

Resource-efficient energy test and parameter estimation in continuous-variable quantum key distribution

Cosmo Lupo *Department of Physics and Astronomy, The University of Sheffield, Sheffield S3 7RH, United Kingdom*

(Received 7 April 2021; accepted 24 June 2021; published 12 July 2021)

Symmetry plays a fundamental role in the security analysis of quantum key distribution (QKD). Here we review how symmetry is exploited in continuous-variable (CV) QKD to prove the optimality of Gaussian attacks in the finite-size regime. We then apply these results to improve the feasibility and the key rate of these protocols. First we show how to improve the feasibility of the energy test, which is one important routine aimed at establishing an upper bound on the effective dimensions of the otherwise infinite-dimensional Hilbert space of CV systems. Second, we show how the routine of parameter estimation can be made resource efficient in measurement-device independent QKD. These results show that all the raw data can be used both for key extraction and for the routines of the energy test and parameter estimation. Furthermore, the improved energy test does not require active symmetrization of the measured data, which is computationally demanding.

DOI: [10.1103/PhysRevA.104.012409](https://doi.org/10.1103/PhysRevA.104.012409)

I. INTRODUCTION

Quantum key distribution (QKD) is the art of exploiting quantum optics to generate a secret key between two distant users linked by an insecure quantum communication channel [1]. Once the secret key is established, it can be used as a one-time pad to achieve ever-lasting security in communication. This is in contrast with public-key cryptography, including postquantum cryptography, whose security relies on computational complexity and is, thus, undermined by increasing computational power as well as quantum computing [2].

QKD protocols can be classified according to the nature of the degrees of freedom that are used to encode information in the quantum electromagnetic field. Discrete-variable (DV) protocols encode information in a discrete way (often binary) using, for example, polarization or time delay. Continuous-variable (CV) protocols encode information in continuous degrees of freedom, for example, quadrature and phase.

CV QKD has the strategic advantages of requiring for decoding off-the-shelf components as homodyne or heterodyne detection, which are mature technologies developed in standard telecommunication, whereas DV QKD needs high-efficiency and low-noise single-photon detectors [3]. For recent experimental demonstrations of CV QKD, see, for example, Refs. [4–6]. However, CV QKD is still not completely characterized from a theoretical point of view. Indeed, technical issues make the mathematical analysis of CV QKD more challenging than DV QKD. This is essentially due to the fact that the quantum states prepared and shared in CV QKD live in a Hilbert space of infinite dimensions.

The security of CV QKD has been first established for *Gaussian attacks*, i.e., under the assumption that the quantum communication channel maps Gaussian states into Gaussian states [7]. Second, it has been extended to *collective attacks*,

i.e., assuming that each signal passing through the quantum channel is subject to an instance of the same noisy transformation [8–10]. The most general attacks are the so-called *coherent attacks*, where the noisy communication channel can act in an unconstrained and unstructured way on the input signals. Finally, the highest standard of security is that of composable security, where the security of QKD is quantified and not only assessed in a qualitative way [11]. The composable quantification of security is especially important in the finite-size scenario where a finite number of quantum signals are exchanged, as is the case in any experimental realization of QKD.

For CV QKD, composable security against coherent attacks has been established for two kinds of protocols: The first is based on squeezed states and homodyne detection, whose security analysis exploits the phase-quadrature uncertainty relations [12,13]; the second is based on coherent states, heterodyne detection, and exploits the *postselection method* [14] to prove the optimality of Gaussian attacks in the finite-size regime [15]. In this paper we focus on the latter approach, which applies to *no-switching* protocols introduced by Weedbrook *et al.* [16]. In both cases the protocols include an *energy test* to project the quantum state into a finite-dimensional Hilbert space. The test requires to measure part of the system. Depending on the output of the measurement, one can assume that the rest of the system belongs with high probability to a Hilbert space of finite dimensions. This implies that part of the raw keys, i.e., the data used for the energy test, cannot be used for key extraction. Here we show how this limitation can be removed by applying an idea first introduced by Leverrier [10]. The impact of this result on practical CV QKD is not on improving the key rate but in making the protocol more experimentally feasible. In fact, our approach does not require Alice (the sender) and Bob

(the receiver) to symmetrize their measured data [15]. Such symmetrization is obtained by applying a random unitary rotation on their raw keys. Due to the large size of the data set (typically 10^8 – 10^{10} samples may be collected), the symmetrization is computationally demanding. We remark that the analysis of Ref. [17], which also focused on the active symmetrization routine, did not consider its application to the energy test.

Parameter estimation is a subroutine of QKD whose goal is to obtain information about the communication channel. The standard way of performing parameter estimation requires Alice and Bob to publicly announce part of their local raw keys. This implies that the data used for parameter estimation are compromised and cannot be used for key extraction, although there exist ways to bypass this limitation [10]. Here we consider parameter estimation in measurement-device-independent (MDI) QKD and show that in this case all the raw data can be used for both parameter estimation and secret key extraction.

MDI QKD was introduced to avoid side-channel attacks on the measurement apparatus [18,19]. Experimental implementations are demanding but feasible, see, for example, Refs. [20,21]. The theory of Leverrier [15] allows us to prove the composable security in the finite-size regime for a class of protocols based on preparation of coherent state and heterodyne detection, including MDI protocols [17]. Recently, Refs. [22,23] introduced modified CV MDI protocols that allow Alice and Bob to use all the measured data for both parameter estimation and key extraction. The scope of this result was questioned by Ghorai *et al.* [17], who suggested that it might *not* be compatible with composable security. Here we address this criticism and show that the protocol is indeed secure in a composable way as follows from the application of the general method put forward in Ref. [15]. We, thus, establish that, in CV MDI QKD, all the raw data can be used for both key extraction and parameter estimation without compromising the composable security of the protocol. This is expected to have an impact in increasing the key rate in the finite-size regime.

Although our result on parameter estimation is confined to MDI protocols (in principle, this can be extended to one-way protocols [22]), our findings about the energy test may be as well applied to a wider range of CV QKD protocols. This is suggested by Ref. [17] where it was shown that the proof techniques of Ref. [15] apply to two-way protocols with Gaussian displacements [24,25] as well as floodlight QKD [26–28].

The paper proceed as follows. First we review the toolbox of CV quantum optics in Sec. II, then we briefly review the use of symmetry in CV QKD in Sec. III. In Sec. IV we introduce the resource-efficient energy test where all the raw keys can be used for both the test and the secret key extraction. In Sec. V we introduce the CV MDI protocol in the entanglement-based (EB) representation, and in Sec. V A we show that parameter estimation can be done in a covariant way. In Sec. V B we extend this result to the equivalent prepare and measure (PM) representation. In Sec. V C we show that parameter estimation can be performed without leaking information to

the adversary. Finally, in Sec. V D we show that all data can be used for parameter estimation without compromising security. Conclusions are presented in Sec. VI.

II. THE TOOLBOX OF CONTINUOUS-VARIABLE QUANTUM CRYPTOGRAPHY

In CV QKD information is encoded in the phase and quadrature of the quantum electromagnetic field [29]. The building block of CV QKD is the bosonic mode, also called the *qumode*, which is formally represented as a quantum harmonic oscillator with annihilation and creation operators \hat{a} and \hat{a}^\dagger , satisfying the canonical commutation relations $[\hat{a}, \hat{a}^\dagger] = 1$. The phase and quadrature operators are defined as $\hat{q} = (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$ and $\hat{p} = (\hat{a} - \hat{a}^\dagger)/\sqrt{2}i$, respectively. The Hamiltonian of the harmonic oscillator is $\hat{H} = (\hat{q}^2 + \hat{p}^2)/2 = \hat{a}^\dagger \hat{a} + 1/2$, where $\hat{N} = \hat{a}^\dagger \hat{a}$ is the number operator. The latter has eigenvectors $\{|n\rangle\}_{n=0, \dots, \infty}$ such that $\hat{N}|n\rangle = n|n\rangle$, which form a complete set $\sum_{n=0}^{\infty} |n\rangle\langle n| = 1$. The number states can be obtained by repeated applications of the creation operator on the vacuum state as $|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle$ with $\hat{N}|0\rangle = 0$.

