Article:
Lupo, C. and Ouyang, Y. (2022) Quantum key distribution with nonideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols. PRX Quantum, 3. 010341. ISSN: 2691-3399

https://doi.org/10.1103/prxquantum.3.010341

Quantum Key Distribution with Nonideal Heterodyne Detection: Composable Security of Discrete-Modulation Continuous-Variable Protocols

Cosmo Lupo[1,*,†] and Yingkai Ouyang[2]

[1] *Dipartimento Interateneo di Fisica, Politecnico di Bari, Bari 70126, Italy*

[2] *Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583*

(Received 4 August 2021; revised 4 October 2021; accepted 14 February 2022; published 14 March 2022)

Continuous-variable quantum key distribution exploits coherent measurements of the electromagnetic field, i.e., homodyne or heterodyne detection. The most advanced security proofs developed so far have relied on idealized mathematical models for such measurements, which assume that the measurement outcomes are continuous and unbounded variables. As physical-measurement devices have a finite range and precision, these mathematical models only serve as an approximation. It is expected that, under suitable conditions, the predictions obtained using these simplified models will be in good agreement with the actual experimental implementations. However, a quantitative analysis of the error introduced by this approximation, and of its impact on composable security, have been lacking so far. Here, we present a theory to rigorously account for the experimental limitations of realistic heterodyne detection. We focus on collective attacks and present security proofs for the asymptotic and finite-size regimes, the latter being within the framework of composable security. In doing this, we establish for the first time the composable security of discrete-modulation continuous-variable quantum key distribution in the finite-size regime. Tight bounds on the key rates are obtained through semidefinite programming and do not rely on a truncation of the Hilbert space.

DOI: 10.1103/PRXQuantum.3.010341

I. INTRODUCTION

Quantum key distribution (QKD) is the art of exploiting quantum optics to distribute a secret key between distant authenticated users. Such a secret key can then be used as a one-time pad to achieve unconditionally secure communication. First introduced in the 1980s by Bennett and Brassard [1], QKD is now at the forefront of quantum science and technology. By encoding information into the quantum electromagnetic field, QKD enables provably secure communication through an insecure communication channel, a task known to be impossible in classical physics. This contrasts with standard and postquantum cryptography, which are based on computational assumptions and do not guarantee long-term security. In fact, future advancements in theoretical computer science or computational power (including quantum computing) may jeopardize the security of these schemes.

To travel the route from fundamental physics to future technologies, we need to account for the trade-off between the rate of key generation of the protocol, its security, and the feasibility and robustness to experimental imperfection. The highest standards of security and robustness are those of device-independent QKD but are achieved at the cost of a reduced key rate. Here, we focus on continuous-variable (CV) QKD, within the device-dependent approach, which allows for feasible implementations with much higher key rates. Our goal is to improve the robustness of CV QKD to experimental imperfections and practical limitations. For a recent review of device-independent QKD and CV QKD, see Ref. [2].

CV QKD denotes a family of protocols where information is carried by the phase and quadrature of the quantum electromagnetic field. A variety of protocols exist that differ in how the quadratures encode this information [3–7]. However, when it comes to decoding, all CV-QKD protocols exploit coherent measurements of the field, i.e., either homodyne or heterodyne detection [8]. The strategic importance of CV QKD indeed relies on this choice of measurement, as homodyne and heterodyne detection are mature, scalable, and noise-resilient technologies. This

*cosmo.lupo@poliba.it

†Previous affiliation: Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, United Kingdom

is in contrast with discrete-variable architectures, which require bulky, high-efficiency, and low-noise single-photon detectors [9].

When modeling a CV-QKD protocol, it is customary to describe its measurement outcomes as continuous and unbounded variables. In these models, homodyne detection measures one quadrature of the field and heterodyne detection provides a joint measurement of both quadrature and phase [8]. These simplified models are powerful mathematical tools due to their continuous symmetry. Two fundamental theoretical results rely on this symmetry: the *optimality of Gaussian attacks* [10–12] and the *Gaussian de Finetti reduction* [13]. However, this symmetry is not exact and is broken by real-world physical devices. In fact, in actual experimental implementations, homodyne and heterodyne detection yield digital outcomes and have a finite range [14,15]. While it is expected that, in some limit, the idealized measurement models will describe actual physical devices well, up to now a quantitative analysis of this approximation has been lacking. In particular, it has not been known how to quantify the impact of these nonidealities on the secret key rate.

In this work, we finally fill this important conceptual gap and present a theory to quantify the secret key rates obtained in actual QKD protocols that exploit actual measurement devices. Up to now, only a handful of results have been available in this direction. Furrer *et al.* have considered digitized homodyne for a protocol based on the distribution of entangled states [6] and Matsuura *et al.* have considered a binary encoding using coherent states, homodyne detection, and a test phase exploiting heterodyne [7]. However, in both cases the key rates do not converge to the asymptotic bounds obtained in Refs. [13,16–18], which are believed to be optimal for ideal detection. In contrast, our results converge to these optimal bounds when the nonidealities are sufficiently small.

We focus on discrete-modulation (DM) protocols, where the sender prepares coherent states the amplitudes of which are sampled from a discrete ensemble. We establish the security against collective attacks in both the asymptotic and the nonasymptotic regime, the latter within the framework of composable security [19]. This contrasts with previous works on DM CV QKD [16–18,20], which have only considered the asymptotic limit of infinite channel uses. Our composable-security proof allows us to quantify the security of QKD in the practical scenario where the number of signal exchanges is finite and QKD is used as a subroutine of an overarching cryptography protocol. Although collective attacks are not the most general attacks, they are known to be optimal, up to some finite-size corrections, through de Finetti reduction [13,21,22] While we focus on heterodyne detection, the same approach may also be applied, with some modifications, to homodyne detection.

II. STRUCTURE OF THE PAPER AND SUMMARY OF RESULTS

We introduce DM CV QKD with nonideal heterodyne detection in Sec. III and review its asymptotic security in Sec. IV. We discuss using a data-driven approach to approximate infinite-dimensional states with ones with finite-dimensional support in Sec. V and in Sec. VI we calculate corresponding corrections to our secret key rate by using a continuity argument.

We bound the secret key rates in three different settings with increasing complexity, where in each setting we find the optimal values using linear semidefinite programming. In the first setting (Sec. VII), the semidefinite programs are still over infinite-dimensional quantum states and knowledge of their optimal values would allow one to determine the secret key rate in the asymptotic limit. In the second setting (Sec. VIII), we map the infinite-dimensional semidefinite programs of Sec. VII into finite-dimensional ones, the latter of which can be solved numerically without truncating the Hilbert space. This gives us a way to exactly numerically evaluate the secret key rate in the asymptotic limit. In the third setting (Sec. IX), within a composable-security framework, we generalize the theory of asymptotic QKD to nonasymptotic QKD; we show how perturbations to the semidefinite programs in Sec. VIII depend on the number of channel uses and we prove that these perturbations vanish when the number of channel uses becomes arbitrarily large. This result allows us to estimate the secret key rate of a nonasymptotic DM-CV-QKD scheme with composable security.

Explicit examples are discussed in Sec. X, for the case of quadrature phase-shift keying (QPSK). These examples suggest that, in the limit of vanishing nonidealities in heterodyne measurement and a growing number of channel uses, the secret key rate of DM CV QKD approaches the highest rate possible. Conclusions and potential future developments are discussed in Sec. XI.

Table I compares our results with previous works that have also presented security analysis of CV-QKD protocols. We only consider works that have obtained a tight estimation of the key rate. The encoding of classical information in quantum signals may happen through either a continuous modulation (CM) or a discrete modulation (DM). In this work, we consider DM, which reflects what is actually done in experiments. We obtain our security proof within the framework of composable security, which is the gold standard in cryptography; composable security permits a quantitative assessment of the security of QKD, including when the QKD protocol is a subroutine of an overarching communication protocol. We consider a realistic model of actual heterodyne detection, instead of the ideal model used in previous works. Our numerical calculation of the lower bound on the secret key rate is exact, as we do not need to impose an arbitrary cutoff of the Hilbert space.

TABLE I. A comparison of our results with previous security analyses of CV QKD. We only include works that have provided a tight estimate of the key rates. Encoding: the protocol considered has continuous (CM) or discrete (DM) modulation. Composable: the security analysis is in the framework of composable security. Heterodyne: the security analysis assumes an ideal or realistic model for heterodyne detection. Key rate: the estimation of the key rate is exact or obtained through numerical approximation.

	Encoding	Composable	Heterodyne	Key rate
Ref. [13]	CM	✔	Ideal	Exact
Ref. [17]	DM	✖	Ideal	Approx.
Ref. [18]	DM	✖	Ideal	Approx.
Ref. [20]	DM	✖	Ideal	Exact
Ref. [16]	DM	✖	Ideal	Exact
This work	DM	✔	Realistic	Exact

III. THE MODEL

We consider one-way QKD where one user (conventionally called Alice) prepares quantum states and sends them to the other user (called Bob), who measures them by heterodyne detection. The transmission is through an insecure quantum channel that may be controlled by an adversary (called Eve). This general scheme defines a *prepare-and-measure* (PM) protocol. In this work, we focus on DM-CV-QKD protocols where, on each channel use, Alice prepares a coherent state $|\alpha\rangle$ the amplitude of which is sampled from an M-ary set, $\{\alpha_x\}_{x=0,\ldots,M-1}$, with probabilities $\mathcal{P}_x$. This defines Alice's M-ary random variable X. An example is QPSK, obtained for $M=4$ and setting $\alpha_x = \alpha i^x$, $\mathcal{P}_x = 1/4$.

