the individual attack. The ancillary modes E_1^c and E_2^c are stored into Eve's quantum memories and collectively measured after the entire ancillae are stored. Since we are modeling Gaussian attacks, we model the total decoherence induced during the collective attack over the storage and processing time by a thermal, lossy Gaussian channel with transmissivity τ and thermal noise variance ω. Explicitly, the ancillary mode E_1^c (E_2^c) undergoes the decoherence, modeled by a Gaussian channel with parameters τ_1, ω_1 (τ_2, ω_2) and the output mode E_1' (E_2'). Note that the output modes D_1 and D_2 are not accessible to Eve. On the other hand, in the individual attack, the ancillary modes E_1^i and E_2^i are mixed in a balanced beam splitter, resulting in modes E_1'' and E_2'', where the $\hat{q}$ quadrature (the $\hat{p}$ quadrature) is measured using the homodyne detection on E_1'' (E_2'') [35,36].

A. Security analysis against the hybrid attack

The finite-size key length of the no-switching protocol in the RR scenario, which is secure against the hybrid attack with the security parameter $\tilde{\epsilon}$, can be given as

$$\ell_{\rm hyb} \leqslant \min_{\mu} \left[N\beta I(A{:}B) - N I_{\mu}^{\rm hyb}(B{:}E) - \Delta_{\rm AEP}^{H} - 2\log_2\left(\frac{1}{2\tilde{\epsilon}}\right)\right], \tag{4}$$

where $I_{\mu}^{\rm hyb}(B{:}E)$ is the upper bound on the mutual information between Eve and Bob, which is given by

$$\begin{aligned} I_{\mu}^{\rm hyb}(B{:}E) = I_{\mu}^{\rm hyb}(B{:}E_1'E_2'E_1''E_2'') &= \chi_{\mu}(BE_1''E_2'':E_1'E_2') \\ &+ I_{\mu}(B{:}E_1''E_2'') - \chi_{\mu}(E_1''E_2'':E_1'E_2'), \end{aligned} \tag{5}$$

where $\chi_{\mu}(BE_1''E_2'':E_1'E_2')$ is Eve's information contributed from the collective attack, limited by the Holevo information, $I_{\mu}(B{:}E_1''E_2'')$ is Eve's information contributed from the individual attack, limited by the Shannon information, and $\chi_{\mu}(E_1''E_2'':E_1'E_2')$ is the mutual information between Eve's ancillary modes for the individual and collective attacks, limited by the Holevo information. See Appendix C for calculation of the right-hand terms of Eq. (5).

Note that the Shannon mutual information denoted by $I(X{:}Y)$ quantifies the amount of correlations between the two classical random variables X and Y, and is given by $I(X{:}Y) = H(X) - H(X|Y)$ [37], with $H(X)$ the Shannon entropy and $H(X|Y)$ the Shannon conditional entropy. In Eq. (5), the term $I_{\mu}(B{:}E_1''E_2'')$ quantifies the amount of correlations between the random variables B resulting from Bob's measurements and the random variables $E_1''E_2''$ resulting from Eve's individual measurements.

Note also that the Holevo information denoted by $\chi(X{:}Y)$ is the upper bound on the mutual information between the classical random variable X and the quantum system ρ_Y, and is given by $\chi(X{:}Y) = S(\rho_Y) - \sum_x p_X(x) S(\rho_Y^x)$ [37], with $S(\rho_Y)$ the von Neumann entropy of the quantum state ρ_Y preceding the measurement, and $S(\rho_Y^x)$ the von Neumann entropy of the quantum state ρ_Y (preceding the measurement) conditioned on the random variable X. Hence, $\chi(X{:}Y)$ does not depend on the type of measurement applied to the quantum state ρ_Y. In Eq. (5), the term $\chi_{\mu}(BE_1''E_2'':E_1'E_2')$ quantifies the upper bound on the mutual information between the random variables $BE_1''E_2''$ resulting from Bob and Eve's individual measurements and the quantum system $\rho_{E_1'E_2'}$. Also, the term $\chi_{\mu}(E_1''E_2'':E_1'E_2')$ quantifies the upper bound on the mutual information between the random variables $E_1''E_2''$ resulting from Eve's individual measurements and the quantum system $\rho_{E_1'E_2'}$.

Since the Δ term in Eq. (4) is different for the coherent and individual attacks, to compute $\ell_{\rm hyb}$ in Eq. (4) we first maximize $I_{\mu}^{\rm hyb}(B{:}E)$ over all possible values of $0 \leqslant \mu \leqslant 1$. When the maximization of $I_{\mu}^{\rm hyb}(B{:}E)$ leads to $\mu = 1$, Eve's hybrid attack reduces to the coherent attack. In this case,

Eq. (4) changes to $\ell_{\rm hyb} = \ell_{\rm coh}$, where

$$\ell_{\rm coh} \leqslant N[\beta I(A{:}B) - \chi(B{:}E_1'E_2')] - \Delta^C_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \quad (6)$$

and where $\chi(B{:}E_1'E_2') = \chi_\mu(BE_1''E_2''{:}E_1'E_2')$ for $\mu = 1$, and $\Delta^C_{\rm AEP}$ is given by $\Delta_{\rm AEP}$ in Eq. (3) for $\epsilon \ll \tilde{\epsilon}$. When the maximization of $I^{\rm hyb}_\mu(B{:}E)$ leads to $\mu = 0$, Eve's hybrid attack always reduces to the individual attack in the asymptotic regime. However, this is not the case for the finite-size regime, since the Δ term for the coherent attack is much larger than that of the individual attack. This is because the Δ term for the individual attack does not have to include the $O(N^4)$ reduction in $\tilde{\epsilon}$ that is required to reduce coherent attacks to collective ones. This means there are instances where, although the coherent attack results in a smaller mutual information with Eve (which we would associate with a higher asymptotic key rate), the coherent-attack finite key rate is still lower than the individual-attack finite key rate because of this difference in the finite-size corrections. Hence, when the maximization of $I^{\rm hyb}_\mu(B{:}E)$ leads to $\mu = 0$, the finite-size key length is obtained by $\ell_{\rm hyb} = \min(\ell_{\rm coh}, \ell_{\rm ind})$, where $\ell_{\rm ind}$ is the finite-size key length where Eve's hybrid attack reduces to the individual attack and is given by

$$\ell_{\rm ind} \leqslant N[\beta I(A{:}B) - I(B{:}E_1''E_2'')] - \Delta^I_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \quad (7)$$

and where $I(B{:}E_1''E_2'') = I_\mu(B{:}E_1''E_2'')$ for $\mu = 0$, and $\Delta^I_{\rm AEP}$ is given by $\Delta_{\rm AEP}$ in Eq. (3) for $\epsilon = \tilde{\epsilon}$. Furthermore, when the maximization of $I^{\rm hyb}_\mu(B{:}E)$ leads to $0 < \mu < 1$, Eve performs a combination of both the individual and coherent attacks. In this case we can only calculate a (presumably loose) lower bound on the finite-size key length $\ell_{\rm hyb}$. Since $\epsilon \ll \tilde{\epsilon}$ leads to $\Delta^C_{\rm AEP} > \Delta^I_{\rm AEP}$, the (loose) lower bound on $\ell_{\rm hyb}$ can be obtained by Eq. (4), where $\Delta^H_{\rm AEP} = \Delta^C_{\rm AEP}$.