Here we focus on QKD protocols where classical information is encoded in a qumode in a continuous way using coherent states. A coherent state $|\alpha\rangle$ is an eigenvector of the annihilation operator, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\alpha \in \mathbb{C}$ is a complex amplitude. Coherent states are expanded in the number basis as $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$. They form an overcomplete set that satisfies $\frac{1}{\pi} \int d^2\alpha |\alpha\rangle\langle\alpha| = 1$, where $d^2\alpha = d \operatorname{Re}(\alpha) d \operatorname{Im}(\alpha)$. In CV QKD, a pair of classical random variables $q^{\text{pre}}, p^{\text{pre}} \in \mathbb{R}$ are encoded in the coherent state $|\alpha\rangle$ with amplitude $\alpha = (q^{\text{pre}} + ip^{\text{pre}})/\sqrt{2}$.

Heterodyne detection is formally represented as the continuous family of positive operator-valued measure elements $\Lambda_\beta = \frac{1}{\pi} |\beta\rangle\langle\beta|$ with $\beta \in \mathbb{C}$. We have $\operatorname{Tr}(\Lambda_\beta |\alpha\rangle\langle\alpha|) = \frac{1}{\pi} |\langle\alpha|\beta\rangle|^2 = \frac{1}{\pi} e^{-|\alpha-\beta|^2}$. Given a quantum state ρ , the output of heterodyne detection $\beta = (q^{\text{het}} + ip^{\text{het}})/\sqrt{2}$ defines the random variables $q^{\text{het}}, p^{\text{het}} \in \mathbb{R}$. An outcome of this measurement in the range of $\beta \pm d \operatorname{Re} \beta/2 \pm id \operatorname{Im} \beta/2$ has probability $\frac{1}{\pi} d^2 \beta \operatorname{Tr}(\Lambda_\beta \rho) = \frac{1}{\pi} d^2 \beta \langle\beta|\rho|\beta\rangle$.

The displacement operator is a unitary operator defined as $D(\gamma) = e^{\gamma \hat{a}^\dagger - \gamma^* \hat{a}}$. It allows us to shift the annihilation and creation operators by a c number, i.e., $D(\gamma)^\dagger \hat{a} D(\gamma) = \hat{a} + \gamma$, and $D(\gamma)^\dagger \hat{a}^\dagger D(\gamma) = \hat{a}^\dagger + \gamma^*$. It follows that the displacement operator also shifts the quadrature operators $D(\gamma)^\dagger \hat{q} D(\gamma) = \hat{q} + \operatorname{Re}(\gamma)/\sqrt{2}$ and $D(\gamma)^\dagger \hat{p} D(\gamma) = \hat{p} + \operatorname{Im}(\gamma)/\sqrt{2}$. The displacement operator maps coherent states into coherent states $D(\gamma)|\alpha\rangle = |\alpha + \gamma\rangle$ and commutes with heterodyne detection, i.e., $\operatorname{Tr}[\Lambda_\beta D(\gamma) \rho D(\gamma)^\dagger] = \operatorname{Tr}[D(\gamma)^\dagger \Lambda_\beta D(\gamma) \rho] = \operatorname{Tr}[\Lambda_{\beta-\gamma} \rho]$. This means that displacing and then measuring is equivalent to measuring and then displacing the measurement output.

The two-mode squeezed vacuum (TMSV) is a quantum state of two qumodes. Its expansion in the number basis is

$$|\Psi\rangle_{AA'} = \sqrt{\frac{1}{N+1}} \sum_{n=0}^{\infty} \left(\frac{N}{N+1} \right)^{n/2} |n\rangle_A |n\rangle_{A'}, \quad (1)$$

where the parameter N quantifies the mean photon number per qumode. We have

$${}_A \langle \beta | \Psi \rangle_{AA'} = \sqrt{\frac{1}{N+1}} e^{-[1/(N+1)]\|\beta\|^2/2} \left| \sqrt{\frac{N}{N+1}} \beta^* \right\rangle_{A'}. \quad (2)$$

This shows that if we measure one qumode of the TMSV Ψ by heterodyne detection and obtain β , then the other qumode is prepared in the coherent-state $|\alpha\rangle$ with amplitude $\alpha = \sqrt{\frac{N}{N+1}} \beta^*$. An outcome of this measurement in the range of $\beta \pm d \operatorname{Re} \beta/2 \pm id \operatorname{Im} \beta/2$ has probability $d^2 \beta \frac{1}{\pi} \frac{1}{N+1} e^{-[1/(N+1)]\|\beta\|^2} = d^2 \alpha \frac{1}{\pi} \frac{1}{N} e^{-(1/N)|\alpha|^2}$.

Consider a system of ℓ qumodes and the 2ℓ classical phase and quadrature variables $\mathbf{q} = q_1, \dots, q_\ell$, $\mathbf{p} = p_1, \dots, p_\ell$. For any density operator ρ , the Wigner function is defined as

$$W(\mathbf{q}, \mathbf{p}) = \frac{1}{\pi^\ell} \int_{-\infty}^{\infty} d^n \mathbf{y} (\mathbf{q} + \mathbf{y} | \rho | \mathbf{q} - \mathbf{y}) e^{-2i\mathbf{p} \cdot \mathbf{y}}, \quad (3)$$

where $\mathbf{y} = y_1, \dots, y_\ell$, $d^n \mathbf{y} = dy_1 \cdots dy_\ell$, and $|\mathbf{q} \pm \mathbf{y}\rangle$ are eigenvectors of the quadrature operators, i.e., $\hat{q}_j |\mathbf{q} \pm \mathbf{y}\rangle = (q_j \pm y_j) |\mathbf{q} \pm \mathbf{y}\rangle$. By definition, a Gaussian state has a Wigner function that is a multivariate normal distribution. Gaussian states are, therefore, uniquely determined by the first moments and the (symmetrically ordered) covariance matrix (CM) of the quadrature operators.

III. SYMMETRY IN CV QKD

In general, the experimental realization of the protocol follows the PM representation where the legitimate users prepare quantum states and send them through an insecure quantum channel controlled by the eavesdropper (Eve). For example, in one-way protocols Alice sends quantum signals to Bob, who measures them, and in MDI protocols both Alice and Bob send signals to a central relay. However, the security of the protocol is proven in the equivalent EB representation where a bipartite quantum state ρ_{AB}^n is distributed to Alice and Bob, and Eve holds a purification. If the protocol is secure in the EB representation, so it is in the PM one. For this reason, in this section we review the security proof of Leverrier [15], which is defined in the EB representation.

A QKD protocol typically acts on n instances of a given physical system. CV QKD, in the EB representation, is defined on a set of $2n$ qumodes. For $j = 1, \dots, n$, these are represented by the creation and annihilation operators a_j^\dagger , a_j and b_j^\dagger , b_j , which are associated with Alice and Bob, respectively.

An EB QKD protocol is formally associated with a completely positive and trace-preserving (CPT) map \mathcal{E} that takes as input ρ_{AB}^n and outputs a shared key. The latter is represented by a classical state of the form $\sum_{x,y=0}^{2^\ell-1} p(x,y) |x\rangle_A \langle x| \otimes |y\rangle_B \langle y|$, where $x, y = 0, \dots, 2^\ell - 1$ are the possible keys obtained by Alice and Bob, respectively. In reality, we expect the keys to be only approximately secret as imperfections in the protocol may leak information to Eve. To assess the security of a QKD protocol we compare \mathcal{E} with the ideal map \mathcal{E}_0 that takes any input state and replaces it with a perfectly secret key of ℓ bits. The latter is represented by a classical-quantum state $\sum_{x=0}^{2^\ell-1} 2^{-\ell} |x\rangle_A \langle x| \otimes |x\rangle_B \langle x| \otimes \rho_E$ where Eve has no information

about the key. We then define $\Delta := \mathcal{E} - \mathcal{E}_0$, and require that

$$\|\Delta\|_\diamond \leq \epsilon \quad (4)$$

for some $\epsilon \ll 1$. We recall that the diamond norm $\|\cdot\|_\diamond$ is defined as the worst-case trace norm over all possible input states, including their purification,

$$\|\Delta\|_\diamond := \sup_{\psi} \|(\Delta \otimes I)\psi_{ABE}\|_1, \quad (5)$$

where the maps Δ acts on the systems AB associated with Alice and Bob and I is the identity map on the purifying system E . Finally, the supremum is over all tripartite states ψ_{ABE} , and $\|O\|_1 := \operatorname{Tr}|O|$ is the trace norm.

The security analysis is, thus, reduced to the task of estimating the above diamond norm. The upper bound ϵ quantifies the (in)security of the protocol, the smaller ϵ , the more the protocol is secure. Operationally, the *security parameter* ϵ quantifies the probability to discriminate between the actual protocol \mathcal{E} and the ideal one \mathcal{E}_0 [23]. Estimating the diamond norm is a very challenging task as it requires the calculation of the supremum over all states in a high-dimensional Hilbert space. In the case of CV QKD this space is infinite dimensional. Fortunately, the task can be dramatically simplified by exploiting symmetry.