In order to prove the security of these protocols, we need to consider a different, though formally equivalent, scenario where a bipartite quantum state ρ_{AB} is distributed to Alice and Bob, of which Eve holds a purification. This kind of setting defines an *entanglement-based* (EB) protocol. It is sufficient to prove the security of the EB protocol, from which the security of the PM protocol follows. In the EB protocol, the state ρ is a two-mode state, where a and $a^\dagger$, and b and $b^\dagger$, are the annihilation and creation operators for Alice and Bob, respectively. The EB representation of DM-CV-QKD protocols is discussed in detail in Ref. [16]. In this work, we focus on *collective attacks*, which are identified by the assumption that, over n uses of the quantum channel, the state factorizes and has the form $\rho_{AB}^{\otimes n}$. In the following, we indicate as $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ the reduced state on Bob's side. To make the notation lighter, we sometimes drop the subscripts AB or B when the meaning is clear from the context.

On the receiver's side, Bob measures by applying heterodyne detection. Ideally, heterodyne detection is a joint measurement of the quadrature (q) and phase (p) of the field, the output of which can be described as a complex variable $\beta = (q+ip)/\sqrt{2}$. Ideal heterodyne detection, applied on a state ρ, would yield a continuous and unbounded output, with probability density $1/\pi\,\langle\beta|\rho|\beta\rangle$, where $|\beta\rangle$ is the coherent state of amplitude β. In contrast, actual experimental realizations of heterodyne detection have measurement outcomes that are confined to a finite region in phase space, $\beta \in \mathcal{R}(R)$, and hence have finite range. Here, we assume that the region $\mathcal{R}(R)$ is defined by the condition $q,p \in [-R,R]$, for some $R>0$. Furthermore, the measurement outputs are digital, such that each quadrature takes d values, with each value corresponding to a unique $\log d$-bit string. This is obtained by binning the values of $q \in [-R,R]$ into d nonoverlapping intervals. For simplicity, we consider intervals of equal size,

$$\mathcal{I}_j = [-R+2(j-1)R/d, -R+2jR/d], \tag{1}$$

for $j=1,\ldots,d$. The output j is then associated with the event $q \in \mathcal{I}_j$, which, in turn, we identify by the central value:

$$q_j = -R+(j-1)R/d + jR/d. \tag{2}$$

The same digitization, when applied to both q and p, yields a description of actual heterodyne detection as a measurement with d^2 possible outputs. This defines Bob's variable Y, which is a discrete random variable and assumes d^2 values. These discrete values can be conveniently labeled using the central points of each interval, i.e.,

$$\beta_{jk} = (q_j + ip_k)/\sqrt{2}. \tag{3}$$

If Bob obtains the average state ρ_B, then the probability of measuring β_{jk} is

$$P_{jk} = \int_{\beta\in\mathcal{I}_{jk}} \frac{d^2\beta}{\pi}\langle\beta|\rho_B|\beta\rangle, \tag{4}$$

where the complex interval $\mathcal{I}_{jk}$ is defined in such a way that $\beta \in \mathcal{I}_{jk}$ if and only if $q \in \mathcal{I}_j$ and $p \in \mathcal{I}_k$, and $d^2\beta = \frac{1}{2}\,dqdp$. Finally, there is a nonzero probability

$$P_0(R) = 1 - \int_{\beta\in\mathcal{R}(R)} \frac{d^2\beta}{\pi}\langle\beta|\rho_B|\beta\rangle \tag{5}$$

of an inconclusive measurement, when the amplitude lies outside the measurement range.

IV. ASYMPTOTIC SECURITY OF CV QKD

In the limit that $n\to\infty$, the secret key rate (i.e., the number of secret bits that can be distilled per transmission

of the signal) is given by the Devetak-Winter formula [23]:

$$r_\infty = \xi I(X;Y) - \chi(Y;E)_\rho, \tag{6}$$

where $I(X;Y)$ is the mutual information between Alice and Bob and $\chi(Y;E)_\rho$ is the Holevo information (quantum mutual information) between Bob and Eve (here, we assume reverse reconciliation on Bob's data, which is optimal for long-distance communication). The factor $\xi \in (0,1)$ accounts for the subunit efficiency of error correction. While $I(X;Y)$ only depends on X and Y, $\chi(Y;E)_\rho$ also depends on the quantum information held by Eve, which in general cannot be estimated directly. Fortunately, the property of extremality of Gaussian states [11,12] allows us to write the upper bound

$$\chi(Y;E)_\rho \leq f_\chi[\gamma_A(\rho), \gamma_B(\rho), \gamma_{AB}(\rho)], \tag{7}$$

where f_χ is a known function of the covariance matrix (CM) elements (see Appendix A):

$$\gamma_A(\rho) := \frac{1}{2}\mathrm{Tr}[(a^\dagger a + aa^\dagger)\rho], \tag{8}$$

$$\gamma_B(\rho) := \frac{1}{2}\mathrm{Tr}[(b^\dagger b + bb^\dagger)\rho], \tag{9}$$

$$\gamma_{AB}(\rho) := \frac{1}{2}\mathrm{Tr}[(a^\dagger b^\dagger + ab)\rho]. \tag{10}$$

In conclusion, estimation of the CM suffices to obtain a universal upper bound on the Holevo information, which holds for collective attacks in the limit of $n \to \infty$. The asymptotic key rate is thus bounded as

$$r_\infty \geq \xi I(X;Y) - f_\chi[\gamma_A(\rho), \gamma_B(\rho), \gamma_{AB}(\rho)]. \tag{11}$$

Since f_χ is an increasing function of γ_A and γ_B and a decreasing function of γ_{AB} [24], the estimation of upper bounds on γ_A, γ_B and a lower bound on γ_{AB} suffices to bound the asymptotic key rate. In practical realizations of CV QKD, where the parameter γ_A is known by definition of the protocol, one only needs to bound γ_B and γ_{AB}.

V. PHOTON-NUMBER CUTOFF

The technical difficulties in the analysis of CV QKD are due to the fact that the quantum information carriers reside in a Hilbert space with infinite dimensions. To overcome this issue, we need to impose a cutoff in the Hilbert space. As we do not want to impose such a cutoff in an arbitrary way, we follow a data-driven approach. Define the following operators on Bob's side:

$$W_R = \int_{|\beta|^2 > R^2} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta| \tag{12}$$

and

$$V_R = \sum_{n > R^2} |n\rangle\langle n|, \tag{13}$$

where $|n\rangle$ is the Fock state with n photons. Renner and Cirac [22] have noted that

$$V_R \leq 2W_R. \tag{14}$$

From the experimental data, Bob can estimate the probability $P_0(R)$ as in Eq. (5). Note that

$$W_R \leq \int_{|\beta|^2 \notin \mathcal{R}(R)} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta|, \tag{15}$$

from which we obtain

$$\mathrm{Tr}(V_R\rho_B) \leq 2\mathrm{Tr}(W_R\rho_B) \leq 2P_0(R). \tag{16}$$

This shows that the probability that Bob receives more than $2R^2$ photons is no larger than $2P_0(R)$. The gentle measurement lemma [25] then yields

$$\|\rho_{AB} - \tau_{AB}\|_1 \leq 2\sqrt{2P_0(R)}, \tag{17}$$

where

$$\tau_{AB} = \frac{(I \otimes \Pi)\rho_{AB}(I \otimes \Pi)}{\mathrm{Tr}(\Pi\rho_B)}, \tag{18}$$

is a normalized state with finite-dimensional support and

$$\Pi = I - V_R = \sum_{n \leq R^2} |n\rangle\langle n| \tag{19}$$

is the projector onto the subspace with up to $N = \lfloor R^2 \rfloor$ photons and $\|\cdot\|_1$ is the trace norm. In conclusion, though ρ is generic, an experimental estimation of the probability $P_0(R)$ allows us to determine the proximity of ρ to a state with finite-dimensional support.

VI. CONTINUITY OF THE HOLEVO INFORMATION

In the EB representation, the two-mode state ρ_{AB} is measured, on Bob's side, by heterodyne detection. In general, ρ_{AB} resides in a Hilbert space with infinite dimensions. However, as discussed above, it is close in trace norm to the state τ_{AB} in Eq. (18). Note that τ_{AB} has support in a space with $M \times \lfloor R^2 + 1 \rfloor$ dimensions.

The Holevo information is a continuous functional of the state. By applying Shirokov's continuity bound [26], we obtain

$$\chi(Y;E)_\rho \leq \chi(Y;E)_\tau + \delta, \tag{20}$$

where (in this paper, we put $\log \equiv \log_2$ and ln denotes the natural logarithm)

$$\delta = \delta' \log d^2 + 2(1+\delta')\log(1+\delta') - 2\delta' \log \delta', \tag{21}$$

with $\delta' = \|\rho_{AB} - \tau_{AB}\|_1 \leq 2\sqrt{2P_0(R)}$.

This implies that, by paying a small penalty in the key rate, we can replace ρ with the finite-dimensional state τ. We thereby obtain the following bound on the asymptotic key rate:

$$r_\infty \geq \xi I(X;Y) - f_\chi[\gamma_A(\tau), \gamma_B(\tau), \gamma_{AB}(\tau)] - \delta. \tag{22}$$

By comparing with Eq. (11), we note that this bound depends on the CM of τ. However, τ is only a mathematical tool and does not describe the state that is prepared and measured in the experimental realization of the protocol. The only state that is physically accessible is ρ. Below, we show how we can estimate the CM of τ by measuring ρ by heterodyne detection. In particular, our goal is to find an upper bound on $\gamma_B(\tau)$ and a lower bound on $\gamma_{AB}(\tau)$.