V. NUMERICAL RESULTS

We illustrate these results with a practical example of realistic devices [38,39] and a lossy channel with transmissivity $T = 0.1$ (or approximately 50 km of telecom fiber) and $\xi = 0.01$. In Fig. 2 the asymptotic and finite-size key rate of the no-switching protocol in the RR scenario is illustrated as a function of Eve's memory-channel transmissivity for different types of attacks: individual, coherent, and hybrid. Note that in our numerical simulations we assume identical (i.e., $\tau_1 = \tau_2 = \tau$ and $\omega_1 = \omega_2 = \omega$) but independent quantum memories.

In the asymptotic regime, the secret key rate in the RR scenario is given by $K_{\rm ind} = \beta I(A{:}B) - I(B{:}E_1''E_2'')$ against the individual attack, $K_{\rm col} = \beta I(A{:}B) - \chi(B{:}E_1'E_2')$ against the collective attack, and $K_{\rm hyb} = \beta I(A{:}B) - \max_\mu[I^{\rm hyb}_\mu(B{:}E)]$ against the hybrid attack. Note that the derived bounds for the secret key rate in the case of collective attacks remain asymptotically valid for the arbitrary coherent attacks [33].

In the finite-size regime, the secret key rate in the RR scenario is given by $K_{\rm ind} = \frac{\ell_{\rm ind}}{N}$ against the individual attack, $K_{\rm coh} = \frac{\ell_{\rm coh}}{N}$ against the coherent attack, and $K_{\rm hyb} = \frac{\ell_{\rm hyb}}{N}$ against the hybrid attack.

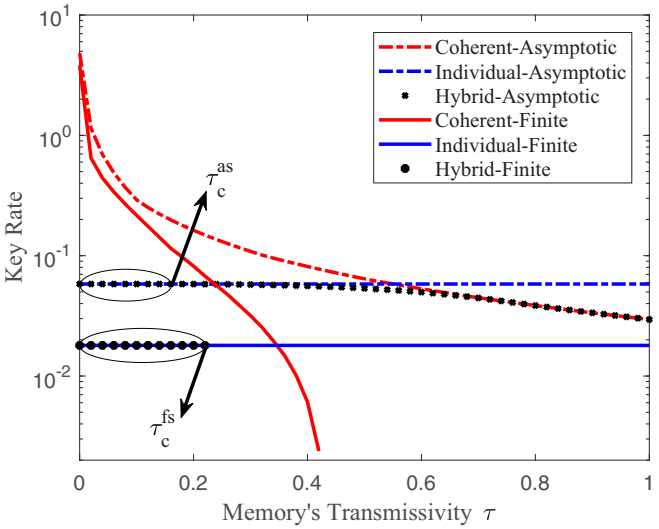

FIG. 2. The finite-size and asymptotic key rate as a function of memory's transmissivity τ for individual (blue), coherent (red), and hybrid attacks (black). The numerical values are $\eta = 0.6$ [38], $\upsilon_{\rm el} = 0.015$ [39], $T = 0.1, \xi = 0.01, d = 5, \omega = 1, \beta = 0.98$ [40], and the modulation variance is optimized. The region marked by the ellipse shows memory's transmissivities for which Eve's optimal attack is the individual attack.

In our numerical calculations of finite-size key rate, for all types of attacks we consider the security parameters $\tilde{\epsilon} = 10^{-6}$ and $n = 10^9$. Recall again that to analyze the security of the no-switching protocol against coherent attacks with the security parameter $\tilde{\epsilon} = 10^{-6}$, it is sufficient to analyze the security of the protocol against Gaussian collective attacks with the security parameter ϵ using Eq. (6) where $\epsilon \ll \tilde{\epsilon}$. Here we consider $\epsilon = 10^{-42} \ll \tilde{\epsilon} = 10^{-6}$ for $n = 10^9$, since the security loss due to the reduction from coherent attacks to collective attacks scales like $O(N^4)$. Thus, for coherent attacks we choose $\epsilon_{\rm PE} = \epsilon_{\rm cor} = \bar{\epsilon} = 10^{-43}$ to satisfy Eq. (1) for $\epsilon = 10^{-42}$, while for individual attacks we choose $\epsilon_{\rm PE} = \epsilon_{\rm cor} = \bar{\epsilon} = 10^{-7}$ to satisfy Eq. (1) for $\epsilon = \tilde{\epsilon} = 10^{-6}$. Note that for hybrid attacks we consider a pessimistic scenario by choosing $\epsilon_{\rm PE} = \epsilon_{\rm cor} = \bar{\epsilon} = 10^{-43}$, which again leads to a loose lower bound on the finite-size hybrid key rate.

In Fig. 2 we see that there is a threshold transmissivity of Eve's memory channel below which an individual attack is always optimal. We denote $\tau_c^{\rm as}$ and $\tau_c^{\rm fs}$ for the threshold transmissivity in the asymptotic and finite-size regime, respectively. In Fig. 2, asymptotically we see that when $\tau \leqslant \tau_c^{\rm as} = 0.17$ individual attacks are optimal. For $\tau_c^{\rm as} < \tau \leqslant 0.72$ Eve's optimal strategy is a hybrid combination of both individual and coherent attacks, and for $\tau > 0.72$ coherent attacks are optimal. In Fig. 2, in the finite-size case when $\tau \leqslant \tau_c^{\rm fs} = 0.23$ individual attacks are optimal, and for $\tau > \tau_c^{\rm fs}$ (where the optimal value of μ indicates hybrid attacks are optimal for $\tau_c^{\rm fs} < \tau \leqslant 0.7$, and coherent attacks are optimal for $\tau > 0.7$) a positive finite key rate cannot be generated, and the protocol is not secure against hybrid attacks. That is why the black circled line (i.e., the finite key rate secure against hybrid attacks) has not been shown for $\tau > \tau_c^{\rm fs}$. Note that

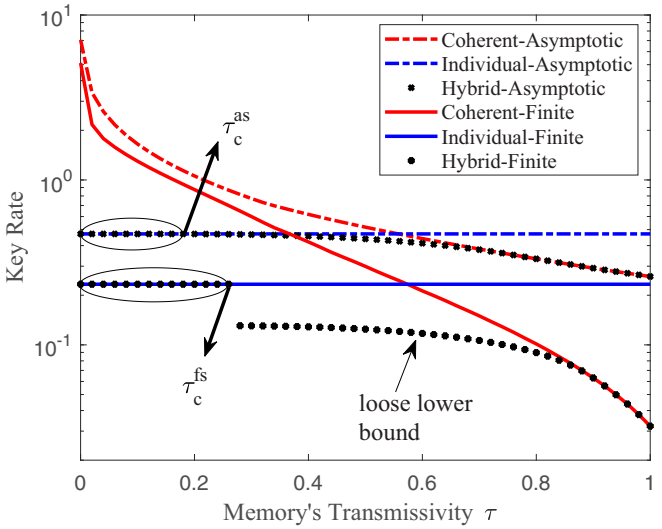

FIG. 3. Same as Fig. 2 except here we have a low-loss channel with $T = 0.5$.