CV QKD protocols that are based on heterodyne detection may be invariant under the symmetry group of *passive linear optics* transformations that mix the qumodes but preserves the separation between Alice and Bob. For any $n \times n$ unitary matrix U , consider the linear transformation on the bosonic operators $a_j \rightarrow \sum_{k=1}^n U_{jk} a_k$ and $b_j^\dagger \rightarrow \sum_{k=1}^n U_{jk} b_k^\dagger$. This map defines a bosonic representation R of the group $U(n)$ of $n \times n$ unitary matrices [30],

$$a_j \rightarrow R_U a_j R_U^\dagger = \sum_{k=1}^n U_{jk} a_k, \quad (6)$$

$$b_j^\dagger \rightarrow R_U b_j^\dagger R_U^\dagger = \sum_{k=1}^n U_{jk} b_k^\dagger. \quad (7)$$

The protocol is covariant under this group of transformation if for any unitary U there exists a CPT map K_U such that

$$\Delta \circ R_U = K_U \circ \Delta. \quad (8)$$

Under this condition it is easy to show that [14]

$$\|\Delta\|_\diamond = \sup_{\bar{\rho}_{AB}^n \in \mathcal{F}_n} \|(\Delta \otimes I)\bar{\rho}_{ABE}^n\|_1, \quad (9)$$

where \mathcal{F}_n is the subspace of states that are invariant under the symmetry group, i.e., $R_U \bar{\rho}_{AB}^n R_U^\dagger = \bar{\rho}_{AB}^n$. The subspace \mathcal{F}_n is spanned by the $SU(1, 1)$ -coherent states over $2n$ qumodes [31]. The $SU(1, 1)$ -coherent states have a number of important properties, in particular: (1) they are Gaussian states and (2) provide a decomposition of the unity.

Equation (9) cannot yet be used to compute the diamond norm. To further simplify it, we need to prepend a suitable *energy test* \mathcal{T} to the QKD protocol \mathcal{E} . The energy test consists of measuring $2k < 2n$ qumodes by heterodyne detection. According to the measurement result, the remaining $2n - 2k$ qumodes are projected, up to a small probability of error ϵ_{test} , into a finite-dimensional Hilbert space.

Conditioned on passing the energy test, the state of the remaining $2n - 2k$ qumodes can be effectively assumed to live in a finite-dimensional Hilbert space. This allows us to write

$$\|\Delta \circ \mathcal{T}\|_{\diamond} \leq c_{n-k,d} \sup_{\sigma_{ABE}} \|(\Delta \otimes I)\sigma_{ABE}^{\otimes n-k}\|_1 + \epsilon_{\text{test}}, \quad (10)$$

where the supremum is over Gaussian states σ_{ABE} and $c_{n-k,d} = K^4/50$. $K \sim (n-k)(d_A + d_B)$ bounds the effective dimensions. In conclusion, this shows that a protocol that is secure against Gaussian attacks is also secure against general coherent attacks provided that the energy test is passed and then one is willing to pay a multiplicative penalty in the security parameter.

The protocol \mathcal{E} is composed of several subroutines. After the energy test \mathcal{T} , one proceeds with the measurement \mathcal{M} (heterodyne detection for this class of symmetric protocols), then the parameter estimation routine \mathcal{P} , followed by error correction \mathcal{C} and privacy amplification \mathcal{A} . We can, therefore, write $\mathcal{E} \circ \mathcal{T} = \mathcal{A} \circ \mathcal{C} \circ \mathcal{P} \circ \mathcal{M} \circ \mathcal{T}$. Since the energy test and the measurement commute, we can as well write $\mathcal{E} \circ \mathcal{T} = \mathcal{A} \circ \mathcal{C} \circ \mathcal{P} \circ \mathcal{T} \circ \mathcal{M}$. Following an argument put forward by Ghorai *et al.* [17], we do not need that the overall protocol $\mathcal{E} \circ \mathcal{T}$ is covariant. In fact, it is sufficient that the covariance property (8) holds for the energy test \mathcal{T} and the parameter estimation \mathcal{P} .

IV. RESOURCE-EFFICIENT ENERGY TEST

In this section we improve on the energy test introduced in Ref. [15] to make it resource efficient and experimentally feasible. In Ref. [15], the energy test applies to a bipartite state ρ_{AB}^n of $2n$ qumodes, where n qumodes are on Alice side, and n on Bob's side: the result of heterodyne detection on $2k < 2n$ qumodes allows Alice and Bob to establish an upper bound on the dimensions of the Hilbert space containing the state of the remaining $2(n-k)$ qumodes. The qumodes measured for the energy test cannot be used for key extraction, therefore, reducing their number from $2n$ to $2(n-k)$.

First we review the energy test of Ref. [15]. Then we modify it to make it resource efficient in such a way that all the qumodes are used for both the energy test and the key extraction. The energy test of Ref. [15] is defined as follows:

(1) Alice and Bob publicly agree on a random unitary matrix of size n and apply the local transformations $a_j \rightarrow \sum_{h=1}^n U_{jh} a_h$, $b_j^\dagger \rightarrow \sum_{h=1}^n U_{jh} b_h^\dagger$.

(2) They measure by heterodyne detection the first $2k < 2n$ qumodes. The output of Alice's measurement is $\alpha_1 \cdots \alpha_n$, and the output of Bob's measurement is $\beta_1 \cdots \beta_n$.

(3) They compute the quantities $E_A^k = \frac{1}{k} \sum_{j=1}^k |\alpha_j|^2$ and $E_B^k = \frac{1}{k} \sum_{j=1}^k |\beta_j|^2$.

(4) If $E_A^k \leq d_A$ and $E_B^k \leq d_B$ for some d_A, d_B , then they conclude that the state of the remaining $2(n-k)$ qumodes lives in a Hilbert space of dimensions not larger than $K = (n-k)(d'_A + d'_B)$, where $\star = A, B$, $d'_\star = d_\star g(n-k, k, \epsilon/4)$ and

$$g(n_1, n_2, \delta) = \frac{1 + 2\sqrt{\frac{\ln(2/\epsilon)}{2n_1}} + \frac{\ln(2/\epsilon)}{n_1}}{1 - 2\sqrt{\frac{\ln(2/\epsilon)}{2n_2}}}. \quad (11)$$

This statement holds with probability, at least, equal to $1 - \epsilon$.

We now present a modified test that allows Alice and Bob to use all the modes for both the test and the key extraction. We do that by applying an idea first introduced in Ref. [10] to solve a similar problem in the context of parameter estimation. The test is applied after all qumodes have been measured by heterodyne detection. The resource-efficient energy test is defined as follows:

(1) Alice and Bob measure all their local qumodes by heterodyne detection, obtaining the output variables $\alpha_1 \cdots \alpha_n$ and $\beta_1 \cdots \beta_n$.

(2) They compute the quantities $E_A^n = \frac{1}{n} \sum_{j=1}^n |\alpha_j|^2$ and $E_B^n = \frac{1}{n} \sum_{j=1}^n |\beta_j|^2$.

(3) If $E_A^n \leq d_A$ and $E_B^n \leq d_B$ for some integers d_A, d_B , then they conclude that the original state ρ_{AB}^n lived in a Hilbert space of dimensions not larger than $K = n(d'_A + d'_B)$ with $d'_\star = (1 + \delta)d_\star$ and

$$\delta = 1.5 \sqrt{\frac{\ln(2/\epsilon)}{n/2}}. \quad (12)$$

As shown below, this statement holds with probability, at least, $1 - 4\epsilon$.

We now show that the resource-efficient energy test is, in fact, equivalent to the original energy test of Ref. [15].