VII. SEMIDEFINITE PROGRAMMING

In the EB representation, Alice prepares the two-mode state

$$|\Psi\rangle_{AA'} = \sum_{x=0}^{M-1} \sqrt{\mathcal{P}_x}|\psi_x\rangle_A \otimes |\alpha_x\rangle_{A'}. \tag{23}$$

Alice keeps the mode A and sends A' to Bob. The vectors $|\psi_x\rangle$ are mutually orthogonal and span an M-dimensional subspace of Alice's mode A. Note that Alice's reduced state is

$$\rho_A = \sum_{x,x'=0}^{M-1} \sqrt{\mathcal{P}_x \mathcal{P}_{x'}}\langle \alpha_{x'}|\alpha_x\rangle |\psi_x\rangle\langle\psi_{x'}| =: \sigma. \tag{24}$$

The equivalence with the PM protocol is obtained by noticing that a projective measurement of A' in the basis $\{|\psi_x\rangle\}_{x=0,\ldots,M-1}$ prepares the mode A in the coherent state $|\alpha_x\rangle$ with probability $\mathcal{P}_x$. A good choice for the vectors $|\psi_x\rangle$'s is presented in Ref. [16].

Our goal is to bound the key rate using the data collected by Alice and Bob, where Bob's measurement is modeled as realistic heterodyne detection with finite range and precision. We follow the seminal ideas of Refs. [17,18] and achieve this by semidefinite programming (SDP). As an example, we apply linear SDP, as done in Ref. [17], to bound the CM of the state τ, but we remark that our theory can also apply to nonlinear SDP as in Ref. [18].

Let $\rho_B(x)$ be the state received by Bob given that Alice sent $|\alpha_x\rangle$. Alice and Bob can experimentally estimate the probability mass distribution

$$P_{jk|x} = \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi}\langle\beta|\rho_B(x)|\beta\rangle, \tag{25}$$

which can be used as a constraint in the SDP that we later formulate. We can also consider linear combinations of the parameters $P_{jk|x}$, which obviously are also experimentally accessible. Here, we consider the quantities

$$v := \sum_{j,k=1}^{d} |\beta_{jk}|^2 P_{jk}, \tag{26}$$

$$c := \sum_{x=0}^{M-1} \mathcal{P}_x \sum_{j,k=1}^{d} \frac{\bar{\alpha}_x \beta_{jk} + \alpha_x \bar{\beta}_{jk}}{2} P_{jk|x} \tag{27}$$

[where the sign ("¯") denotes complex conjugation], which are the expectation values of the variance and the covariance between Alice's and Bob's variables. Note that $v = \mathrm{Tr}(\mathcal{V}\rho)$ and $c = \mathrm{Tr}(\mathcal{C}\rho)$ are the expectation values of the operators

$$\mathcal{V} = \sum_{j,k=1}^{d} |\beta_{jk}|^2 \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi}|\beta\rangle\langle\beta|, \tag{28}$$

$$\mathcal{C} = \frac{1}{2}\sum_{x=0}^{M-1}\sum_{j,k=1}^{d} \bar{\alpha}_x \beta_{jk}|\psi_x\rangle\langle\psi_x| \otimes \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi}|\beta\rangle\langle\beta| + \mathrm{h.c.} \tag{29}$$

Similarly, from Eq. (5), the quantity $1 - P_0(R) = \mathrm{Tr}(\mathcal{U}\rho)$ is the expectation value of the operator

$$\mathcal{U} = \int_{\beta\in\mathcal{R}(R)} \frac{d^2\beta}{\pi}|\beta\rangle\langle\beta|. \tag{30}$$

Denote as $\tilde{\gamma}_B(\tau)$ the optimal value of the semidefinite program

$$\begin{aligned} &\underset{\rho_B\geq 0}{\text{maximize}} \frac{1}{2}\mathrm{Tr}[\Pi(b^\dagger b + bb^\dagger)\Pi\rho_B] \\ &\text{subject to} \mathrm{Tr}(\mathcal{V}\rho_B) \leq v \\ &\qquad\quad \mathrm{Tr}(\mathcal{U}\rho_B) \geq 1 - P_0(R) \\ &\qquad\quad \mathrm{Tr}(\rho_B) = 1. \end{aligned} \tag{31}$$

Taking normalization into account, we obtain the upper bound on $\gamma_B(\tau)$,

$$\gamma_B(\tau) \leq \frac{\tilde{\gamma}_B(\tau)}{\mathrm{Tr}(\Pi\rho_B)} \leq \frac{\tilde{\gamma}_B(\tau)}{1 - 2P_0(R)}. \tag{32}$$

Similarly, consider the optimal value $\tilde{\gamma}_{AB}(\tau)$ of the semidefinite program

$$\begin{aligned} \underset{\rho_{AB}\geq 0}{\text{minimize}} & \frac{1}{2}\text{Tr}[(a^\dagger \Pi b^\dagger \Pi + a\Pi b\Pi)\rho_{AB}] \\ \text{subject to} & \text{Tr}[(I\otimes \mathcal{V})\rho_{AB}] \leq v \\ & \text{Tr}(\mathcal{C}\rho_{AB}) \geq c \\ & \text{Tr}[(I\otimes \mathcal{U})\rho_{AB}] \geq 1 - P_0(R) \\ & \text{Tr}_B(\rho_{AB}) = \sigma \\ & \text{Tr}(\rho_{AB}) = 1, \end{aligned} \tag{33}$$

from which we obtain the lower bound

$$\gamma_{AB}(\tau) \geq \frac{\tilde{\gamma}_{AB}(\tau)}{\text{Tr}[(I\otimes\Pi)\rho_{AB}]} \geq \tilde{\gamma}_{AB}(\tau). \tag{34}$$

Note that the projector Π appears in the objective functions but not in the constraints. For this reason, we cannot simply replace ρ with τ and the optimal values of the semidefinite programs remain defined in an infinite-dimensional Hilbert space. However, when numerically solving these semidefinite programs, we find solutions of the form $\Pi\rho_B\Pi$ and $(I\otimes\Pi)\rho_{AB}(I\otimes\Pi)$. This suggests that the presence of the projector operator Π in the objective function suffices to make the problem effectively finite dimensional (see the Appendix D for further detail). To numerically evaluate the optimal values of these semidefinite programs, we derive the corresponding dual programs, which are more efficient to evaluate, and detail this in Appendix D.

VIII. FINITE-DIMENSIONAL SDP

In this section, we obtain, from Eqs. (31) and (33), two semidefinite programs that are defined in a finite-dimensional Hilbert space. We do this by replacing the constraints appearing in Eqs. (31) and (33) with weaker constraints. This represents no loss of generality, as our goal is to obtain an upper bound on $\gamma_B(\tau)$ and a lower bound on $\gamma_{AB}(\tau)$. We express the new semidefinite programs in terms of the normalized state τ_{AB}, defined in Eq. (18), which has support in the finite-dimensional subspace containing no more than $N = \lfloor R^2 \rfloor$ photons.

First, consider the semidefinite program in Eq. (31). Note that, since $\mathcal{V}$ is positive semidefinite, we have

$$\text{Tr}(\Pi\mathcal{V}\Pi\rho_B) \leq \text{Tr}(\mathcal{V}\rho_B). \tag{35}$$

Therefore, the condition $\text{Tr}(\mathcal{V}\rho_B) \leq v$ implies $\text{Tr}(\mathcal{V}\Pi\rho_B\Pi) \leq v$. Taking into account the fact that the trace of $\Pi\rho_B\Pi$ is larger than $1 - 2P_0(R)$ [from Eq. (16)], we obtain the following constraint:

$$\text{Tr}(\mathcal{V}\tau_B) = \frac{\text{Tr}(\mathcal{V}\Pi\rho_B\Pi)}{\text{Tr}(\Pi\rho_B\Pi)} \tag{36}$$

$$\leq \frac{\text{Tr}(\mathcal{V}\Pi\rho_B\Pi)}{1-2P_0(R)} \leq \frac{v}{1-2P_0(R)}. \tag{37}$$

Note also that the constraint $\text{Tr}(\mathcal{U}\rho_B) \geq 1 - P_0(R)$ can be rewritten as $\text{Tr}[(I-\mathcal{U})\rho_B] \leq P_0(R)$. As $I-\mathcal{U}$ is positive semidefinite, this constraint can be replaced with $\text{Tr}[(I-\mathcal{U})\Pi\rho_B\Pi] \leq P_0(R)$. Applying the same argument as above, we obtain the constraint

$$\text{Tr}((I-\mathcal{U})\tau_B) \leq \frac{P_0(R)}{1-2P_0(R)}, \tag{38}$$

which in turn implies

$$\text{Tr}(\mathcal{U}\tau_B) \geq 1 - \frac{P_0(R)}{1-2P_0(R)}. \tag{39}$$

Putting all this together, Eq. (31) can be replaced with the finite-dimensional semidefinite problem:

$$\begin{aligned} \underset{\tau_B\geq 0}{\text{maximize}} & \frac{1}{2}\text{Tr}[(b^\dagger b + bb^\dagger)\tau_B] \\ \text{subject to} & \text{Tr}(\mathcal{V}\tau_B) \leq \frac{v}{1-2P_0(R)} \\ & \text{Tr}(\mathcal{U}\tau_B) \geq 1 - \frac{P_0(R)}{1-2P_0(R)} \\ & \text{Tr}(\tau_B) = 1. \end{aligned} \tag{40}$$

Now consider Eq. (33). Note that the operator $\mathcal{C}$ is bounded,

$$\|\mathcal{C}\|_\infty = \sup_x \left\| \sum_{j,k=1}^{d} \frac{\bar{\alpha}_x\beta_{jk} + \alpha_x\bar{\beta}_{jk}}{2} \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta| \right\|_\infty \tag{41}$$

$$\leq \sup_{x,j,k} \frac{\left|\bar{\alpha}_x\beta_{jk} + \alpha_x\bar{\beta}_{jk}\right|}{2} \left\| \int_{\beta\in\mathcal{R}(R)} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta| \right\|_\infty \tag{42}$$

$$\leq \frac{1}{2} \sup_{x,j,k} \left|\bar{\alpha}_x\beta_{jk} + \alpha_x\bar{\beta}_{jk}\right|, \tag{43}$$

where $\|O\|_\infty = \sup_\psi \frac{|\langle\psi|O|\psi\rangle|}{\langle\psi|\psi\rangle}$ denotes the operator norm.