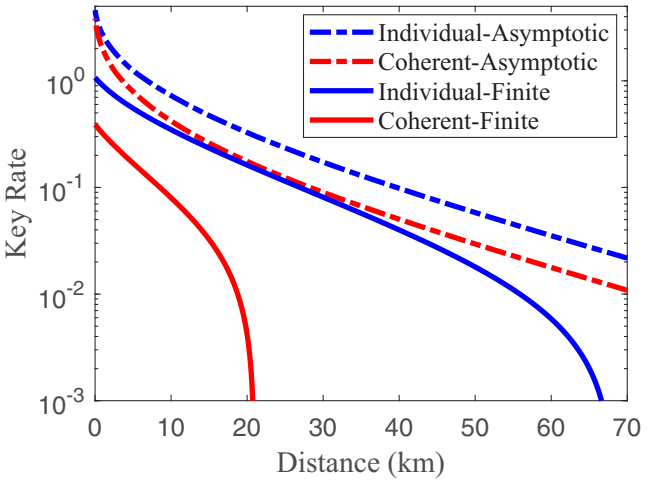

FIG. 4. The finite-size and asymptotic key rate as a function of channel distance (with the assumption of 0.2 dB loss per kilometer) for individual (blue) and perfect coherent attacks (red). The numerical values are the same as Fig. 2.

in the presence of memory's thermal noise (i.e., $\omega > 1$) the threshold transmissivity becomes higher than that in the case of Eve's pure-loss quantum memory (i.e., $\omega = 1$).

We repeat our numerical simulations for a low-loss quantum channel in Fig. 3, which result in similar trends to high-loss channels. Asymptotically we see that when $\tau \leqslant \tau_c^{as} = 0.18$ individual attacks are optimal, for $\tau_c^{as} < \tau \leqslant 0.75$ Eve's optimal strategy is a hybrid combination of both individual and coherent attacks, and for $\tau > 0.75$ coherent attacks are optimal. In the finite-size case when $\tau \leqslant \tau_c^{fs} = 0.26$ individual attacks are optimal, for $\tau_c^{fs} < \tau \leqslant 0.89$ Eve's optimal strategy is a hybrid combination of both individual and coherent attacks (only a loose lower bound on the finite-size hybrid key rate can be calculated), and for $\tau > 0.89$ coherent attacks are optimal.

Note that in Figs. 2 and 3 the threshold transmissivity of the finite-size regime is higher than that of the asymptotic regime, since the finite key rate is calculated based on the estimated values of the channel (see Appendix A for more details), while the asymptotic key rate is calculated based on the expected values of the channel. Note also that in Fig. 3 for the transmissivities $\tau > \tau_c^{fs}$ which are close to τ_c^{fs}, the optimal value of μ is close to zero, which means most of Eve's signal undergoes the individual measurement in the hybrid scheme. However, we can see a discontinuity in the finite key rate around τ_c^{fs}, which is because the Δ term (and also ϵ_{PE}) for the hybrid attack is always chosen pessimistically much larger (much smaller) than that of the individual attack, even when the hybrid attack is very close to the individual attack.

Additional calculations beyond those illustrated here have been carried out covering direct reconciliation (DR), which results in similar trends to those indicated here. However, DR is successful only when the channel loss is below 3 dB. For instance, in the DR scenario of the no-switching protocol with the same parameters as Fig. 3, individual attacks result in positive finite key rates only for low-loss channels with $T \geqslant 0.72$. Hence, if Eve's decoherence is large enough to make individual attacks the optimal attacks, positive finite key rates can be generated only for $T \geqslant 0.72$.

Thus, we find that our analysis can translate a model for the decoherence of Eve's attack into a rigorous, quantifiable bound on performance. This fact results in a remarkable improvement of the key rate up to that achievable under the assumption of individual attacks. For a Gaussian-channel model we generically find a threshold value for the overall decoherence of Eve's attack above which the mutual information between Bob and Eve is degraded so severely that Eve is forced to make an individual attack. These results are of significant practical relevance. For instance, Fig. 2 shows that while positive finite key rates cannot be generated under the unrealistic assumption of perfect coherent attacks, by considering Eve's attack decoherence we are able to move from an insecure regime to a secure regime and generate nontrivial positive finite key rates. Figure 4 also shows the advantage of individual attacks over perfect coherent attacks in terms of the maximum secure transmission distance of the CV-QKD protocol, where this advantage is significant, especially in the finite-size regime.

VI. DISCUSSION

In our model of restricted attack we make no assumption on the size of Eve's quantum memory. In fact, we assume a less-restricted assumption on Eve's storage ability where she is able to store *all* the ancillary modes. However, we assume any mode stored into the memory undergoes the same amount of decoherence. It could also be reasonable to consider a bounded memory, where only a small fraction of the total modes can be stored and the rest of them are only individually measured. Further, it would be more realistic to consider different amounts of decoherence for Eve's stored ancillary modes, as some of them are stored in the memory longer than others. Finally, it would be desirable to extend this result to the other Gaussian CV-QKD protocols, although this would

require solving the open problem of explicitly identifying the corresponding optimal attacks.

VII. CONCLUSIONS

Given the realistic restriction that in a coherent (or collective) attack, Eve's quantum system undergoes a certain amount of decoherence over the storage and processing time, we found that there is always a threshold for Eve's decoherence above which Eve's best strategy is limited to individual attacks. Since the decoherence is an increasing function of the storage time, if Eve's required time to store the entire ensemble and perform a collective measurement on the stored ensemble is sufficiently long, the security analysis of the protocol reduces to that of individual attacks, which substantially improves the key rate and the secure transmission distance of the CV-QKD protocol.

ACKNOWLEDGMENTS

The authors gratefully acknowledge valuable discussions with Andrew Lance, Thomas Symul, and Helen M. Chrzanowski. This research was supported by funding from the Australian Department of Defence. This research is also supported by the Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE170100012). N.W. acknowledges funding support from the EPSRC National Quantum Technology Hub in Networked Quantum Information Technologies and funding from the European Union's Horizon 2020 Research and Innovation Program under Marie Sklodowska-Curie Grant Agreement No. 750905.

APPENDIX A: COMPOSABLE FINITE-SIZE SECURITY ANALYSIS

In the finite-size security analysis the key is proved to be secure against Eve's attacks up to a small failure probability, while in the asymptotic security analysis the key is proved to be perfectly secure in the limit of infinite quantum states distributed between Alice and Bob.

The security of a QKD protocol against general attacks is established by proving that the *real* protocol is approximately equal to an *ideal* protocol. We first introduce the properties an ideal protocol is required to achieve—correctness, secrecy, and robustness. Note that an entanglement-based QKD protocol can be described as a completely positive trace-preserving map that takes an input state ρ_{AB} and outputs a key consisting of two classical strings S_A and S_B on Alice's and Bob's side, respectively. The protocol is correct when $S_A = S_B$. The resultant key is secret when S_A is uniformly distributed and is uncorrelated with Eve's system. A protocol is called secure if it is both correct and secret. The protocol is robust if it never aborts when Eve is passive (i.e., Eve does not disturb the quantum channel) [24,25].