Proof. First of all, we note that the quantities E_A^n, E_B^n are invariant under the symmetry group. Therefore, we can equivalently write $E_A^n = \frac{1}{n} \sum_{j=1}^n |\alpha'_j|^2$, $E_B^n = \frac{1}{n} \sum_{j=1}^n |\beta'_j|^2$, where $\alpha'_j = \sum_{h=1}^n U_{jh} \alpha_h$ and $\beta_j = \sum_{h=1}^n U_{jh}^* \beta_h$ for any unitary matrix U . We can then define a thought experiment where Alice and Bob first randomize they measurement outcomes by applying a random unitary U , then apply the energy test of Ref. [15] on the first $n_1 = n/2$ qumodes to obtain an upper bound on the dimensions of the remaining $n_2 = n/2$ qumodes (for simplicity we assume that n is even). In this case, they would compute the quantities $E_A^{n_1}, E_B^{n_1}$. Similarly, we could consider a dual thought experiment where they measure the last n_2 modes to bound the dimension of the first block of n_1 modes. In this case they would compute the quantities $E_A^{n_2}, E_B^{n_2}$. The two thought experiments are linked by the invariant relations $E_A^n = E_A^{n_1} + E_A^{n_2}$ and $E_B^n = E_B^{n_1} + E_B^{n_2}$. To draw a conclusion about the two thought experiments from the knowledge of E_A^n, E_B^n , we can apply the following tail bound [15]. For a random choice of the unitary U , it holds that for any $\epsilon \geq 2e^{-n_1/2}$,

$$\Pr \left\{ E_\star^{n_j} \geq \left[1 + 1.5 \sqrt{\frac{\ln(2/\epsilon)}{n/2}} \right] E_\star^n \right\} \leq \epsilon \quad (13)$$

for $\star = A, B$ and $j = 1, 2$. This means that, if $E_\star^n \leq d_\star$, then with probability, at least, $1 - \epsilon$, we also have $E_\star^{n_j} \leq d_\star(1 + \delta)$ for a random choice of the unitary matrix U . This implies that both thought experiments would be successful with probability, at least, $1 - 4\epsilon$. \square

In conclusion, at the price of paying an extra additive penalty of 4ϵ , the resource-efficient energy test allows Alice and Bob to: (1) use all their modes for both the energy test and for key extraction; and (2) avoid the application of the transformation $a_j \rightarrow \sum_{h=1}^n U_{jh} a_h$, $b_j^\dagger \rightarrow \sum_{h=1}^n U_{jh} b_h^\dagger$.

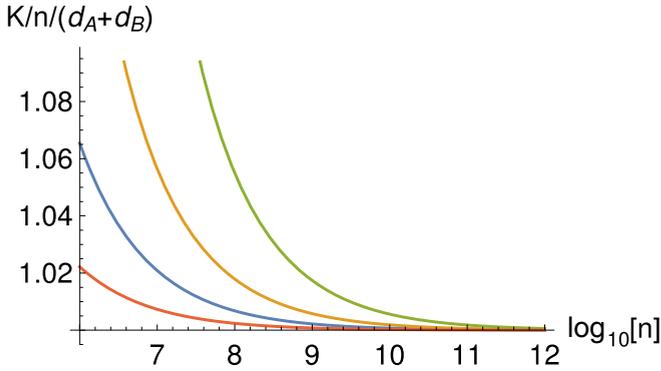


FIG. 1. The normalized effective dimension $K/n/(d_A + d_B)$ of the truncated Hilbert space subject to passing the energy test, plotted vs the sample size n . The three top lines are for the energy test of Ref. [15] with [from top to bottom $k = 10^{-3}n$ (green line), $k = 10^{-2}n$ (orange line), and $k = 10^{-1}n$ (blue line)]. The bottom line (red) is for our efficient energy test that uses all data for both the test and for key extraction. The lines are obtained by imposing that the probability of failing the test is smaller than 10^{-20} .

To summarize, the goal of the energy test is to estimate an effective, finite dimension for the Hilbert space of Alice's and Bob's signals. In the limit of $n \rightarrow \infty$ (and $k \rightarrow \infty$ for the energy test of Ref. [15]) the effective dimension, per symbol sent, is given as $K/n = d_A + d_B$. For finite n and k , the estimate for this dimension is larger by a multiplicative factor $K/n/(d_A + d_B)$. For the energy test of Ref. [15], the factor is $g(n - k, k, \epsilon/4)$ from Eq. (11). For our energy test it is $1 + 1.5\sqrt{2 \ln(8/\epsilon)/n}$ from Eq. (12). Figure 1 compares the ratio $K/n/(d_A + d_B)$ for both approaches. The fact that they are both of order one shows that as anticipated our efficient energy test is not substantially changing the key rate in the finite-size regime (although a small improvement is observed). As discussed above, the important impact of our energy test is to make the protocol experimentally feasible.

V. CV MDI QKD

MDI QKD was introduced to avoid side-channel attacks on the measurement apparatus [18,19]. In the PM representation, the legitimate users Alice and Bob prepare and send quantum states, whereas the task of measuring them is delegated to a third untrusted party. Here we refer to the latter as the relay and assume without loss of generality that it is fully controlled by Eve. On the contrary, in the EB representation Alice and Bob also need to apply some local measurements. However, this does not expose MDI to side-channel attacks as the EB representation is only used as a theoretical tool to prove the security of the equivalent PM protocol. It is only the PM protocol that is implemented experimentally.

It is useful to formally split the description of the MDI protocol in two parts. The first part is *state preparation*, whose goal is to establish a correlated quantum state ρ_{AB}^n shared between the legitimate users. It is the preparation phase that characterizes CV MDI QKD with respect to other one-way and two-way CV QKD protocols. Once the quantum state has been distributed, the users proceed with *key extraction*. The map \mathcal{E} discussed in Sec. III corresponds to the key

extraction part of the protocol, which takes state ρ_{AB}^n as input. This second part of the MDI protocol comprises local measurements, parameter estimation, error correction, and privacy amplification. Here we consider a MDI protocol where the measurement is heterodyne detection.

The phase of state preparation, in the EB protocol, is as follows:

(1) Alice prepares a TMSV state $\psi_{AA'}$ with mean photon number N_A on her modes A and A' . Similarly, Bob prepares a TMSV state $\psi_{BB'}$ with mean photon number N_B on his local modes B and B' . They retain modes A , B and send modes A' , B' to the relay.

(2) The relay publicly announces a complex number $z = (q_Z + ip_Z)/\sqrt{2}$.

(3) Alice and Bob apply the phase-space displacement operators $D(\gamma_A)$, $D(\gamma_B)$ to their local modes with displacement amplitudes determined by z [32]

$$\gamma_A = az, \quad \gamma_B = bz^*, \quad (14)$$

where a and b are real-valued constants and z^* denotes the complex conjugate of z .

These steps are repeated n times. The state prepared in this way is denoted as ρ_{AB}^n and is the input of the second phase of the protocol. The phase of key extraction develops as follows:

(4) Alice and Bob measure their local modes by heterodyne detection. The output is a pair of n -fold complex vectors $\alpha = \alpha_1 \cdots \alpha_n$ and $\beta = \beta_1 \cdots \beta_n$, respectively, which represent their local raw keys.

(5) They perform the energy test, for example, the resource-efficient energy test described in Sec. IV.

(6) They apply a random rotation on their raw keys $\alpha_j \rightarrow \sum_{h=1}^n U_{jh} \alpha_h$ and $\beta_j \rightarrow \sum_{h=1}^n U_{jh}^* \beta_h$, where U is a $n \times n$ unitary matrix.

They then select $k < n$ elements (for example, $\alpha_1, \dots, \alpha_k$ and β_1, \dots, β_k) and share their values on a public channel. These data allow Alice and Bob to estimate the number of secret bits that can be distilled from what is left of the raw keys.

This is discussed in more detail below.

(7) Alice and Bob perform error correction and privacy amplification to distill their secret keys from the remaining raw data of size $n - k$.

In order to apply the theory of Ref. [15] it is important to verify that the energy test and parameter estimation routine are covariant under the symmetry group. The resource-efficient energy test is clearly covariant by construction. The same holds for the parameter estimation routine as we now discuss in detail. In this description of the protocol, we require active symmetrization of the local modes, although there are ways to avoid it [10].

A. Covariant parameter estimation

Alice and Bob share quantum state ρ_{AB}^n , they measure it by local heterodyne detection and obtain the raw data $\alpha = \alpha_1, \dots, \alpha_n$, $\beta = \beta_1, \dots, \beta_n$. The fundamental question of QKD is to determine how many secret bits they can extract from their raw data. According to the theory of Ref. [15], to answer this question we can without loss of generality assume that state ρ_{AB}^n is Gaussian, symmetric, and is factorized, i.e.,

$\rho_{AB}^n = \rho_{AB}^{\otimes n}$ (provided that the QKD protocol is covariant and the state has passed the energy test).

In other words, initial-state ρ_{AB}^n can be assumed to be the collection of n identical copies of a two-mode Gaussian state ρ_{AB} . We recall that a Gaussian state is uniquely determined by the first and second moments of the quadrature operators, denoted as \hat{q}_A, \hat{p}_A for Alice’s mode and as \hat{q}_B, \hat{p}_B for Bob’s mode. In Appendix A we review how we can obtain the CM of the Wigner function from one of the outputs of heterodyne

detection. Using relation (A3), the CM of the Wigner function can be obtained from the CM of the heterodyne measurement outputs in Eq. (A2). To simplify the notation we drop the label het and indicate the heterodyne output variables simply as q_A, p_A, q_B, p_B .