This observation allows us to express the constraint in terms of the state τ_{AB} instead of ρ_{AB} by introducing a small error,

$$|\mathrm{Tr}(\mathcal{C}\rho_{AB}) - \mathrm{Tr}(\mathcal{C}\tau_{AB})| = |\mathrm{Tr}[\mathcal{C}(\rho_{AB} - \tau_{AB})]| \quad (44)$$

$$\leq \|\mathcal{C}\|_\infty \|\rho_{AB} - \tau_{AB}\|_1 \quad (45)$$

$$\leq 2\sqrt{2P_0(R)}\|\mathcal{C}\|_\infty, \quad (46)$$

where the first inequality follows from the general property that $|\mathrm{Tr}(OO')| \leq \|O\|_\infty \|O'\|_1$, for any pair of Hermitian operators O, O'.

In conclusion, we replace Eq. (33) with the finite-dimensional semidefinite problem:

$$\begin{aligned} \underset{\tau_{AB}\geq 0}{\text{minimize}} \; & \frac{1}{2}\mathrm{Tr}[(a^\dagger b^\dagger + ab)\tau_{AB}] \\ \text{subject to} \; & \mathrm{Tr}[(I\otimes\mathcal{V})\tau_{AB}] \leq \frac{v}{1-2P_0(R)} \\ & \mathrm{Tr}(\mathcal{C}\tau_{AB}) \geq c - 2\sqrt{2P_0(R)}\|\mathcal{C}\|_\infty \\ & \mathrm{Tr}[(I\otimes\mathcal{U})\tau_{AB}] \geq 1 - \frac{P_0(R)}{1-2P_0(R)} \\ & \mathrm{Tr}_B(\rho_{AB}) = \sigma \\ & \mathrm{Tr}(\tau_{AB}) = 1. \end{aligned} \quad (47)$$

IX. NONASYMPTOTIC REGIME

Entropic uncertainty relations are often used to establish the security of QKD in the nonasymptotic regime [27]. In particular, they have been applied successfully in CV QKD by Furrer *et al.* [6]. Unfortunately, this elegant method does not yield a tight bound on the key rate for CV QKD. To quote Leverrier [13]:

> *"This [CV-QKD] protocol can be analyzed thanks to an entropic uncertainty relation, but [$\cdots$] this approach does not recover the secret key rate corresponding to Gaussian attacks in the asymptotic limit of large n, even though these attacks are expected to be optimal."*

In the same paper, Leverrier shows that the asymptotic equipartition property (AEP) [28] is better suited for CV QKD as it converges to the secret key rate corresponding to Gaussian attacks in the asymptotic limit.

As we show below, the theory developed in the previous sections can be extended to the nonasymptotic regime where a finite number n of signals is exchanged between Alice and Bob. To achieve this goal, we need to make two main modifications to our theoretical analysis.

The first modification accounts for the finite-size correction to the entropic functions appearing in the asymptotic rate in Eq. (22). These corrections can be computed using the AEP [28]:

$$r_n \geq \xi I(X;Y) - f_\chi[\gamma_A(\tau), \gamma_B(\tau), \gamma_{AB}(\tau)] - \delta - \frac{\Delta(d,\epsilon_s)}{\sqrt{n}} + \frac{2\log(\sqrt{2}\epsilon_h)}{n}, \quad (48)$$

where the additive term Δ can be bounded as [29]

$$\Delta(d,\epsilon_s) \leq 4(1+\log d)\sqrt{\log(2/\epsilon_s^2)} \quad (49)$$

and ϵ_s is the entropy smoothing parameter. Furthermore, Eq. (48) also includes a term due to privacy amplification, characterized by the hashing parameter ϵ_h. The corresponding key is secure up to probability $\epsilon = \epsilon_s + \epsilon_h$ (for more details, see Ref. [28]).

The invocation of the AEP is not sufficient to analyze the nonasymptotic regime. In order to achieve composable security in the nonasymptotic regime, we also need to provide confidence intervals for the channel parameters that are not known exactly but obtained through parameter estimation. Our second modification to our theory takes this into account, and we discuss this further below. The provision of confidence intervals for parameter estimation is a difficult problem in CV QKD because the variables measured in ideal homodyne or heterodyne detection are unbounded. This problem has been solved by Leverrier [13] by exploiting a continuous symmetry of heterodyne detection for CV-QKD protocol with Gaussian modulation. Unfortunately, discrete modulation occurs on a finite range and does not have a continuous symmetry. Hence, Leverrier's approach cannot be applied to any CV protocol with discrete modulation. In our work, since we consider nonideal heterodyne detection (which is bounded), we are able to compute confidence intervals for all the relevant parameters of the communication channel. Therefore, although the AEP can be applied to previous asymptotic security proofs (see, e.g., Refs. [16–18,20]), our work is the first one to allow for a composable analysis of parameter estimation for a CV-QKD protocol with discrete modulation.

A. Parameter estimation: Confidence intervals

The second modification arises because the parameters v, c, and $P_0(R)$, which enter the semidefinite programs, need to be estimated from experimental data. In the nonasymptotic regime, these estimates are subject to statistical errors due to finite-size fluctuations. To account for this, we need to compute confidence intervals for these quantities for any finite n. It is sufficient to consider one-sided confidence intervals, as the parameters enter the semidefinite programs in constraints expressed through inequalities. Following the approach of Ref. [24], we assume that parameter estimation is performed after

error correction. This allows Alice and Bob to use all their raw keys for both parameter estimation and key extraction.

First, consider the variance parameter v. Given n signal transmissions, Bob obtains from his measurements a string of quadrature and phase values, $q_1^B, q_2^B, \ldots, q_n^B$ and $p_1^B, p_2^B, \ldots, p_n^B$. His best estimate for v is

$$\hat{v} = \frac{1}{n}\sum_{i=1}^{n} \frac{(q_i^B)^2 + (p_i^B)^2}{2}. \tag{50}$$

In the scenario of collective attacks, this is the sum of n independent identically distributed (IID) variables, with each variable taking values in the interval $[0, R^2]$. We can then obtain a confidence interval for v using the additive Chernoff bound. For any $\delta_v > 0$,

$$\Pr\left\{\hat{v} < v - \delta_v\right\} \leq \exp\left[-nD\left(\frac{v-\delta_v}{R^2}\,\middle\|\,\frac{v}{R^2}\right)\right], \tag{51}$$

where $D(a\|b) = a\ln(a/b) + (1-a)\ln(1-a/1-b)$ is the relative entropy. Note that, for $p < 1/2$, we have

$$D(p-\epsilon\|p) > \frac{\epsilon^2}{2p(1-p)}, \tag{52}$$

which yields

$$\Pr\left\{\hat{v} < v - \delta_v\right\} \leq \exp\left[-\frac{n\delta_v^2}{2R^2 v(1-v/R^2)}\right] \tag{53}$$

$$\leq \exp\left(-\frac{n\delta_v^2}{2R^2 v}\right) =: \epsilon_v. \tag{54}$$

To obtain a confidence interval for the covariance parameter c, we apply the Hoeffding bound. Let us denote as $q_1^A, q_2^A, \ldots, q_n^A$ and $p_1^A, p_2^A, \ldots, p_n^A$ the raw data collected by Alice. The best estimate for c is

$$\hat{c} = \frac{1}{n}\sum_{i=1}^{n} \frac{q_i^A q_i^B + p_i^A p_i^B}{2}. \tag{55}$$

This quantity is the sum of n IID variables, with each variable chosen from the interval $[-AR, AR]$, where $A = \max_x\{|\mathrm{Re}(\alpha_x)| + |\mathrm{Im}(\alpha_x)|\}/\sqrt{2}$. The Hoeffding tail bound then yields

$$\Pr\left\{\hat{c} > c + \delta_c\right\} \leq \exp\left(-\frac{2n\delta_c^2}{A^2R^2}\right) =: \epsilon_c. \tag{56}$$

Finally, consider the estimation of $P_0(R)$. This parameter is estimated by counting the number of times that a measurement output falls outside of the allowed range $\mathcal{R}(R)$. Bob can locally estimate this with the help of the auxiliary variables S_i, where $S_i = 0$ if the ith signal falls inside the range and $S_i = 1$ otherwise. Therefore, Bob's best estimate for $P_0(R)$ is

$$\hat{P}_0(R) = \frac{1}{n}\sum_{i=1}^{n} S_i. \tag{57}$$

This is the average of independent Bernoulli trials and therefore follows the Binomial distribution. A confidence interval can be obtained from the additive Chernoff bound:

$$\Pr\left\{\hat{P}_0(R) < P_0(R) - \delta_P\right\} \leq \exp\left\{-nD[P_0(R) - \delta_P\|P_0(R)]\right\}. \tag{58}$$

Applying the bound in Eq. (52), we obtain

$$\Pr\left\{\hat{P}_0(R) < P_0(R) - \delta_P\right\} \leq \exp\left\{-\frac{n\delta_P^2}{2P_0(R)[1-P_0(R)]}\right\} \tag{59}$$

$$\leq \exp\left[-\frac{n\delta_P^2}{2P_0(R)}\right] =: \epsilon_P. \tag{60}$$

We require that the probabilities ϵ_v, ϵ_c, and ϵ_P are much smaller than 1, of the order of 10^{-10}.