However, for a real protocol we can only hope to achieve an almost ideal protocol up to small failure probabilities $\epsilon_{\rm cor}$ and $\epsilon_{\rm sec}$. The protocol is $\epsilon_{\rm cor}$-correct when $\Pr[S_A \neq S_B] \leqslant \epsilon_{\rm cor}$. The protocol is $\epsilon_{\rm sec}$-secret when the key is δ-close in trace distance to a uniformly distributed key that is uncorrelated with Eve's system, i.e., $\frac{1}{2}\|\rho_{S_A E'} - \tau_{S_A} \otimes \rho_{E'}\| \leqslant \delta$ and $(1 - p_{\rm abort})\delta \leqslant \epsilon_{\rm sec}$, where $\|.\|$ is the trace norm and $p_{\rm abort}$ is the probability to abort. In this definition τ_{S_A} is the uniform (i.e., fully mixed) state over S_A, $\rho_{E'}$ are states on Eve's system E' (which characterizes Eve's quantum states E, as well as the public classical information C leaked during the QKD protocol), and $\rho_{S_A E'} = \sum_s |s\rangle\langle s| \otimes \rho^s_{E'}$ is a classical quantum state describing the state of S_A and Eve's system E' [24,25]. A QKD protocol is called ϵ-secure when it is $\epsilon_{\rm cor}$-correct and $\epsilon_{\rm sec}$-secret, with $\epsilon_{\rm cor} + \epsilon_{\rm sec} \leqslant \epsilon$ [24,25]. Note that this security definition also ensures that the QKD protocol is secure in the framework of composable security [24,25], in which different cryptographic protocols can be combined without compromising the overall security.

Let us consider the equivalent entanglement-based scheme of a no-switching CV-QKD protocol [4,5] in the reverse reconciliation scheme where Alice prepares $N = 2n$ two-mode squeezed vacuum states with the quadrature variance V, keeping the first mode of each state while sending the second mode to Bob over an insecure quantum channel with transmissivity T and excess noise ξ (relative to the input of the quantum channel). Alice and Bob measure their own modes with heterodyne detection to obtain two strings: $X \in \mathbb{R}^{4n}$ and $Y \in \mathbb{R}^{4n}$. Bob discretizes his string by dividing the continuous range of his quadrature variables Y into 2^d intervals $\mathcal{I}_1, ..., \mathcal{I}_{2^d}$ of the normal distribution, where d is the discretization parameter. Bob applies the discretization map $\mathcal{D} : Y \to U$ such that $\mathcal{D}(Y_k) = j$ if $Y_k \in \mathcal{I}_j$ [24]. As a result of the discretization, Bob ends up with the $m = 4dn$-bit string U, where each symbol is encoded with d bits of precision.

Here, similar to [24] we assume parameter estimation can be performed after the reconciliation (or error correction). This assumption leads to the improvement of parameter estimation and enables us to use almost all the raw data to distill the secret key. In the error-correction step based on a linear error-correcting code agreed on in advance, Bob sends the syndrome of his vector U of size $l_{\rm EC}$ to Alice, who outputs an estimate $\hat{U}$ of U. In order to know whether the error correction passed (i.e., $\hat{U} = U$), Alice and Bob compute a hash of their strings $\hat{U}$ and U, respectively. Bob then reveals his hash to Alice. If both hashes coincide, the protocol proceeds; otherwise it aborts. Note that the syndrome of size $l_{\rm EC}$ contributes to most of the leakage during the error correction. In the parameter estimation which is performed after the error correction, Bob sends only a few additional bits of information to Alice that allow her to compute the covariance matrix of the state $\rho_{AB}^{\otimes(2n)}$ as well as a confidence region for the covariance matrix. (For a detailed discussion of the parameter estimation and how Alice and Bob know the parameter estimation passed, see Ref. [24].) We indicate the maximum failure probabilities for the error correction and parameter estimation steps with $\epsilon_{\rm cor}$ and $\epsilon_{\rm PE}$. In the privacy amplification step Alice and Bob apply a random universal$_2$ hash function to their respective strings in order to extract two strings S_A and S_B of size ℓ.

Based on the leftover hash lemma [41,42], the key of size ℓ is $\epsilon_{\rm sec}$-secret, provided that ℓ is slightly smaller than the smooth min-entropy of Bob's string U conditioned on Eve's system E', $H_{\min}^{\epsilon_{\rm sm}}(U^m|E')$ [41], where m indicates

the length of the string U, and $\epsilon_{\rm sm}$ is the smoothing parameter which is dependent on the value of $\epsilon_{\rm sec}$.[1] The conditional smooth min-entropy $H_{\min}^{\epsilon_{\rm sm}}(U^m|E')$ characterizes Eve's uncertainty (or lack of knowledge) about Bob's string U. Note that the chain rule for the smooth min-entropy [24] gives $H_{\min}^{\epsilon_{\rm sm}}(U^m|E') = H_{\min}^{\epsilon_{\rm sm}}(U^m|EC) \geqslant H_{\min}^{\epsilon_{\rm sm}}(U^m|E) - \log_2|C|$, where $\log_2|C| = l_{\rm EC}$.

In order to calculate the length ℓ of the final key which is ϵ-secure, the conditional smooth min-entropy $H_{\min}^{\epsilon_{\rm sm}}(U^m|E)$ has to be lower bounded when the protocol did not abort, but this is usually a hard task. However, under the assumption of individual and collective attacks (meaning that every signal sent from Alice to Bob is attacked with the same quantum operation), where the state between Alice, Bob, and Eve has a tensor product structure, we can employ the asymptotic equipartition property [24,43,44] and provide a bound in terms of von Neumann entropy. This property states that for large N, the conditional smooth min-entropy approaches the conditional von Neumann entropy. Explicitly, we have $H_{\min}^{\epsilon_{\rm sm}}(U^m|E) \geqslant S(U^m|E) - \Delta_{\rm AEP}$ [24], where $S(U^m|E)$ is the conditional von Neumann entropy, and $\Delta_{\rm AEP} = \sqrt{N}[(d+1)^2 + 4(d+1)\sqrt{\log_2(2/\epsilon_{\rm sm}^2)} + 2\log_2(2/(\epsilon^2\epsilon_{\rm sm}))] + 4\epsilon_{\rm sm}d/\epsilon$ [24,28]. The conditional von Neumann entropy $S(U^m|E)$ is given by $S(U^m|E) = NH(U) - N\chi(U{:}E)$, where $H(U)$ is Bob's Shannon entropy and $\chi(U{:}E)$ is the Holevo information between Eve and Bob for collective attacks. Note that for individual attacks $\chi(U{:}E)$ must be replaced by the Shannon mutual information between Eve and Bob, $I(U{:}E)$.