Since the state is symmetric, we can further assume that the first moments $\mathbb{E}[q_A], \mathbb{E}[p_A], \mathbb{E}[q_B], \mathbb{E}[p_B]$ vanish [33] and that the CM has the following form [15]:

$$V_{\text{EB}}^{\text{het}} = \frac{1}{2} \begin{pmatrix} \mathbb{E}[q_A^2] + \mathbb{E}[p_A^2] & 0 & \mathbb{E}[q_A q_B] - \mathbb{E}[p_A p_B] & \star \\ 0 & \mathbb{E}[q_A^2] + \mathbb{E}[p_A^2] & \star & -\mathbb{E}[q_A q_B] + \mathbb{E}[p_A p_B] \\ \mathbb{E}[q_A q_B] - \mathbb{E}[p_A p_B] & \star & \mathbb{E}[q_B^2] + \mathbb{E}[p_B^2] & 0 \\ \star & -\mathbb{E}[q_A q_B] + \mathbb{E}[p_A p_B] & 0 & \mathbb{E}[q_B^2] + \mathbb{E}[p_B^2] \end{pmatrix}, \quad (15)$$

where the matrix entries with the postholder \star can be assumed to be zero with no loss of generality.

The security of CV QKD when the state is Gaussian and independent and identically distributed (i.i.d.) is well established [7]. Knowing the entries of the above CM, we can bound how many secret bits can be distilled from the state. As a matter of fact, it is sufficient to know upper bounds on the diagonal entries $\mathbb{E}[q_A^2] + \mathbb{E}[p_A^2], \mathbb{E}[q_B^2] + \mathbb{E}[p_B^2]$, and a lower bound on the absolute value of the off-diagonal term $\mathbb{E}[q_A q_B] - \mathbb{E}[p_A p_B]$. Given the output of heterodyne detection $q_{Aj}, p_{Aj}, q_{Bj}, p_{Bj}$ for $j = 1, \dots, k$, we can estimate the following bounds:

$$\mathbb{E}[q_A^2] + \mathbb{E}[p_A^2] \leq \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k q_{Aj}^2 + p_{Aj}^2, \quad (16)$$

$$\mathbb{E}[q_B^2] + \mathbb{E}[p_B^2] \leq \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k q_{Bj}^2 + p_{Bj}^2, \quad (17)$$

and

$$|\mathbb{E}[q_A q_B] - \mathbb{E}[p_A p_B]| \geq \frac{1}{1-t^2} \frac{1}{k} \left| \sum_{j=1}^k q_{Aj} q_{Bj} - p_{Aj} p_{Bj} \right| - \frac{t}{1-t^2} \frac{1}{k} \sum_{j=1}^k \frac{q_{Aj}^2 + q_{Bj}^2 + p_{Aj}^2 + p_{Bj}^2}{2}. \quad (18)$$

For any $t > 0$, these bounds hold with probability larger than $1 - 8e^{-kt^2/8}$. These estimates are obtained in Appendix B. Although these bounds are not necessarily optimal, the important point here is that they are invariant under the symmetry-group $q_{Aj} + ip_{Aj} \rightarrow \sum_h U_{jh}(q_{Ah} + ip_{Ah}), q_{Bj} + ip_{Bj} \rightarrow \sum_h U_{jh}^*(q_{Bh} + ip_{Bh})$.

B. MDI in the PM representation

The equivalence of the EB and PM representations follows from (see Sec. II for more detail): (1) If we measure by heterodyne detection one mode of a TMSV with N mean photon per mode and obtain β , then the other mode is prepared in a coherent state with amplitude $\alpha = \sqrt{\frac{N}{N+1}}\beta^*$; and (2) if we first displace a mode and then measure it by heterodyne, this is equivalent to first measure and then displace the measurement output. Therefore, the EB protocol described in Sec. V is equivalent to the following PM protocol:

(a) Alice prepares coherent states $|\alpha^0\rangle$ by sampling its complex amplitude $\alpha^0 = (q_A^{\text{pre},0} + ip_A^{\text{pre},0})/\sqrt{2}$ from a circularly symmetric Gaussian distribution with zero mean and variance N_A . Similarly, Bob prepares coherent states with amplitude $\beta^0 = (q_B^{\text{pre},0} + ip_B^{\text{pre},0})/\sqrt{2}$ sampling from a Gaussian distribution with variance N_B . They retain the values of the amplitudes and send the coherent states to the relay.

(b) The relay publicly announces a complex number $z = (q_z + ip_z)/\sqrt{2}$.

(c) Alice and Bob apply the following linear transformation to their local amplitude data:

$$\alpha^0 \rightarrow \alpha = \alpha^0 + \sqrt{\frac{N_A}{N_A + 1}} a z^*, \quad (19)$$

$$\beta^0 \rightarrow \beta = \beta^0 + \sqrt{\frac{N_B}{N_B + 1}} b z. \quad (20)$$

We put $\alpha = (q_A^{\text{pre}} + ip_A^{\text{pre}})/\sqrt{2}$ and $\beta = (q_B^{\text{pre}} + ip_B^{\text{pre}})/\sqrt{2}$ from which it follows that

$$q_A^{\text{pre}} = q_A^{\text{pre},0} + a q z, \quad (21)$$

$$p_A^{\text{pre}} = p_A^{\text{pre},0} - a p z, \quad (22)$$

$$q_B^{\text{pre}} = q_B^{\text{pre},0} + b q z, \quad (23)$$

$$p_B^{\text{pre}} = p_B^{\text{pre},0} + b p z. \quad (24)$$

These steps are repeated n times. Then they proceed as follows:

(d) They perform the resource-efficient energy test as described in Sec. IV.

(e) They apply a rotation on their raw keys $\alpha_j \rightarrow \sum_{h=1}^n U_{jh}^* \alpha_h$, $\beta_j \rightarrow \sum_{h=1}^n U_{jh} \beta_h$, where U is a $n \times n$ random unitary matrix.

They then select $k < n$ elements (for example, $\alpha_1, \dots, \alpha_k$ and β_1, \dots, β_k) and share their values on a public channel. These data allow Alice and Bob to estimate the number of secret bits that can be distilled from what is left of the raw keys.

(f) Alice and Bob perform error correction and privacy amplification to distill their secret key from the remaining raw data of size $n - k$.

The security of this PM protocol follows from the one of the EB protocol. The equivalence between the two representation follows from the equivalence between the corresponding steps $a \equiv 1$ and 4 , $b \equiv 2$, $c \equiv 3$.

C. A closer look at parameter estimation

In the PM representation of the protocol, Alice and Bob need to estimate the CM $V_{\text{PM}}^{\text{MDI}}$ in Eq. (A6) from the preparation data $q_{A_j}^{\text{pre}}, p_{A_j}^{\text{pre}}, q_{B_j}^{\text{pre}}, p_{B_j}^{\text{pre}}$ for $j = 1, \dots, n$. In turn, they obtain their estimate of the CM $V_{\text{EB}}^{\text{het}}$ using Eq. (A7). To make the notation lighter, below we drop the label pre and simply refer to the preparation data as $q_{A_j}, p_{A_j}, q_{B_j}, p_{B_j}$.

The covariant parameter estimation routine relies on the computation of following quantities from a sample of the raw data:

$$C_1 = \frac{1}{k} \sum_{j=1}^k q_{A_j}^2 + q_{B_j}^2, \quad (25)$$

$$C_2 = \frac{1}{k} \sum_{j=1}^k p_{A_j}^2 + p_{B_j}^2, \quad (26)$$

$$C_3 = \frac{1}{k} \left| \sum_{j=1}^k q_{A_j} q_{B_j} - p_{A_j} p_{B_j} \right|. \quad (27)$$

Note that C_1 and C_2 can be computed locally by Alice and Bob. However, to compute C_3 they need to share their local data on a public channel. This implies that the data used for parameter estimation are compromised and cannot be used for secret key extraction. Here we show that this limitation can be avoided by using the public data q_{Z_j}, p_{Z_j} from the relay.