In summary, we obtain that the bounds

$$\hat{v} \geq v - \delta_v, \tag{61}$$

$$\hat{c} \leq c + \delta_c, \tag{62}$$

$$\hat{P}_0(R) \geq P_0(R) - \delta_P, \tag{63}$$

hold true with almost unit probability (larger than $1 - \epsilon_{\mathrm{PE}}$, where $\epsilon_{\mathrm{PE}} = \epsilon_v + \epsilon_c + \epsilon_P$ follows from an application of the union bound). For simplicity, we put $\epsilon_v = \epsilon_c = \epsilon_P = \epsilon_{\mathrm{PE}}/3$. By inverting Eq. (56), we obtain

$$\delta_c = AR\sqrt{\frac{\ln(3/\epsilon_{\mathrm{PE}})}{2n}}. \tag{64}$$

From Eqs. (54) and (60), we obtain the following conditions for δ_v and δ_P:

$$\delta_v = R\sqrt{\frac{2v\ln(3/\epsilon_{\mathrm{PE}})}{n}}, \tag{65}$$

$$\delta_P = \sqrt{\frac{2P_0(R)\ln(3/\epsilon_{\mathrm{PE}})}{n}}. \tag{66}$$

To estimate these quantities, we apply the inequalities given in Eqs. (61) and (63):

$$\delta_v \leq R\sqrt{\frac{2(\hat{v}+\delta_v)\ln(3/\epsilon_{\rm PE})}{n}}, \tag{67}$$

$$\delta_P \leq \sqrt{\frac{2(\hat{P}_0(R)+\delta_P)\ln(3/\epsilon_{\rm PE})}{n}}. \tag{68}$$

Finally, solving for δ_v and δ_P, we obtain

$$\delta_v \leq R\sqrt{\frac{2\hat{v}\ln(3/\epsilon_{\rm PE})}{n}+\left[\frac{R\ln(3/\epsilon_{\rm PE})}{n}\right]^2} + \frac{R^2\ln(3/\epsilon_{\rm PE})}{n}, \tag{69}$$

$$\delta_P \leq \sqrt{\frac{2\hat{P}_0(R)\ln(3/\epsilon_{\rm PE})}{n}+\left[\frac{\ln(3/\epsilon_{\rm PE})}{n}\right]^2} + \frac{\ln(3/\epsilon_{\rm PE})}{n}. \tag{70}$$

In conclusion, the nonasymptotic secret key rates are obtained using the formula in Eq. (48), where the parameters $\gamma_B(\tau)$ and $\gamma_{AB}(\tau)$ are obtained by solving the semidefinite programs given in Eqs. (40) and (47), with the replacements

$$v \to \hat{v}+\delta_v, \tag{71}$$

$$c \to \hat{c}-\delta_c, \tag{72}$$

$$P_0(R) \to \hat{P}_0(R)+\delta_P, \tag{73}$$

and δ_v, δ_c, and δ_P bounded as in Eqs. (64), (69), and (70). The key rate obtained in this way is secure up to probability not larger than $\epsilon' = \epsilon_{\rm s}+\epsilon_h+\epsilon_{\rm PE}$.

X. QPSK: SECRET KEY RATES

Our theoretical analysis applies to any DM protocol. As a concrete example, we describe the application of our theory to QPSK encoding, where $\alpha_x = \alpha i^x$ and $\mathcal{P}_x = 1/4$, for $x = 0,1,2,3$. To align with the symmetry of our model of realistic heterodyne detection, we set $\alpha = |\alpha|e^{i\pi/4}$.

We have

$$\alpha_x = |\alpha|e^{i\pi/4}i^x = |\alpha|\frac{\pm 1 \pm i}{\sqrt{2}}. \tag{74}$$

From this, we obtain

$$A = \frac{1}{\sqrt{2}}\max_x\{|{\rm Re}(\alpha_x)|+|{\rm Im}(\alpha_x)|\} = |\alpha|, \tag{75}$$

and

$$\|\mathcal{C}\|_\infty \leq \frac{1}{2}\sup_{x,j,k}\left|\bar{\alpha}_x\beta_{jk}+\alpha_x\bar{\beta}_{jk}\right| \leq |\alpha|R. \tag{76}$$

For the sake of presentation, we assume a Gaussian channel from Alice to Bob, characterized by the loss factor $\eta \in [0,1]$ and the excess noise variance $u \geq 0$. Given that a and $a^\dagger$ are the canonical annihilation and creation operators on Alice's input mode, and b and $b^\dagger$ on Bob's output mode, a Gaussian channel (in the Heisenberg picture) is a map of the form

$$b \to \sqrt{\eta}a+\sqrt{1-\eta}e+w, \tag{77}$$

$$b^\dagger \to \sqrt{\eta}a^\dagger+\sqrt{1-\eta}e^\dagger+\bar{w}, \tag{78}$$

where e and $e^\dagger$ are the canonical operators associated with an auxiliary vacuum mode and w is a Gaussian random variable with zero mean and variance u. Assuming this form for the channel from Alice to Bob, we can explicitly compute the expected asymptotic values of the constraint parameters v, c, and $P_0(R)$ and then solve the semidefinite programs to estimate the CM elements $\gamma_B(\tau)$ and $\gamma_{AB}(\tau)$ (more details on this are discussed in Appendix E).

The computed secret key rates (measured in bits per channel use, i.e., per mode) are shown in Figs. 1–2 versus the loss η, expressed in decibels. The other parameters of the protocol are fixed as $|\alpha| = 0.5$ and $u = 0.001$.

Figure 1(top) is obtained by solving the semidefinite programs given in Eqs. (31) and (33), which are defined in an infinite-dimensional Hilbert space. To find a solution, we truncate the Hilbert space. The figure shows that, as expected, by increasing R, and for d large enough, the secret key rate converges toward the value expected for ideal heterodyne detection (which has recently been computed in Ref. [16]). Our theory allows us to rigorously compute the deviation from this ideal rate.

Figure 1(bottom) is obtained by solving the semidefinite programs given in Eqs. (40) and (47), which are defined in a finite-dimensional Hilbert space. In this case, a solution can be found without arbitrary truncation of the Hilbert space. Compared with Fig. 1(top), we note that the secret key rate is reduced, especially if the value of R is not large enough. This is due to the term proportional to $\|\mathcal{C}\|_\infty$ introduced in constraints of the semidefinite programs to account for the projections into the finite-dimensional space (therefore, an improved key rate can be obtained with a better bound for $\|\mathcal{C}\|_\infty$). However, already for $R = 7$, the difference with the solution of the infinite-dimensional problem is relatively small.

Figure 2 is obtained by solving finite-dimensional semidefinite programs and including the finite-size corrections in the constraints, as discussed in Sec. IX. For the sake of illustration, the calculations are done by putting the best estimates of the parameters equal to the expected values, i.e., the semidefinite programs given in Eqs. (40) and (47) are solved with the replacements

$$v \to v+\delta_v, \tag{79}$$

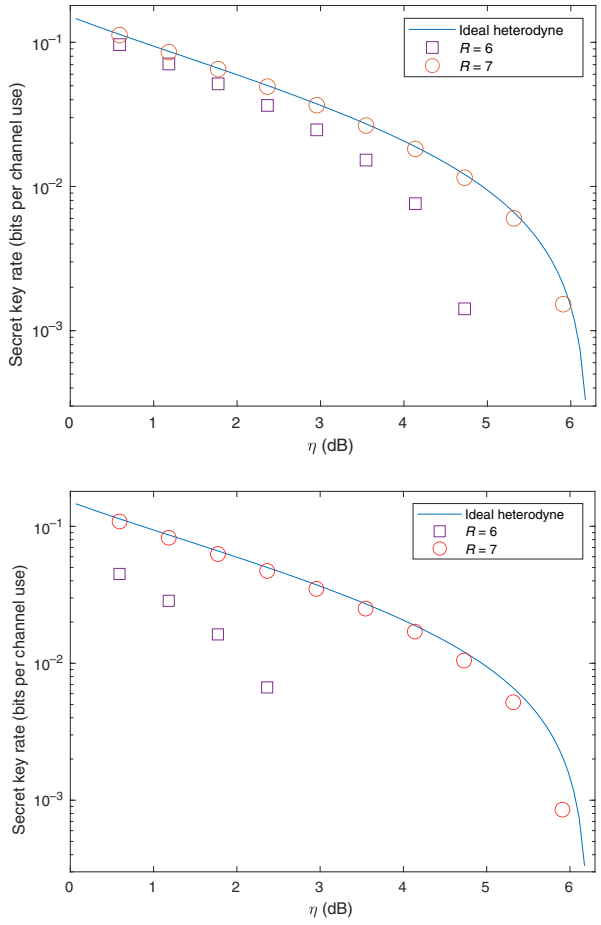

FIG. 1. The asymptotic secret key rates versus the channel loss for QPSK encoding, for collective attacks in the limit of $n \to \infty$. The channel parameters are $|\alpha| = 0.5$, $u = 0.001$, and $\xi = 0.97$. The solid lines show the theoretical rate expected for ideal heterodyne detection, from Ref. [16]. For nonideal heterodyne, the key rate is computed for $d = 16$ and $R = 6$ (squares) and $R = 7$ (circles). Top: the key rate is obtained by truncating and solving the *infinite-dimensional* semidefinite programs given in Eqs. (31) and (33). Bottom: the key rate is obtained by solving the *finite-dimensional* semidefinite programs given in Eqs. (40) and (47).

$$c \to c - \delta_c, \tag{80}$$

$$P_0(R) \to P_0(R) + \delta_P. \tag{81}$$

The error parameters are $\epsilon_h = \epsilon_s = \epsilon_{PE} = 10^{-10}$. The figure shows that a nonzero secret key rate is obtained when the block size is about $n = 10^{10}$ or larger. The dominant finite-size corrections are due to δ_v and δ_c. This means that an improved key rate could be obtained by using tighter confidence intervals for the estimation of these parameters. This, in turn, would allow us to reduce the block-size without compromising composable security.