According to the security theorem proved in [24,28], the no-switching CV-QKD protocol is ϵ-secure against collective attacks if [2]

$$\epsilon = 2\epsilon_{\rm sm} + \bar{\epsilon} + \epsilon_{\rm PE} + \epsilon_{\rm cor} \tag{A1}$$

and if the key length ℓ is chosen such that[3]

$$\ell \leqslant N[H(U) - \chi(U{:}E)] - l_{\rm EC} - \Delta_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right). \tag{A2}$$

Considering that the leakage during the error correction is given by $l_{\rm EC} = N[H(U) - \beta I(A{:}B)]$ [24,25,28], where $I(A{:}B)$ is the Shannon mutual information between Alice and Bob, we can rewrite Eq. (A2) as

$$\ell \leqslant N[\beta I(A{:}B) - \chi(U{:}E)] - \Delta_{\rm AEP} - 2\log_2\left(\frac{1}{2\bar{\epsilon}}\right), \tag{A3}$$

where $\chi(U{:}E)$ is upper bounded by $\chi(Y{:}E) = \chi(B{:}E)$, since the discretization algorithm cannot increase the mutual information. According to [24] the Holevo information $\chi(B{:}E)$ can be calculated based on a covariance matrix $\mathbf{M}_{ab} = [\sum_a^{\max}\mathbf{I}, \sum_c^{\min}\mathbf{Z}; \sum_c^{\min}\mathbf{Z}, \sum_b^{\max}\mathbf{I}]$ with $\mathbf{I}$ a 2×2 identity matrix, and $\mathbf{Z} = \mathrm{diag}(1,-1)$, where the elements of $\mathbf{M}_{ab}$ provide a bound on the elements of the covariance matrix of the state shared between Alice and Bob:

$$\begin{aligned}
\sum_a^{\max} &= \frac{1}{2n}\left[1 + 2\sqrt{\frac{\log(36/\epsilon_{\rm PE})}{n}}\right]\|X\|^2 - 1,\\
\sum_b^{\max} &= \frac{1}{2n}\left[1 + 2\sqrt{\frac{\log(36/\epsilon_{\rm PE})}{n}}\right]\|Y\|^2 - 1,\\
\sum_c^{\min} &= \frac{1}{2n}\langle X, Y\rangle - 5\sqrt{\frac{\log(8/\epsilon_{\rm PE})}{n^3}}(\|X\|^2 + \|Y\|^2),
\end{aligned} \tag{A4}$$

where $\|X\|^2$, $\|Y\|^2$, $\langle X, Y\rangle$ can be achieved by taking values differing by three standard deviations from the expected values [24] (for an expected Gaussian channel with parameters T and ξ). It is then assumed that Eve's information can be upper bounded by calculating $\chi(B{:}E)$ based on the covariance matrix $\mathbf{M}_{ab}$, except with the probability of $\epsilon_{\rm PE}$.

The final key rate where the key is ϵ-secure against collective attacks is given by ℓ/N. We recall that in Eq. (A3) we have considered the same scenario as [24], where almost all the raw data can be utilized to distill the secret key[4] (by performing the parameter estimation after the error correction). However, if the parameter estimation is performed before the error correction, Alice and Bob are required to disclose a non-negligible number of data points of size $N_{\rm PE}$ during the parameter estimation, which means a classical data of size N' is used for the key extraction, where $N' = N - N_{\rm PE}$. As a result, the final secure key rate is given by ℓ/N, where ℓ is given by Eq. (A3), but now N in Eq. (A3) has to be replaced by N'.

In order to prove the security of the no-switching CV-QKD protocol against coherent attacks, we apply the Gaussian

[1] In fact, the $\epsilon_{\rm sm}$-smooth min-entropy of Bob's string U conditioned on Eve's system characterizes that given Eve's system, how much $\epsilon_{\rm sm}$-close to uniform randomness (which is uncorrelated with Eve's system) can be extracted from the random variable U.

[2] Note that terms here are slightly different to [24] because, as pointed out in [28], they are unnecessarily pessimistic on two counts. First, in Theorem 1 of the Supplemental Information of [24], the terms $\epsilon_{\rm PE}$ and $\epsilon_{\rm cor}$ are both divided by p (the unknown passing probability of the protocol), which is subsequently lower bounded by ϵ, the overall collective security parameter. This is unnecessarily pessimistic and stems from substituting the unconditional failure probability for parameter estimation and error correction, which are indeed $\epsilon_{\rm PE}/p$ and $\epsilon_{\rm cor}/p$, respectively. However, the quantity in Eq. (A1) is conditioned upon passing the test; therefore the terms should be multiplied by p, which cancels. Second, in [24] an extra step is introduced to bound the Shannon entropy appearing in Eq. (A2) by the so-called empirical entropy. This leads to an extra correction term in Eq. (A2) and an extra failure probability in Eq. (A1). However, neither of these are necessary, since the term $NH(U) - l_{\rm EC}$ is directly measured in an experiment. Therefore it does not need to be rigorously bounded by the empirical entropy but can instead be modeled for the purposes of plotting the expected key rate by $N\beta I(A{:}B)$.

[3] Note that $\bar{\epsilon}$ comes from the leftover hash lemma [24].

[4] Note that it has been recently shown in [29] that in CV-QKD the whole raw keys can be used for both parameter estimation and secret key generation, without compromising the security and without any requirements of doing error correction before parameter estimation.

de Finetti reduction technique [6]. In order to apply this technique we need to truncate the Hilbert space in a suitable manner. This can be achieved with the help of an energy test [6], which ensures that the state shared between Alice and Bob is suitably described by assigning a low-dimensional Hilbert space. Considering the input state shared between Alice and Bob is a $2(N+k)$-mode state, Alice and Bob should symmetrize this state and measure the last k modes with heterodyne detection. If the average energy per mode is below d_A for Alice and d_B for Bob, the energy test passes and Alice and Bob apply the CV-QKD to their remaining modes; otherwise the protocol aborts. The thresholds d_A and d_B should be chosen properly to ensure that the energy test passes with large success probability.

According to the security theorem proved in [6], if we are given a no-switching CV-QKD protocol acting on a $2N$-mode state shared between Alice and Bob (which is suitably symmetrized) such that the protocol is ϵ-secure against Gaussian collective attacks, the modified protocol, including an energy test and an additional privacy amplification step [6], is $\tilde{\epsilon}$-secure against coherent attacks, with $\tilde{\epsilon} = (K^4/50)\epsilon$, where

$$K = \max\{1, N(d_A+d_B)(1+2\sqrt{[(\ln(8/\epsilon))/2N]} + (\ln(8/\epsilon))/N)(1-2\sqrt{[(\ln(8/\epsilon))/2k]})^{-1}\}. \quad \text{(A5)}$$

Thus, the security loss due to the reduction from coherent attacks to collective attacks scales like $O(N^4)$.

Note that in our numerical calculations of finite-size key rate we do not directly use the covariance matrix shared between Alice and Bob given by $\mathbf{M}_{ab}$ to compute the key rate. More specifically, we first calculate the matrix $\mathbf{M}_{ab}$ and then estimate the required parameters (T, ξ, and V) from the elements of the matrix $\mathbf{M}_{ab}$, and then proceed to compute the key rate based on the calculations provided in the next sections.