In the PM representation of the protocol we have (putting $a' := \sqrt{\frac{N_A}{N_A+1}} a$, $b' := \sqrt{\frac{N_B}{N_B+1}} b$),

$$C_3 = \frac{1}{k} \left| \sum_{j=1}^k q_{A_j} q_{B_j} - p_{A_j} p_{B_j} \right| \quad (28)$$

$$= \frac{1}{k} \left| \sum_{j=1}^k (q_{A_j}^0 + a' q_{Z_j}) (q_{B_j}^0 + b' q_{Z_j}) - (p_{A_j}^0 - a' p_{Z_j}) (p_{B_j}^0 + b' p_{Z_j}) \right| \quad (29)$$

$$= \frac{1}{k} \left| \sum_{j=1}^k q_{A_j}^0 q_{B_j}^0 - p_{A_j}^0 p_{B_j}^0 + \frac{1}{k} \sum_{j=1}^k a' (q_{Z_j} q_{B_j}^0 + p_{Z_j} p_{B_j}^0) + b' (q_{A_j}^0 q_{Z_j} - p_{A_j}^0 p_{Z_j}) + a' b' (q_{Z_j}^2 + p_{Z_j}^2) \right|. \quad (30)$$

We can then write $C_3 = |C_{3,1} + C_{3,2}|$, where

$$C_{3,1} = \frac{1}{k} \sum_{j=1}^k q_{A_j}^0 q_{B_j}^0 - p_{A_j}^0 p_{B_j}^0, \quad (31)$$

and

$$C_{3,2} = \frac{1}{k} \sum_{j=1}^k a' (q_{Z_j} q_{B_j}^0 + p_{Z_j} p_{B_j}^0) + b' (q_{A_j}^0 q_{Z_j} - p_{A_j}^0 p_{Z_j}) + a' b' (q_{Z_j}^2 + p_{Z_j}^2). \quad (32)$$

Note that $C_{3,2}$ can be computed locally by Alice and Bob using only their measured data and the public data q_{Z_j}, p_{Z_j} . Consider now the first term,

$$C_{3,1} = \frac{1}{k} \sum_{j=1}^k q_{A_j}^0 q_{B_j}^0 - p_{A_j}^0 p_{B_j}^0. \quad (33)$$

Note that, by construction of the PM protocol, we know that $\mathbb{E}[q_A^0 q_B^0] = \mathbb{E}[p_A^0 p_B^0] = 0$, and $\mathbb{E}[(q_A^0)^2] = \mathbb{E}[(q_B^0)^2] = N_A$, $\mathbb{E}[(q_B^0)^2] = \mathbb{E}[(p_B^0)^2] = N_B$. We can then apply the tail bounds (see Appendix B),

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k q_{A_j}^0 q_{B_j}^0 - p_{A_j}^0 p_{B_j}^0 > t(N_A + N_B) \right\} < 4e^{-kt^2/8}, \quad (34)$$

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k q_{A_j}^0 q_{B_j}^0 - p_{A_j}^0 p_{B_j}^0 < -t(N_A + N_B) \right\} < 4e^{-kt^2/8}, \quad (35)$$

which imply

$$\Pr \left\{ \frac{1}{k} \left| \sum_{j=1}^k q_{A_j} q_{B_j} - p_{A_j} p_{B_j} \right| < |C_{3,2}| - t(N_A + N_B) \right\} < 4e^{-kt^2/8}. \quad (36)$$

Finally, by combining Eq. (36) with Eqs. (16)–(18), we establish the following bounds on the entries of the CM:

$$\mathbb{E}[q_A^2] + \mathbb{E}[p_A^2] \leq \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k q_{A_j}^2 + p_{A_j}^2, \quad (37)$$

$$\mathbb{E}[q_B^2] + \mathbb{E}[p_B^2] \leq \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k q_{B_j}^2 + p_{B_j}^2, \quad (38)$$

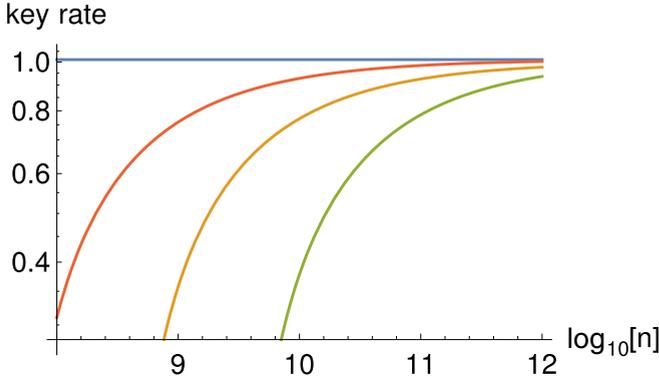


FIG. 2. Key rate (against Gaussian attacks) vs the sample size n . The top line (blue) shows the asymptotic key rate. The second line from the top (red) is the finite-size key rate obtained with our resource-efficient parameter estimation. The other two lines are for traditional parameter estimation with $k = 10^{-3}n$ (bottom line, green) and $k = 10^{-2}n$ (second line from the bottom, orange). The plot is obtained assuming a symmetric scenario where the channel from Alice to the relay is the same as from Bob to the relay. Such a channel has loss 1 dB, excess noise of 0.01 in shot-noise units, the input photon number is 10, the error correction efficiency is 0.95, and the security parameter is 10^{-20} .

and

$$\begin{aligned}
 & |\mathbb{E}[q_A q_B] - \mathbb{E}[p_A p_B]| \\
 & \geq \frac{1}{1-t^2} |C_{3,2}| - \frac{t}{1-t^2} (N_A + N_B) \\
 & \quad - \frac{t}{1-t^2} \frac{1}{k} \sum_{j=1}^k \frac{q_{A_j}^2 + q_{B_j}^2 + p_{A_j}^2 + p_{B_j}^2}{2}. \quad (39)
 \end{aligned}$$

These bounds hold for any $t > 0$ with probability larger than $1 - 12e^{-kt^2/8}$.

In conclusion, we have shown that in the PM representation of the MDI protocol, parameter estimation can be performed locally with no need to compromise the raw keys. In particular, this implies that Alice and Bob can choose $k = n$ and use all the raw keys for both parameter estimation and secret key extraction.

D. Resource-efficient CV MDI QKD

We are finally in the position of presenting a PM protocol for CV MDI QKD where Alice and Bob can use all their raw data for both key extraction and parameter estimation (as well as the energy test). The state preparation phase is as for (a)–(c) in Sec. VB. The key extraction phase is as follows:

(d) Alice and Bob apply the resource-efficient energy test as described in Sec. IV.

(e) They perform parameter estimation as described in Sec. VC with $k = n$. Note that no information about the raw keys is revealed. They can, therefore, use all the raw data for key extraction. Also note that the active symmetrization is not longer needed.

(f) Finally, Alice and Bob perform error correction and privacy amplification to distill their secret key from all the block of raw data of size n .

As an example, Fig. 2 shows a comparison of the finite-size key rates (against Gaussian attacks) obtained using different approaches. The plot is obtained for the symmetric setting where the channel from Alice is the same as the channel from Bob. The choice of the other parameters are described in the figure caption. To emphasize the impact of our method, the plot is obtained by taking into account only the finite-size effects related to parameter estimation. As expected, this numerical example shows that the impact on boosting the key rate can be relevant in the finite-size regime.

VI. CONCLUSIONS

We have analyzed the efficiency of two routines in CV QKD: energy test and parameter estimation. We have shown that these routines can be realized in a resource-efficient way where all the raw data are used for key extraction, hence, improving the expected secret key rate. Here we have focused on the no-switching protocols of Weedbrook *et al.* [16] and Braunstein and Pirandola [18]. The security analysis of *switching* protocols where the users choose between two quadratures for encoding information is less developed when it comes to general coherent attacks. However, it is reasonable to expect that our conclusions may as well be extended to these protocols.

The goal of the energy test is to project the infinite-dimensional Hilbert space that characterizes CV systems into a finite-dimensional one. Here we have used an approach previously introduced in Ref. [10] in the context of parameter estimation to show that all the raw data can be used for the energy test and for key extraction. As the energy test is necessary to achieve composable security against coherent attacks, this result will allow to improve the feasibility of CV QKD. In fact, our approach does not require active symmetrization of the measured data, which is computationally demanding and would make CV QKD impractical.

We have as well analyzed the routine of parameter estimation in CV MDI QKD and have established the composable security of the protocols introduced in Refs. [22,23]. These protocols allow us to use all the raw data for both key extraction and parameter estimation (in some regimes this property can be extended to more general protocols [22]). To show this we have applied the following line of reasoning: (1) Our starting point is a standard CV MDI QKD protocol, described in the EB representation, whose composable security against coherent attacks has been established in Refs. [15,17]; (2) we have considered its equivalent PM protocol, which is also secure; (3) we have shown that the parameter estimation in the PM protocol is covariant under the relevant symmetry group and can be implemented without revealing any information about the raw data; (4) finally, as no raw data is revealed, it follows that it is possible for Alice and Bob to use all their raw keys for both parameter estimation and key extraction, hence, allowing a higher key rate in the finite-size regime.