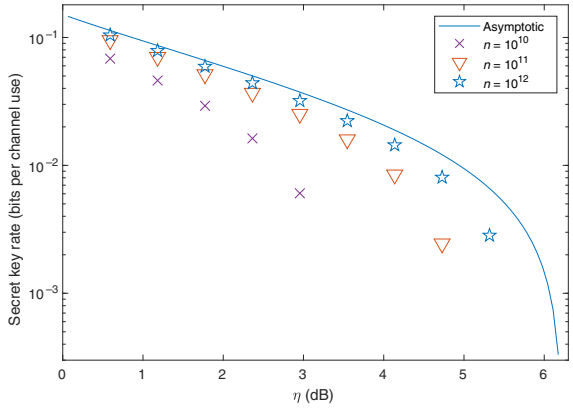

FIG. 2. The composable secret key rates versus the channel loss for QPSK encoding, for collective attacks in the regime of finite n. The channel parameters are $|\alpha| = 0.5$, $u = 0.001$, and $\xi = 0.97$. The solid line is the theoretical rate expected in the asymptotic limit of $n \to \infty$ and for ideal heterodyne detection, from Ref. [16]. For nonideal heterodyne, the expected rate is computed from the *finite-dimensional* semidefinite programs and by taking into account finite-size corrections as described in Sec. IX. For $d = 16$ and $R = 7$, the plot shows the results for $n = 10^{10}$ (crosses), $n = 10^{11}$ (triangles), and $n = 10^{12}$ (stars). The error parameters are $\epsilon_h = \epsilon_s = \epsilon_{PE} = 10^{-10}$.

XI. CONCLUSIONS

In CV QKD, information is decoded by a coherent measurement of the quantum electromagnetic field, i.e., homodyne or heterodyne. These are mature technologies and they represent the strategic advantage of CV QKD over discrete-variable architectures. This applies to both continuous [3,4,13,24] and discrete modulation protocols [5,16–18,20,30,31]. Ideal homodyne and heterodyne detection, which are measurements of the quadratures of the field, possess a continuous symmetry that plays a central role in our theoretical understanding of CV QKD. However, this symmetry is broken in real homodyne and heterodyne detection that are implemented in actual experiments [14,15]. While it is expected that, in practice, these measurements will be well approximated by their idealized models in some regimes, a quantitative assessment of the error introduced by this approximation, and of its impact on the secret key rate, has so far been elusive. Here, we fill this gap and present a theory to quantify the security of CV QKD with real imperfect heterodyne detection. Within this theory, we establish the composable security of DM CV QKD in the nonasymptotic regime. To the best of our knowledge, this is the first result obtained in this direction, as previous works have only considered asymptotic noncomposable security [16–18,20]. Extension to most general attacks, which in principle can be obtained through a de Finetti reduction, remains an open problem.

In this paper, we extend the approach of Ref. [17], in which one first estimates the covariance matrix of the

quadratures, and then obtain a bound on the key rate using the property of extremality of Gaussian states. However, our theory can also be applied to the method of Refs. [18,20], in which one uses the measured data to bound the key rate directly through nonlinear semidefinite programming. We focus on a particular kind of nonideality in detection but our approach can be applied to other nonidealities in both detection and state preparation. Examples of these nonidealities include nonlinearities in the analog-to-digital converter [32] and noise in the state preparation [16]. In principle, accounting for experimental imperfections in the security analysis mitigates the threat from side-channel attacks. Our approach may also be extended to measurement-device-independent QKD [29,33,34], which protects against unknown side-channel attacks on the detectors. The results presented here are not only conceptually important but also enable secure, practical, and reliable DM CV QKD. In fact, to obtain reliable bounds on the secret key rates, the practitioner of CV QKD needs to carefully assess, in a composable way, finite-size effects as well as the impact of nonidealities in the measurement devices, including but not limited to, the effects of finite range and precision considered in this work.

ACKNOWLEDGMENTS

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) Quantum Communications Hub, Grant No. EP/T001011/1. Y.O. is supported in part by National University of Singapore (NUS) startup Grants No. R-263-000-E32-133 and No. R-263-000-E32-731, and the National Research Foundation, Prime Minister's Office, Singapore and the Ministry of Education, Singapore under the Research Centres of Excellence program.

APPENDIX A: HOLEVO INFORMATION

Consider a two-mode state ρ_{AB} shared between Alice and Bob. We denote by a and $a^\dagger$, and b and $b^\dagger$, the annihilation and creation operators on Alice's and Bob's mode, respectively. Their local quadrature and phase operators are $q_A = (a + a^\dagger)/\sqrt{2}$, $p_A = (a - a^\dagger)/(i\sqrt{2})$, $q_B = (b + b^\dagger)/\sqrt{2}, p_B = (b - b^\dagger)/(i\sqrt{2})$. The symmetrically ordered CM $\gamma'(\rho)$ of the two-mode state ρ is defined as

$$\mathrm{Tr}\left[\rho\begin{pmatrix} q_A^2 & \Sigma(q_A,p_A) & q_Aq_B & q_Ap_B \\ \Sigma(q_A,p_A) & p_A^2 & p_Aq_B & p_Ap_B \\ q_Bq_A & q_Bp_A & q_B^2 & \Sigma(q_B,p_B) \\ p_Bq_A & p_Bp_A & \Sigma(q_B,p_B) & p_B^2 \end{pmatrix}\right], \tag{A1}$$

where $\Sigma(x,y) := (xy + yx)/2$. The CM can be written in a block form as

$$\gamma'(\rho) = \begin{pmatrix} A & C \\ C^\intercal & B \end{pmatrix}, \tag{A2}$$

where A, B, and C are 2×2 matrices. We denote as ν_+ and ν_- the symplectic eigenvalues of $\gamma'(\rho)$. When Bob measures his mode by ideal heterodyne detection, the conditional state of Alice has CM

$$\gamma'(\rho_{A|B}) = A - C(B + 1/2)^{-1}C^\intercal. \tag{A3}$$

We denote ν_0 as the symplectic eigenvalue of $\gamma(\rho_{A|B})$.

The property of extremality of Gaussian states yields the following bound on the Holevo information:

$$\chi(Y;E)_\rho \leq F_\chi[\gamma'(\rho)], \tag{A4}$$

where

$$F_\chi[\gamma'(\rho)] = g(\nu_+ - 1/2) + g(\nu_- - 1/2) - g(\nu_0 - 1/2), \tag{A5}$$

and for any $x > 0$, the function g is defined as

$$g(x) := (x + 1)\log_2(x + 1) - x\log_2 x, \tag{A6}$$

and $g(x) := 0$ if $x = 0$.

It is possible to show [24] that the function F_χ increases if we replace $\gamma'(\rho)$ with the matrix $\gamma(\rho)$:

$$\mathrm{Tr}\left[\rho\begin{pmatrix} \Sigma(q_A^2,p_A^2) & 0 & \Delta & 0 \\ 0 & \Sigma(q_A^2,p_A^2) & 0 & -\Delta \\ \Delta & 0 & \Sigma(q_B^2,p_B^2) & 0 \\ 0 & -\Delta & 0 & \Sigma(q_B^2,p_B^2) \end{pmatrix}\right], \tag{A7}$$

where $\Delta := (q_Aq_B - p_Ap_B)/2$. From this, we obtain the bound

$$\chi(Y;E)_\rho \leq F_\chi[\gamma(\rho)], \tag{A8}$$

Note that

$$\gamma_A(\rho) := \frac{1}{2}\mathrm{Tr}[(a^\dagger a + aa^\dagger)\rho] = \mathrm{Tr}[\rho\Sigma(q_A^2,p_A^2)], \tag{A9}$$

$$\gamma_B(\rho) := \frac{1}{2}\mathrm{Tr}[(b^\dagger b + bb^\dagger)\rho] = \mathrm{Tr}[\rho\Sigma(q_B^2,p_B^2)], \tag{A10}$$

$$\gamma_{AB}(\rho) := \frac{1}{2}\mathrm{Tr}[(a^\dagger b^\dagger + ab)\rho] = \mathrm{Tr}[\rho\Delta]. \tag{A11}$$

Obviously, $F_\chi[\gamma(\rho)]$ is a function of $\gamma_A(\rho)$, $\gamma_B(\rho)$, and $\gamma_{AB}(\rho)$. We therefore define

$$f_\chi[\gamma_A(\rho),\gamma_B(\rho),\gamma_{AB}(\rho)] := F_\chi[\gamma(\rho)]. \tag{A12}$$

APPENDIX B: QPSK: EB REPRESENTATION

In the PM representation, Alice prepares the state $|\alpha_x\rangle$ with probability $\mathcal{P}_x = 1/4$, for $\alpha_x = \alpha e^{ix\pi/2}$ and $x = 0, 1, 2, 3$, where we put $\alpha = |\alpha| e^{i\pi/4}$.