APPENDIX B: CALCULATION OF $I(A:B)$

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

$$\mathbf{M}_{AB} = \begin{bmatrix} V\,\mathbf{I} & \sqrt{V^2-1}\,\mathbf{Z} \\ \sqrt{V^2-1}\,\mathbf{Z} & V\,\mathbf{I} \end{bmatrix}. \quad \text{(B1)}$$

After transmission of mode B through a quantum channel with transmissivity T and excess noise ξ, the covariance matrix of the mixed state ρ_{AB_1} at the output of the channel is given by

$$\mathbf{M}_{AB_1} = \begin{bmatrix} V\,\mathbf{I} & \sqrt{T}\sqrt{V^2-1}\,\mathbf{Z} \\ \sqrt{T}\sqrt{V^2-1}\,\mathbf{Z} & [T(V+\chi_{\text{line}})]\,\mathbf{I} \end{bmatrix}, \quad \text{(B2)}$$

where $\chi_{\text{line}} = \xi + \frac{1}{T} - 1$. At the output of the channel, Bob applies heterodyne detection to mode B_1. Bob's heterodyne detector, with efficiency η and electronic noise variance υ_{el}, can be modeled by placing a beam splitter of transmissivity η before an ideal heterodyne detector [22,23]. The heterodyne detector's electronic noise can be modeled by a two-mode squeezed vacuum state ρ_{F_0G} of quadrature variance υ, where $\upsilon = 1 + 2\upsilon_{\text{el}}/(1-\eta)$. 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.

The Shannon mutual information between Alice and Bob, $I(A:B)$, is given by

$$I(A:B) = \log_2 \frac{V_{B_2^{\text{het}}}}{V_{B_2^{\text{het}}|A^{\text{het}}}}, \quad \text{(B3)}$$

where $V_{B_2^{\text{het}}}$ is the variance of heterodyne-detected mode B_2 and is given by $V_{B_2^{\text{het}}} = \eta T(V+\chi_{\text{tot}})/2$, where $\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}$ and $\chi_{\text{het}} = [1+(1-\eta)+2\upsilon_{\text{el}}]/\eta$. 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 $V_{B_2^{\text{het}}|A^{\text{het}}} = \eta T(1+\chi_{\text{tot}})/2$.

APPENDIX C: CALCULATION OF $I_\mu^{\text{hyb}}(B:E)$

The upper bound on the mutual information between Eve and Bob in the hybrid attack, $I_\mu^{\text{hyb}}(B:E)$, is given by

$$I_\mu^{\text{hyb}}(B:E) = I_\mu^{\text{hyb}}(B:E_1'E_2'E_1''E_2'') = \chi_\mu(BE_1''E_2'':E_1'E_2') + I_\mu(B:E_1''E_2'') - \chi_\mu(E_1''E_2'':E_1'E_2'). \quad \text{(C1)}$$

We now analyze the calculation of the mutual information terms on the right-hand side of Eq. (C1).

1. Calculation of $\chi_\mu(BE_1''E_2'':E_1'E_2')$

In Eq. (C1) the Holevo mutual information $\chi_\mu(BE_1''E_2'':E_1'E_2')$ is given by

$$\chi_\mu(BE_1''E_2'':E_1'E_2') = S(\rho_{E_1'E_2'}) - S(\rho_{E_1'E_2'|E_1''E_2''B_2}), \quad \text{(C2)}$$

where $S(\rho)$ is the von Neumann entropy[5] of the quantum state ρ. Note that here we assume Bob's detection noise is not accessible to Eve. The first entropy $S(\rho_{E_1'E_2'})$ is calculated through the symplectic eigenvalues of the covariance matrix $\mathbf{M}_{E_1'E_2'}$, which is given by

$$\mathbf{M}_{E_1'E_2'} = \begin{bmatrix} [\tau_1 V_{E_1^c} + (1-\tau_1)\omega_1]\mathbf{I} & \sqrt{\tau_1\tau_2}C_{E_1^c,E_2^c}\mathbf{Z} \\ \sqrt{\tau_1\tau_2}C_{E_1^c,E_2^c}\mathbf{Z} & [\tau_2 V_{E_2^c} + (1-\tau_2)\omega_2]\mathbf{I} \end{bmatrix}, \quad \text{(C3)}$$

where $V_{E_1^c} = \mu V_{E_1} + (1-\mu)$, $V_{E_2^c} = \mu V_{E_2} + (1-\mu)$, and $C_{E_1^c,E_2^c} = \mu C_{E_1,E_2}$. Note that $V_{E_1} = T\omega_E + (1-T)V$, $V_{E_2} = \omega_E$, and $C_{E_1,E_2} = \sqrt{T}\sqrt{\omega_E^2-1}$. The second entropy we require in order to determine $\chi_\mu(BE_1''E_2'':E_1'E_2')$ is $S(\rho_{E_1'E_2'|E_1''E_2''B_2})$, which is calculated through the symplectic eigenvalues of the conditional covariance matrix $\mathbf{M}_{E_1'E_2'|E_1''E_2''B_2}$. This conditional covariance matrix is actually the covariance matrix of the quantum state $\rho_{E_1'E_2'}$ conditioned on the homodyne detection of modes $E_1''E_2''$ and heterodyne detection of mode B_2. Let us recall that the heterodyne detection of

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

mode B_2 is the combination of mode B_2 with a vacuum mode in a balanced beam splitter, which outputs mode B_3 and mode C, where the $\hat{q}$ ($\hat{p}$) quadrature is measured on mode B_3 (mode C) using a homodyne detector. Hence, the heterodyne detection on mode B_2 is actually a conjugate homodyne detection on modes B_3 and C. In this case we have $\mathbf{M}_{E_1'E_2'|E_1''E_2''B_2} = \mathbf{M}_{E_1'E_2'|E_1''E_2''B_3C}$, where we have

$$\mathbf{M}_{E_1'E_2'|E_1''E_2''B_3C} = \mathbf{M}_{E_1'E_2'} - \boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''B_3C}\ \mathbf{H}_{\text{hom}}\ \boldsymbol{\sigma}^T_{E_1'E_2',E_1''E_2''B_3C}. \tag{C4}$$

In Eq. (C4) the covariance matrix $\mathbf{M}_{E_1'E_2'}$ is given by Eq. (C3), and the matrix $\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''B_3C}$ is given by

$$\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''B_3C} = \begin{bmatrix}\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''} & \boldsymbol{\sigma}_{E_1'E_2',B_3} & \boldsymbol{\sigma}_{E_1'E_2',C}\end{bmatrix}. \tag{C5}$$

In Eq. (C5) the matrix $\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''}$ is given by

$$\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''} = \begin{bmatrix} C_{q_{E_1'},q_{E_1''}} & 0 & C_{q_{E_1'},q_{E_2''}} & 0 \\ 0 & C_{p_{E_1'},p_{E_1''}} & 0 & C_{p_{E_1'},p_{E_2''}} \\ C_{q_{E_2'},q_{E_1''}} & 0 & C_{q_{E_2'},q_{E_2''}} & 0 \\ 0 & C_{p_{E_2'},p_{E_1''}} & 0 & C_{p_{E_2'},p_{E_2''}} \end{bmatrix}. \tag{C6}$$