ACKNOWLEDGMENT

This work was supported by the EPSRC Quantum Communications Hub, Grant No. EP/T001011/1.

APPENDIX A: COVARIANCE MATRICES

Consider state ρ_{AB} of two modes. The CM of the Wigner function is

$$V_W = \frac{1}{2} \left\langle \begin{pmatrix} \hat{q}_A - \langle \hat{q}_A \rangle \\ \hat{p}_A - \langle \hat{p}_A \rangle \\ \hat{q}_B - \langle \hat{q}_B \rangle \\ \hat{p}_B - \langle \hat{p}_B \rangle \end{pmatrix} (q_A - \langle \hat{q}_A \rangle, \quad \hat{p}_A - \langle \hat{p}_A \rangle, \quad \hat{q}_B - \langle \hat{q}_B \rangle, \quad \hat{p}_B - \langle \hat{p}_B \rangle) + \text{H.c.} \right\rangle, \quad (\text{A1})$$

where H.c. stands for the Hermitian conjugate and $\langle O \rangle = \text{Tr}(\hat{O}\rho_{AB})$ is the quantum mechanical expectation value of the operator \hat{O} .

If we measure the two modes of ρ_{AB} by heterodyne detection, the outcomes of the measurements $\alpha = (q_A^{\text{het}} + ip_A^{\text{het}})/\sqrt{2}$ and $\beta = (q_B^{\text{het}} + ip_B^{\text{het}})/\sqrt{2}$ define a set of four real-value random variables. The corresponding CM is

$$V_{\text{EB}}^{\text{het}} = \mathbb{E} \left[\begin{pmatrix} q_A^{\text{het}} - \mathbb{E}[q_A^{\text{het}}] \\ p_A^{\text{het}} - \mathbb{E}[p_A^{\text{het}}] \\ q_B^{\text{het}} - \mathbb{E}[q_B^{\text{het}}] \\ p_B^{\text{het}} - \mathbb{E}[p_B^{\text{het}}] \end{pmatrix} (q_A^{\text{het}} - \mathbb{E}[q_A^{\text{het}}], \quad p_A^{\text{het}} - \mathbb{E}[p_A^{\text{het}}], \quad q_B^{\text{het}} - \mathbb{E}[q_B^{\text{het}}], \quad p_B^{\text{het}} - \mathbb{E}[p_B^{\text{het}}]) \right], \quad (\text{A2})$$

where $\mathbb{E}[O]$ denotes the expectation value of the random variable O . This is related to the Wigner function CM by the relation,

$$V_{\text{EB}}^{\text{het}} = V_W + I/2, \quad (\text{A3})$$

where I is the identity matrix.

Consider now a one-way PM protocol where Alice prepares coherent states of amplitude $\alpha = (q_A^{\text{pre}} + ip_A^{\text{pre}})/\sqrt{2}$ and sends them to Bob, and Bob measures them by heterodyne detection. The amplitude measured by Bob is denoted as $\beta = (q_B^{\text{het}} + ip_B^{\text{het}})/\sqrt{2}$. The CM of these variables is

$$V_{\text{PM}}^{\text{one-way}} = \mathbb{E} \left[\begin{pmatrix} q_A^{\text{pre}} - \mathbb{E}[q_A^{\text{pre}}] \\ p_A^{\text{pre}} - \mathbb{E}[p_A^{\text{pre}}] \\ q_B^{\text{het}} - \mathbb{E}[q_B^{\text{het}}] \\ p_B^{\text{het}} - \mathbb{E}[p_B^{\text{het}}] \end{pmatrix} (q_A^{\text{pre}} - \mathbb{E}[q_A^{\text{pre}}], \quad p_A^{\text{pre}} - \mathbb{E}[p_A^{\text{pre}}], \quad q_B^{\text{het}} - \mathbb{E}[q_B^{\text{het}}], \quad p_B^{\text{het}} - \mathbb{E}[p_B^{\text{het}}]) \right], \quad (\text{A4})$$

which is related to the EB heterodyne CM by the relation,

$$V_{\text{PM}}^{\text{one-way}} = \begin{pmatrix} \sqrt{\frac{N_A}{N_A+1}} & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{N_A}{N_A+1}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} V_{\text{EB}}^{\text{het}} \begin{pmatrix} \sqrt{\frac{N_A}{N_A+1}} & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{N_A}{N_A+1}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (\text{A5})$$

In CV MDI QKD, both Alice and Bob locally prepare coherent states with random amplitudes $\alpha = (q_A^{\text{pre}} + ip_A^{\text{pre}})/\sqrt{2}$ and $\beta = (q_B^{\text{pre}} + ip_B^{\text{pre}})/\sqrt{2}$ where the amplitudes are Gaussian with zero mean and variance N_A and N_B , respectively. The CM of these variables is

$$V_{\text{PM}}^{\text{MDI}} = \mathbb{E} \left[\begin{pmatrix} q_A^{\text{pre}} - \mathbb{E}[q_A^{\text{pre}}] \\ p_A^{\text{pre}} - \mathbb{E}[p_A^{\text{pre}}] \\ q_B^{\text{pre}} - \mathbb{E}[q_B^{\text{pre}}] \\ p_B^{\text{pre}} - \mathbb{E}[p_B^{\text{pre}}] \end{pmatrix} (q_A^{\text{pre}} - \mathbb{E}[q_A^{\text{pre}}], \quad p_A^{\text{pre}} - \mathbb{E}[p_A^{\text{pre}}], \quad q_B^{\text{pre}} - \mathbb{E}[q_B^{\text{pre}}], \quad p_B^{\text{pre}} - \mathbb{E}[p_B^{\text{pre}}]) \right], \quad (\text{A6})$$

with

$$V_{\text{PM}}^{\text{MDI}} = \begin{pmatrix} \sqrt{\frac{N_A}{N_A+1}} & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{N_A}{N_A+1}} & 0 & 0 \\ 0 & 0 & \sqrt{\frac{N_B}{N_B+1}} & 0 \\ 0 & 0 & 0 & -\sqrt{\frac{N_B}{N_B+1}} \end{pmatrix} V_{\text{EB}}^{\text{het}} \begin{pmatrix} \sqrt{\frac{N_A}{N_A+1}} & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{N_A}{N_A+1}} & 0 & 0 \\ 0 & 0 & \sqrt{\frac{N_B}{N_B+1}} & 0 \\ 0 & 0 & 0 & -\sqrt{\frac{N_B}{N_B+1}} \end{pmatrix}. \quad (\text{A7})$$

APPENDIX B: PARAMETER ESTIMATION FOR GAUSSIAN ATTACKS

Consider k i.i.d. Gaussian variables X_1, \dots, X_k , which are with zero mean and variance $\mathbb{E}[X^2]$. The random variable $\chi_k = \mathbb{E}[X^2]^{-1} \sum_{j=1}^k X_j^2$ is distributed as χ^2 variable of degree k . We have

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j^2 > (1+t)\mathbb{E}[X^2] \right\} < e^{-kt^2/8}, \tag{B1}$$

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j^2 < (1-t)\mathbb{E}[X^2] \right\} < e^{-kt^2/8}. \tag{B2}$$

Consider now another set of i.i.d. zero-mean Gaussian variables Y_1, \dots, Y_k with variance $\mathbb{E}[Y^2]$. From

$$\left\{ \sum_{j=1}^k X_j^2 > a \right\} \quad \text{and} \quad \left\{ \sum_{j=1}^k Y_j^2 > b \right\} \quad \Rightarrow \quad \left\{ \sum_{j=1}^k X_j^2 + Y_j^2 > a + b \right\}, \tag{B3}$$

it follows that

$$\left\{ \sum_{j=1}^k X_j^2 + Y_j^2 < a + b \right\} \quad \Rightarrow \quad \left\{ \sum_{j=1}^k X_j^2 < a \right\} \quad \text{or} \quad \left\{ \sum_{j=1}^k Y_j^2 < b \right\}. \tag{B4}$$

This, in turn, implies

$$\Pr \left\{ \sum_{j=1}^k X_j^2 + Y_j^2 < a + b \right\} \leq \Pr \left\{ \sum_{j=1}^k X_j^2 < a \right\} + \Pr \left\{ \sum_{j=1}^k Y_j^2 < b \right\}. \tag{B5}$$