The average state prepared by Alice is

$$\rho_{A'} = \frac{1}{4} \sum_x |\alpha_x\rangle\langle\alpha_x|. \tag{B1}$$

We can expand this state in the number basis. Its (n, n') entry is

$$\rho_{A'}^{nn'} = \frac{e^{-|\alpha|^2}}{4} \sum_x \frac{\alpha_x^n \bar{\alpha}_x^{n'}}{\sqrt{n!n'!}} \tag{B2}$$

$$= \frac{e^{-|\alpha|^2}}{4} \frac{\alpha^n \bar{\alpha}^{n'}}{\sqrt{n!n'!}} \sum_x e^{i(n-n')x\pi/2} \tag{B3}$$

$$= \frac{e^{-|\alpha|^2}}{4} \frac{\alpha^n \bar{\alpha}^{n'}}{\sqrt{n!n'!}} \left(1 + e^{(n-n')\pi/2}\right) \left(1 + e^{(n-n')\pi}\right). \tag{B4}$$

That is, $\rho_{A'}^{nn'} = 0$ unless $n - n'$ is a multiple of 4, in which case,

$$\rho_{A'}^{nn'} = e^{-|\alpha|^2} \frac{\alpha^n \bar{\alpha}^{n'}}{\sqrt{n!n'!}}. \tag{B5}$$

As this state is invariant under rotation of $\pi/2$ in phase space, the eigenvectors have the form, for $y = 0, 1, 2, 3$,

$$|\phi_y\rangle = \sum_{n\geq 0} c_{y,n} |y + 4n\rangle. \tag{B6}$$

From

$$\frac{1}{4} \sum_x |\alpha_x\rangle\langle\alpha_x| = \sum_y \lambda_y |\phi_y\rangle\langle\phi_y|, \tag{B7}$$

we obtain

$$\sqrt{\lambda_y}\, c_{y,n} = e^{-|\alpha|^2/2} \frac{\alpha^{y+4n}}{\sqrt{(y+4n)!}}. \tag{B8}$$

By imposing normalization, we find

$$|\phi_y\rangle = \frac{e^{-|\alpha|^2/2}}{\sqrt{\lambda_y}} \sum_{n\geq 0} \frac{\alpha^{y+4n}}{\sqrt{(y+4n)!}} |y + 4n\rangle, \tag{B9}$$

where

$$\lambda_y = e^{-|\alpha|^2} \sum_{n\geq 0} \frac{|\alpha|^{2(y+4n)}}{(y+4n)!}. \tag{B10}$$

Explicitly,

$$\lambda_0 = \frac{e^{-|\alpha|^2}}{2} \left(\cosh\alpha^2 + \cos\alpha^2\right), \tag{B11}$$

$$\lambda_1 = \frac{e^{-|\alpha|^2}}{2} \left(\sinh\alpha^2 + \sin\alpha^2\right), \tag{B12}$$

$$\lambda_2 = \frac{e^{-|\alpha|^2}}{2} \left(\cosh\alpha^2 - \cos\alpha^2\right), \tag{B13}$$

$$\lambda_3 = \frac{e^{-|\alpha|^2}}{2} \left(\sinh\alpha^2 - \sin\alpha^2\right). \tag{B14}$$

We define the purification of the state $\rho_{A'}$ through its Schmidt decomposition,

$$|\Psi\rangle_{AA'} = \sum_y \sqrt{\lambda_y} |\bar{\phi}_y\rangle |\phi_y\rangle, \tag{B15}$$

where

$$|\bar{\phi}_y\rangle = \frac{e^{-|\alpha|^2/2}}{\sqrt{\lambda_y}} \sum_{n\geq 0} \frac{\bar{\alpha}^{y+4n}}{\sqrt{(y+4n)!}} |y + 4n\rangle. \tag{B16}$$

It is easy to check that

$$|\alpha_x\rangle = \sum_y e^{ixy\pi/2} \sqrt{\lambda_y} |\phi_y\rangle, \tag{B17}$$

which we can invert to obtain

$$\sqrt{\lambda_y} |\phi_y\rangle = \sum_x \frac{e^{-ixy\pi/2}}{4} |\alpha_x\rangle. \tag{B18}$$

We can then write

$$|\Psi\rangle_{AA'} = \sum_y \sqrt{\lambda_y} |\bar{\phi}_y\rangle |\phi_y\rangle \tag{B19}$$

$$= \sum_{xy} \frac{e^{-ixy\pi/2}}{4} |\bar{\phi}_y\rangle |\alpha_x\rangle \tag{B20}$$

$$= \frac{1}{2} \sum_x |\psi_x\rangle |\alpha_x\rangle, \tag{B21}$$

where we define

$$|\psi_x\rangle = \frac{1}{2} \sum_y e^{-ixy\pi/2} |\bar{\phi}_y\rangle. \tag{B22}$$

APPENDIX C: OPERATORS IN THE NUMBER REPRESENTATION

We now express the operators that appear in our semidefinite programs in the basis $\{|\psi_x\rangle \otimes |n\rangle\}_{x=0,\ldots,3;n=0,\ldots,\infty}$, where $|n\rangle$'s are the number states of Bob's side, satisfying $b^\dagger b|n\rangle = n|n\rangle$.

The operator ρ_B is a density matrix of one bosonic mode. We can express it in the number basis, $\{|n\rangle\}_{n=0,\ldots,\infty}$, as

$$\rho_B = \sum_{nn'=0}^{\infty} \rho_{nn'} |n\rangle\langle n'|. \tag{C1}$$

Similarly, ρ_{AB} reads

$$\rho_{AB} = \sum_{xx'=0}^{3} \sum_{nn'=0}^{\infty} \rho_{xx'nn'} |\psi_x\rangle\langle\psi_{x'}| \otimes |n\rangle\langle n'|. \tag{C2}$$

The operator Π projects into the subspace with at most $N = \lfloor 2R^2 \rfloor$ photons, i.e.,

$$\Pi = \sum_{n=0}^{N} |n\rangle\langle n|. \tag{C3}$$

Therefore,

$$\frac{1}{2}\Pi(b^\dagger b + bb^\dagger)\Pi = \sum_{n=1}^{N} \left(n + \frac{1}{2}\right) |n\rangle\langle n|. \tag{C4}$$

The operator $\mathcal{V}$ is

$$\mathcal{V} = \sum_{jk} |\beta_{jk}|^2 \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta| = \sum_{nn'=0}^{\infty} \mathcal{V}_{nn'} |n\rangle\langle n'|, \tag{C5}$$

where

$$\mathcal{V}_{nn'} = \sum_{jk} |\beta_{jk}|^2 \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} e^{-|\beta|^2} \frac{\beta^n \bar{\beta}^{n'}}{\sqrt{n!n'!}}. \tag{C6}$$

Note that, by symmetry, $\mathcal{V}_{nn'} = 0$ unless $n - n'$ is multiple of 4. Also by symmetry, $\mathcal{V}$ is a real matrix in the Fock basis.

Similarly, we have

$$\mathcal{U} = \int_{\beta\in\mathcal{R}(R)} \frac{d^2\beta}{\pi} |\beta\rangle\langle\beta| = \sum_{n,n'=0}^{\infty} \mathcal{U}_{nn'} |n\rangle\langle n'|, \tag{C7}$$

with

$$\mathcal{U}_{nn'} = \int_{\beta\in\mathcal{R}(R)} \frac{d^2\beta}{\pi} e^{-|\beta|^2} \frac{\beta^n \bar{\beta}^{n'}}{\sqrt{n!n'!}}. \tag{C8}$$

The covariance operator in the objective function reads

$$\begin{aligned}
&\frac{1}{2}(a\Pi b\Pi + a^\dagger \Pi b^\dagger \Pi) \\
&\quad = \frac{1}{2} \sum_{xx'=0}^{3} \sum_{n=1}^{N} \sqrt{n} \langle\psi_x|a|\psi_{x'}\rangle |\psi_x\rangle\langle\psi_{x'}| \otimes |n-1\rangle\langle n| \\
&\quad + \sqrt{n} \langle\psi_x|a^\dagger|\psi_{x'}\rangle |\psi_x\rangle\langle\psi_{x'}| \otimes |n\rangle\langle n-1|, \qquad \text{(C9)} \\
&\quad = \frac{1}{2} \sum_{xx'=0}^{3} \sum_{n=1}^{N} \sqrt{n} \langle\psi_x|a|\psi_{x'}\rangle |\psi_x\rangle\langle\psi_{x'}| \otimes |n-1\rangle\langle n| \\
&\quad + \sqrt{n} \langle\psi_{x'}|a|\psi_x\rangle^* |\psi_x\rangle\langle\psi_{x'}| \otimes |n\rangle\langle n-1|. \qquad \text{(C10)}
\end{aligned}$$

To compute this, first note that

$$\langle\bar{\phi}_{y-1}|a|\bar{\phi}_y\rangle = \bar{\alpha}\sqrt{\frac{\lambda_{y-1}}{\lambda_y}}, \tag{C11}$$

from which we obtain

$$\begin{aligned}
\langle\psi_x|a|\psi_{x'}\rangle &= \frac{1}{4} \sum_{yy'=0}^{3} e^{iyx\pi/2} e^{-iy'x'\pi/2} \langle\bar{\phi}_y|a|\bar{\phi}_{y'}\rangle & \text{(C12)} \\
&= \frac{1}{4} \sum_{y=0}^{3} e^{i(y-1)x\pi/2} e^{-iyx'\pi/2} \langle\bar{\phi}_{y-1}|a|\bar{\phi}_y\rangle & \text{(C13)} \\
&= \bar{\alpha}\, \frac{1}{4} \sum_{y=0}^{3} e^{i(y-1)x\pi/2} e^{-iyx'\pi/2} \sqrt{\frac{\lambda_{y-1}}{\lambda_y}} & \text{(C14)} \\
&= \bar{\alpha}_x\, \frac{1}{4} \sum_{y=0}^{3} e^{iy(x-x')\pi/2} \sqrt{\frac{\lambda_{y-1}}{\lambda_y}}. & \text{(C15)}
\end{aligned}$$