In Eq. (C6) we have $C_{q_{E_1'},q_{E_1''}} = C_{p_{E_1'},p_{E_2''}} = (C_{E_1^i,E_1'} - C_{E_2^i,E_1'})/\sqrt{2}$, $C_{p_{E_1'},p_{E_1''}} = C_{q_{E_1'},q_{E_2''}} = (C_{E_1^i,E_1'} + C_{E_2^i,E_1'})/\sqrt{2}$, $C_{q_{E_2'},q_{E_2''}} = -C_{p_{E_2'},p_{E_1''}} = (C_{E_1^i,E_2'} + C_{E_2^i,E_2'})/\sqrt{2}$, and $C_{p_{E_2'},p_{E_2''}} = -C_{q_{E_2'},q_{E_1''}} = (-C_{E_1^i,E_2'} + C_{E_2^i,E_2'})/\sqrt{2}$, and where

$$\begin{aligned} C_{E_1^i,E_1'} &= \sqrt{\tau_1(1-\mu)\mu}(1 - V_{E_1}), \\ C_{E_2^i,E_1'} &= -\sqrt{\tau_1(1-\mu)\mu}C_{E_1,E_2}, \\ C_{E_1^i,E_2'} &= -\sqrt{\tau_2(1-\mu)\mu}C_{E_1,E_2}, \\ C_{E_2^i,E_2'} &= \sqrt{\tau_2(1-\mu)\mu}(1 - V_{E_2}). \end{aligned} \tag{C7}$$

In Eq. (C5) the matrices $\boldsymbol{\sigma}_{E_1'E_2',B_3}$ and $\boldsymbol{\sigma}_{E_1'E_2',C}$ are given by $\boldsymbol{\sigma}_{E_1'E_2',B_3} = -\boldsymbol{\sigma}_{E_1'E_2',C} = \frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{E_1'E_2',B_2}$, where we have

$$\boldsymbol{\sigma}_{E_1'E_2',B_2} = \begin{bmatrix} \sqrt{\tau_1\mu(1-T)T\eta}(\omega_E - V)\mathbf{I} \\ \sqrt{\tau_2\mu(1-T)\eta}\sqrt{\omega_E^2 - 1}\mathbf{Z} \end{bmatrix}. \tag{C8}$$

In Eq. (C4) the matrix $\mathbf{H}_{\text{hom}}$ is given by $\mathbf{H}_{\text{hom}} = (\mathbf{X}\mathbf{M}_{E_1''E_2''B_3C}\mathbf{X})^{\text{MP}}$, where $\mathbf{X} = \text{diag}(1, 0, 0, 1, 1, 0, 0, 1)$, MP stands for the Moore-Penrose pseudoinverse of a matrix, and the covariance matrix $\mathbf{M}_{E_1''E_2''B_3C}$ is given by

$$\mathbf{M}_{E_1''E_2''B_3C} = \begin{bmatrix} \mathbf{M}_{E_1''E_2''} & \boldsymbol{\sigma}^T_{B_3,E_1''E_2''} & \boldsymbol{\sigma}^T_{C,E_1''E_2''} \\ \boldsymbol{\sigma}_{B_3,E_1''E_2''} & \mathbf{M}_{B_3} & \boldsymbol{\sigma}^T_{C,B_3} \\ \boldsymbol{\sigma}_{C,E_1''E_2''} & \boldsymbol{\sigma}_{C,B_3} & \mathbf{M}_C \end{bmatrix}. \tag{C9}$$

In Eq. (C9) the covariance matrix $\mathbf{M}_{E_1''E_2''}$ is given by

$$\mathbf{M}_{E_1''E_2''} = \begin{bmatrix} V_{q_{E_1''}} & 0 & C_{q_{E_1''},q_{E_2''}} & 0 \\ 0 & V_{p_{E_1''}} & 0 & C_{p_{E_1''},p_{E_2''}} \\ C_{q_{E_1''},q_{E_2''}} & 0 & V_{q_{E_2''}} & 0 \\ 0 & C_{p_{E_1''},p_{E_2''}} & 0 & V_{p_{E_2''}} \end{bmatrix}, \tag{C10}$$

where $V_{q_{E_1''}} = V_{p_{E_2''}} = (V_{E_1^i} + V_{E_2^i})/2 - C_{E_1^i,E_2^i}$, $V_{p_{E_1''}} = V_{q_{E_2''}} = (V_{E_1^i} + V_{E_2^i})/2 + C_{E_1^i,E_2^i}$, and $C_{q_{E_1''},q_{E_2''}} = C_{p_{E_1''},p_{E_2''}} = (V_{E_1^i} - V_{E_2^i})/2$, and where

$$\begin{aligned} V_{E_1^i} &= (1-\mu)V_{E_1} + \mu, \quad V_{E_2^i} = (1-\mu)V_{E_2} + \mu, \\ C_{E_1^i,E_2^i} &= (1-\mu)C_{E_1,E_2}. \end{aligned} \tag{C11}$$

In Eq. (C9) the matrices $\boldsymbol{\sigma}_{B_3,E_1''E_2''}$ and $\boldsymbol{\sigma}_{C,E_1''E_2''}$ are given by $\boldsymbol{\sigma}_{B_3,E_1''E_2''} = -\boldsymbol{\sigma}_{C,E_1''E_2''} = \frac{1}{\sqrt{2}}\boldsymbol{\sigma}_{B_2,E_1''E_2''}$, where

$$\boldsymbol{\sigma}_{B_2,E_1''E_2''} = \begin{bmatrix} C_{q_{B_2},q_{E_1''}} & 0 & C_{q_{B_2},q_{E_2''}} & 0 \\ 0 & C_{p_{B_2},p_{E_1''}} & 0 & C_{p_{B_2},p_{E_2''}} \end{bmatrix}. \tag{C12}$$

In Eq. (C12) we have $C_{q_{B_2},q_{E_1''}} = C_{p_{B_2},p_{E_2''}} = (C_{B_2,E_1^i} - C_{B_2,E_2^i})/\sqrt{2}$ and $C_{p_{B_2},p_{E_1''}} = C_{q_{B_2},q_{E_2''}} = (C_{B_2,E_1^i} + C_{B_2,E_2^i})/\sqrt{2}$, and where

$$\begin{aligned} C_{B_2,E_1^i} &= \sqrt{(1-\mu)(1-T)T\eta}(V-\omega_E), \\ C_{B_2,E_2^i} &= -\sqrt{(1-\mu)(1-T)\eta}\sqrt{\omega_E^2-1}. \end{aligned} \tag{C13}$$

In Eq. (C9) we have $\mathbf{M}_{B_3} = \mathbf{M}_C = 0.5(V_{B_2}+1)\mathbf{I}$ and $\boldsymbol{\sigma}_{C,B_3} = 0.5(1-V_{B_2})\mathbf{I}$, where $V_{B_2} = \eta T(V+\chi_t)$ and where $\chi_t = \chi_{\text{line}} + \frac{\chi_D}{T}$, and where $\chi_D = [(1-\eta)+2\upsilon_{\text{el}}]/\eta$.