In particular, we obtain

$$\Pr \left\{ \mathbb{E}[X^2] + \mathbb{E}[Y^2] > \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k X_j^2 + Y_j^2 \right\} < 2e^{-kt^2/8}. \tag{B6}$$

Consider now the identities,

$$(X + Y)^2 - (X - Y)^2 = 4XY, \tag{B7}$$

$$(X + Y)^2 + (X - Y)^2 = 2X^2 + 2Y^2, \tag{B8}$$

where $(X + Y)$ and $(X - Y)$ are both Gaussian variables. We can, therefore, write

$$\Pr \left\{ \mathbb{E}[(X + Y)^2] < \frac{1}{1+t} \frac{1}{k} \sum_{j=1}^k (X_j + Y_j)^2 \right\} < e^{-kt^2/8}, \tag{B9}$$

$$\Pr \left\{ \mathbb{E}[(X - Y)^2] > \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k (X_j - Y_j)^2 \right\} < e^{-kt^2/8}. \tag{B10}$$

This implies

$$\Pr \left\{ \mathbb{E}[(X + Y)^2] - \mathbb{E}[(X - Y)^2] < \frac{1}{1+t} \frac{1}{k} \sum_{j=1}^k (X_j + Y_j)^2 - \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k (X_j - Y_j)^2 \right\} < 2e^{-kt^2/8}, \tag{B11}$$

which is equivalent to

$$\Pr \left\{ \mathbb{E}[XY] < \frac{1}{1-t^2} \frac{1}{k} \sum_{j=1}^k X_j Y_j - \frac{t}{1-t^2} \frac{1}{k} \sum_{j=1}^k \frac{X_j^2 + Y_j^2}{2} \right\} < 2e^{-kt^2/8}. \tag{B12}$$

In the same way, starting from

$$\Pr \left\{ \mathbb{E}[(X + Y)^2] > \frac{1}{1-t} \frac{1}{k} \sum_{j=1}^k (X_j + Y_j)^2 \right\} < e^{-kt^2/8}, \tag{B13}$$

$$\Pr \left\{ \mathbb{E}[(X - Y)^2] < \frac{1}{1+t} \frac{1}{k} \sum_{j=1}^k (X_j - Y_j)^2 \right\} < e^{-kt^2/8}, \tag{B14}$$

we obtain

$$\Pr \left\{ \mathbb{E}[XY] > \frac{1}{1-t^2} \frac{1}{k} \sum_{j=1}^k X_j Y_j + \frac{t}{1-t^2} \frac{1}{k} \sum_{j=1}^k \frac{X_j^2 + Y_j^2}{2} \right\} < 2e^{-kt^2/8}. \tag{B15}$$

Finally, consider a set of four variables X , Y , W , and Z . By combining the above results we obtain

$$\Pr \left\{ \left| \mathbb{E}[XY] - \mathbb{E}[WZ] \right| < \frac{1}{1-t^2} \frac{1}{k} \left| \sum_{j=1}^k X_j Y_j - W_j Z_j \right| - \frac{t}{1-t^2} \frac{1}{k} \sum_{j=1}^k \frac{X_j^2 + Y_j^2 + W_j^2 + Z_j^2}{2} \right\} < 4e^{-kt^2/8}. \tag{B16}$$

Further tail bounds

Proceeding as above, we obtain

$$\Pr \left\{ \sum_{j=1}^k (X_j + Y_j)^2 - (X_j - Y_j)^2 > (1+t)k\mathbb{E}[(X+Y)^2] - (1-t)k\mathbb{E}[(X-Y)^2] \right\} < 2e^{-kt^2/8}, \tag{B17}$$

which implies

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j Y_j > \mathbb{E}[XY] + t \frac{\mathbb{E}[X^2] + \mathbb{E}[Y^2]}{2} \right\} < 2e^{-kt^2/8}. \tag{B18}$$

Similarly we obtain

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j Y_j < \mathbb{E}[XY] - t \frac{\mathbb{E}[X^2] + \mathbb{E}[Y^2]}{2} \right\} < 2e^{-kt^2/8}. \tag{B19}$$

Finally, given four variables X , Y , W , and Z , by combining the above results we obtain

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j Y_j - W_j Z_j > \mathbb{E}[XY] - \mathbb{E}[WZ] + t \frac{\mathbb{E}[X^2] + \mathbb{E}[Y^2] + \mathbb{E}[W^2] + \mathbb{E}[Z^2]}{2} \right\} < 4e^{-kt^2/8}, \tag{B20}$$

$$\Pr \left\{ \frac{1}{k} \sum_{j=1}^k X_j Y_j - W_j Z_j < \mathbb{E}[XY] - \mathbb{E}[WZ] - t \frac{\mathbb{E}[X^2] + \mathbb{E}[Y^2] + \mathbb{E}[W^2] + \mathbb{E}[Z^2]}{2} \right\} < 4e^{-kt^2/8}. \tag{B21}$$

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in quantum cryptography*, *Adv. Opt. Photon.* **12**, 1012 (2020).

[2] M. Mosca, *Cybersecurity in an Era with quantum computers: Will we be ready?* *IEEE Security & Privacy* **16**, 38 (2018).

[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, *Practical challenges in quantum key distribution*, *npj Quantum Inf.* **2**, 16025 (2016).

[4] G. Zhang, J. Y. 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).

[5] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu *et al.*, *Continuous-variable QKD over 50 km commercial fiber*, *Quantum Sci. Technol.* **4**, 035006 (2019).

[6] 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).

[7] 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).

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

[9] M. Navascués, F. Grosshans, and A. Acín, *Optimality of Gaussian Attacks in Continuous-variable Quantum Cryptography*, *Phys. Rev. Lett.* **97**, 190502 (2006).

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

[11] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, *The universal composable security of quantum key distribution*, in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian, Lecture Notes in Computer Science Vol. 3378 (Springer-Verlag, Berlin, 2005), pp. 386–406.

[12] 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); **112**, 019902(E) (2014).
- [13] F. Furrer, Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle, *Phys. Rev. A* **90**, 042325 (2014).
- [14] M. Christandl, R. König, and R. Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [15] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, *Phys. Rev. Lett.* **118**, 200501 (2017).
- [16] 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).
- [17] 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).
- [18] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [19] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [20] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* **89**, 052301 (2014).
- [21] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photon.* **9**, 397 (2015).
- [22] 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).
- [23] 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).
- [24] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous-variable quantum cryptography using two-way quantum communication, *Nat. Phys.* **4**, 726 (2008).
- [25] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro, Security-proof framework for two-way Gaussian quantum-key-distribution protocols, *Phys. Rev. A* **98**, 032332 (2018).
- [26] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates, *Phys. Rev. A* **94**, 012322 (2016).
- [27] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Floodlight quantum key distribution: Demonstrating a framework for high-rate secure communication, *Phys. Rev. A* **95**, 012332 (2017).
- [28] Q. Zhuang, Z. Zhang, and J. H. Shapiro, High-order encoding schemes for floodlight quantum key distribution, *Phys. Rev. A* **98**, 012323 (2018).
- [29] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).
- [30] P. Aniello, C. Lupo, and M. Napolitano, Exploring representation theory of unitary groups via linear optical passive devices, *Open Syst. Inf. Dyn.* **13**, 415 (2006).
- [31] A. Leverrier, SU(p, q) coherent states and a Gaussian de Finetti theorem, *J. Math. Phys.* **59**, 042202 (2018).
- [32] A more general displacement of the form $\gamma_A = u_A z + v_A z^*$, $\gamma_B = u_B z^* + v_B z$ with $u_A, v_A, u_B, v_B \in \mathbb{C}$ was considered in Refs. [22,23]. The displacement rule in Eq. (14) is less general but is explicitly covariant under the transformation $a_j \rightarrow \sum_{k=1}^n U_{jk} a_k$, $b_j^\dagger \rightarrow \sum_{k=1}^n U_{jk} b_k^\dagger$, $z_j \rightarrow \sum_{k=1}^n U_{jk} z_k$ for any unitary matrix U .
- [33] The symmetry of the state implies that $\mathbb{E}[q_A] + i\mathbb{E}[p_A] = \sum_k U_{jk} (\mathbb{E}[q_A] + i\mathbb{E}[p_A])$ for any unitary matrix U . This condition is satisfied if only $\mathbb{E}[q_A] + i\mathbb{E}[p_A] = 0$. The same conclusion holds for $\mathbb{E}[q_B]$ and $\mathbb{E}[p_B]$.