2. Calculation of $I_\mu(B : E_1''E_2'')$

In Eq. (C1) the Shannon mutual information $I_\mu(B : E_1''E_2'')$ is given by

$$I_\mu(B : E_1''E_2'') = \frac{1}{2}\log_2\frac{V_{B_2^{\text{het}}}}{V_{q_{B_2^{\text{het}}}|q_{E_1''}}} + \frac{1}{2}\log_2\frac{V_{B_2^{\text{het}}}}{V_{p_{B_2^{\text{het}}}|p_{E_2''}}}, \tag{C14}$$

where $V_{q_{B_2^{\text{het}}}|q_{E_1''}}$ is the variance of the $\hat{q}$ quadrature of heterodyne-detected mode B_2 conditioned on Eve's homodyne detection of the $\hat{q}$ quadrature of mode E_1'' and is given by $V_{q_{B_2^{\text{het}}}|q_{E_1''}} = (V_{q_{B_2}|q_{E_1''}}+1)/2$, and similarly for the $\hat{p}$ quadrature we have $V_{p_{B_2^{\text{het}}}|p_{E_2''}} = (V_{p_{B_2}|p_{E_2''}}+1)/2$. The symmetry of Eve's information on $\hat{q}_{B_2}$ and $\hat{p}_{B_2}$ imposes that $V_{q_{B_2}|q_{E_1''}} = V_{p_{B_2}|p_{E_2''}}$. Note that $V_{q_{B_2}|q_{E_1''}} = V_{q_{B_2}} - C_{q_{B_2},q_{E_1''}}/V_{q_{E_1''}}$, where $V_{q_{B_2}} = \eta T(V+\chi_t)$. Note also that $V_{B_2^{\text{het}}}$, $C_{q_{B_2},q_{E_1''}}$, and $V_{q_{E_1''}}$ have been already calculated and provided in the previous sections.

3. Calculation of $\chi_\mu(E_1''E_2'' : E_1'E_2')$

In Eq. (C1) the Holevo information $\chi_\mu(E_1''E_2'' : E_1'E_2')$ is given by

$$\chi_\mu(E_1''E_2'' : E_1'E_2') = S\big(\rho_{E_1'E_2'}\big) - S\big(\rho_{E_1'E_2'|E_1''E_2''}\big). \tag{C15}$$

The conditional entropy $S(\rho_{E_1'E_2'|E_1''E_2''})$ is calculated through the symplectic eigenvalues of the conditional covariance matrix $\mathbf{M}_{E_1'E_2'|E_1''E_2''}$. This conditional covariance matrix is given by

$$\mathbf{M}_{E_1'E_2'|E_1''E_2''} = \mathbf{M}_{E_1'E_2'} - \boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''}\ \mathbf{H}_{\text{hom}}^i\ \boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''}^T. \tag{C16}$$

The matrix $\mathbf{H}_{\text{hom}}^i$ is given by $\mathbf{H}_{\text{hom}}^i = (\mathbf{X}_i\mathbf{M}_{E_1''E_2''}\mathbf{X}_i)^{\text{MP}}$, where $\mathbf{X}_i = \text{diag}(1,0,0,1)$. Note that the matrices $\mathbf{M}_{E_1'E_2'}$, $\boldsymbol{\sigma}_{E_1'E_2',E_1''E_2''}$, and $\mathbf{M}_{E_1''E_2''}$ are given by Eqs. (C3), (C6), and (C10), respectively.

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

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

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

[4] 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).

[5] 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).

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

[7] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Inf. Transm. (Engl. Transl.) **9**, 177 (1973).

[8] A. S. Holevo, The capacity of quantum channel with general signal states, IEEE Trans. Inf. Theory **44**, 269 (1998).

[9] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, Phys. Rev. A **56**, 131 (1997).

[10] V. Giovannetti, S. Lloyd, and L. Maccone, Achieving the Holevo bound via sequential measurements, Phys. Rev. A **85**, 012302 (2012).

[11] V. Giovannetti, S. Lloyd, and L. Maccone, Explicit capacity-achieving receivers for optical communication and quantum reading, *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Cambridge, MA (IEEE, New York, 2012), pp. 551–555.

[12] M. Rosati and V. Giovannetti, Achieving the Holevo bound via a bisection decoding protocol, J. Math. Phys. **57**, 062204 (2016).

[13] C. Lupo and S. Lloyd, Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate, Phys. Rev. Lett. **113**, 160502 (2014).

[14] C. Lupo and S. Lloyd, Quantum data locking for high-rate private communication, New J. Phys. **17**, 033022 (2015).

[15] C. Lupo and S. Lloyd, Continuous-variable quantum enigma machines for long-distance key distribution, Phys. Rev. A **92**, 062312 (2015).

[16] C. Lupo, Quantum data locking for secure communication against an eavesdropper with time-limited storage, Entropy **17**, 3194 (2015).
[17] S. Wehner, C. Schaffner, and B. M. Terhal, Cryptography from Noisy Storage, Phys. Rev. Lett. **100**, 220502 (2008).
[18] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Implementation of two-party protocols in the noisy-storage model, Phys. Rev. A **81**, 052336 (2010).
[19] R. Konig, S. Wehner, and J. Wullschleger, Unconditional security from noisy quantum storage, IEEE Trans. Inf. Theory **58**, 1962 (2012).
[20] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, An experimental implementation of oblivious transfer in the noisy storage model, Nat. Commun. **5**, 3418 (2014).
[21] F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabe, and S. Wehner, Continuous-variable protocol for oblivious transfer in the noisy-storage model, Nat. Commun. **9**, 1450 (2018).
[22] R. Garcia-Patron and N. J. Cerf, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Phys. Rev. Lett. **102**, 130501 (2009).
[23] 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).
[24] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, Phys. Rev. Lett. **114**, 070501 (2015).
[25] 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).
[26] F. Furrer, Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle, Phys. Rev. A **90**, 042325 (2014).
[27] T. Gehring, V. Handchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided–device-independent security against coherent attacks, Nat. Commun. **6**, 8795 (2015).
[28] 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).
[29] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Parameter Estimation with Almost no Public Communication for Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **120**, 220505 (2018).
[30] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).
[31] M. Navascues, F. Grosshans, and A. Acin, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).
[32] R. García-Patron and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).
[33] 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).
[34] 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).
[35] J. Lodewyck and P. Grangier, Tight bound on the coherent-state quantum key distribution with heterodyne detection, Phys. Rev. A **76**, 022332 (2007).
[36] 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).
[37] M. M. Wilde, From classical to quantum Shannon theory, arXiv:1106.1445.
[38] 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).
[39] 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).
[40] C. Pacher, J. Martinez-Mateo, J. Duhme, T. Gehring, and F. Furrer, Information reconciliation for continuous-variable quantum key distribution using non-binary low-density parity-check codes, arXiv:1602.09140.
[41] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).
[42] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).
[43] M. Tomamichel, Ph.D. thesis, Swiss Federal Institute of Technology (ETH), Zurich, 2012.
[44] M. Tomamichel, R. Colbeck, and R. Renner, A fully quantum asymptotic equipartition property, IEEE Trans. Inf. Theory **55**, 5840 (2009).