Finally, the operator $\mathcal{C}$ has components

$$\begin{aligned}
\mathcal{C}_{xx'nn'} &= \frac{1}{2}\, \delta_{xx'} \bar{\alpha}_x \sum_{j,k=1}^{d} \beta_{jk} \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} e^{-|\beta|^2} \frac{\beta^n \bar{\beta}^{n'}}{\sqrt{n!n'!}} \\
&\quad + \frac{1}{2}\, \delta_{xx'} \alpha_x \sum_{j,k=1}^{d} \bar{\beta}_{jk} \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} e^{-|\beta|^2} \frac{\beta^n \bar{\beta}^{n'}}{\sqrt{n!n'!}}.
\end{aligned} \tag{C16}$$

The operator can thus be written as

$$\mathcal{C} = \frac{1}{2}\left(\mathcal{A}^\dagger \otimes \mathcal{B} + \mathcal{A} \otimes \mathcal{B}^\dagger\right), \tag{C17}$$

where

$$\mathcal{A} = \sum_{x=0}^{3} \alpha_x |\psi_x\rangle\langle\psi_x|, \tag{C18}$$

$$\mathcal{B} = \sum_{nn'} \sum_{j,k=1}^{d} \beta_{jk} \int_{\mathcal{I}_{jk}} \frac{d^2\beta}{\pi} e^{-|\beta|^2} \frac{\beta^n \bar{\beta}^{n'}}{\sqrt{n!n'!}} |n\rangle\langle n'|. \quad \text{(C19)}$$

Note that, by symmetry, $[\mathcal{B}]_{nn'} = 0$ for $n - n'$ even. Also by symmetry, the entries of $\mathcal{C}$ are all real.

APPENDIX D: SEMIDEFINITE PROGRAMMING

In the main text of the paper, we formulate the following optimization problems:

$$\begin{aligned} &\underset{\rho\geq 0}{\text{maximize}} \frac{1}{2}\langle \Pi(b^\dagger b + bb^\dagger)\Pi, \rho\rangle \\ &\text{subject to} \langle \mathcal{V}, \rho\rangle \leq v \\ &\qquad \langle \mathcal{U}, \rho\rangle \geq 1 - P_0(R) \\ &\qquad \langle I, \rho\rangle = 1. \end{aligned} \quad \text{(D1)}$$

and

$$\begin{aligned} &\underset{\rho\geq 0}{\text{minimize}} \frac{1}{2}\langle a\Pi b\Pi + a^\dagger \Pi b^\dagger \Pi, \rho\rangle \\ &\text{subject to} \langle I\otimes \mathcal{V}, \rho\rangle \leq v \\ &\qquad \langle \mathcal{C}, \rho\rangle \geq c \\ &\qquad \langle I\otimes \mathcal{U}, \rho\rangle \geq 1 - P_0(R) \\ &\qquad \mathrm{Tr}_B(\rho) = \sigma \\ &\qquad \langle I, \rho\rangle = 1, \end{aligned} \quad \text{(D2)}$$

where $\langle A, X\rangle = \mathrm{Tr}(A^\dagger X)$ denotes the Hilbert-Schmidt inner product. To derive the corresponding dual programs, which are more numerically efficient to evaluate, we revisit duality theory for SDP with mixed constraints. Given any semidefinite program of the form

$$\begin{aligned} &\underset{X\geq 0}{\text{minimize}} \langle C, X\rangle \\ &\text{subject to} \langle A_i, X\rangle \leq a_i \\ &\qquad \langle B_j, X\rangle = b_j, \end{aligned} \quad \text{(D3)}$$

where C, A_i, and B_j are Hermitian matrices, the Lagrangian is given by

$$L = \langle C, X\rangle + \sum_i y_i \left(\langle A_i, X\rangle - a_i\right) + \sum_j z_j \left(\langle B_j, X\rangle - b_j\right), \quad \text{(D4)}$$

where $y_i \geq 0, z_i \in \mathbb{R}$. By linearity of inner products, we can rewrite the Lagrangian as

$$L = \langle C + \sum_i y_i A_i + \sum_j z_j B_j, X\rangle - \sum_i y_i a_i - \sum_j z_j b_j. \quad \text{(D5)}$$

The Lagrange dual is then given by

$$\begin{aligned} &\underset{y_i\geq 0, z_j\in\mathbb{R}}{\text{maximize}} -\sum_i y_i a_i - \sum_j z_j b_j \\ &\text{subject to} C + \sum_i y_i A_i + \sum_j z_j B_j \geq 0. \end{aligned} \quad \text{(D6)}$$

The Lagrange dual of Eq. (D1) is thus given by

$$\begin{aligned} &\underset{y_1,y_2\geq 0, z\in\mathbb{R}}{\text{minimize}} y_1 v - y_2[1 - P_0(R)] + z \\ &\qquad -\frac{1}{2}\Pi(b^\dagger b + bb^\dagger)\Pi + y_1\mathcal{V} - y_2\mathcal{U} + zI \geq 0. \end{aligned} \quad \text{(D7)}$$

Strong duality in this case holds because the inequality constraints can be strictly feasible and the Slater constraint qualification holds.

The Lagrange dual of Eq. (D2) can be written as

$$\begin{aligned} &\underset{\substack{y_1,y_2,y_3\geq 0, y_4\in\mathbb{R} \\ z_{h,k}\in\mathbb{R}}}{\text{minimize}} y_1 c - y_2 v + y_3[1 - P_0(R)] - y_4 - \phi(z) \\ &\text{subject to} \frac{1}{2}(a\Pi b\Pi + a^\dagger\Pi b^\dagger\Pi) + \kappa(y,z) \geq 0. \end{aligned} \quad \text{(D8)}$$

where

$$\kappa(y,z) = -y_1\mathcal{C} + y_2\mathcal{V} - y_3\mathcal{U} + y_4 I + \sum_{h,k} z_{h,k} Z_{h,k}, \quad \text{(D9)}$$

$$\phi(z) = \sum_{h\geq k} z_{h,k}\mathrm{Re}(\sigma_{h,k}) + \sum_{h<k} z_{h,k}\mathrm{Im}(\sigma_{h,k}), \quad \text{(D10)}$$

and $Z_{h,k} = E_{h,k}\otimes I_B$ when $h \geq k$ and $Z_{h,k} = F_{k,h}\otimes I_B$ when $h < k$, with

$$E_{h,k} = \frac{|k\rangle\langle h| + |h\rangle\langle k|}{2}, \quad \text{(D11)}$$

$$F_{h,k} = i\,\frac{|k\rangle\langle h| - |h\rangle\langle k|}{2}. \quad \text{(D12)}$$

To solve these optimization problems numerically, we need to impose a cutoff to Bob's Hilbert space, and work within a finite-dimensional space of dimensions dim, containing no more than (dim − 1) photons on Bob's side. The value of dim can be arbitrarily large, as long as it is larger than $N + 1$, where $N = \lfloor 2R^2 \rfloor$ is determined by the rank of the projector Π. However, our numerical results suggest that it is sufficient to put dim $= N + 1$. As an example, Fig. 3 shows the optimal values for QPSK encoding and for the optimization problems given in Eqs. (D7) and (D8), as a function of dim.

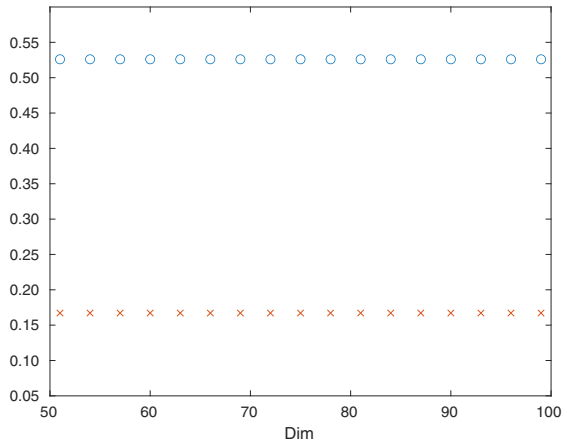

FIG. 3. The optimal values plotted versus the Hilbert space cutoff dim, for Eq. (D7) (circles) and Eq. (D8) (crosses), and for $R = 7$, $d = 16$, $\alpha = 0.5$, $\eta = 0.1$, and $u = 0.001$. The optimal values are largely independent of dim as long as dim $\geq \lfloor R^2 \rfloor + 1$.

APPENDIX E: QPSK: SECRET KEY RATES

As a concrete example, we apply our theory to QPSK encoding, where $\alpha_x = \alpha i^x$ and $\mathcal{P}_x = 1/4$, for $x = 0, 1, 2, 3$. To align with the symmetry of our model of realistic heterodyne detection, we set $\alpha = |\alpha| e^{i\pi/4}$. We simulate a Gaussian channel from Alice to Bob, characterized by the loss factor $\eta \in [0, 1]$ and the excess noise variance $u \geq 0$.

First, we compute the expected value for the mutual information,

$$I(X;Y) = H(Y) - H(Y|X), \tag{E1}$$

where $H(Y)$ is the entropy of Bob's measurement outcome and $H(Y|X)$ is the conditional entropy for a given input state prepared by Alice. If Alice prepares the coherent state $|\alpha_x\rangle$, with $\alpha_x = (q_x + ip_x)/\sqrt{2}$, then the state $\rho_B(x)$ received by Bob is described by the Wigner function $W_x(q,p)$, where

$$W_x(q,p) = \frac{1}{\pi(2u+1)}\, e^{-\frac{(q-\sqrt{\eta}\,q_x)^2 + (p-\sqrt{\eta}\,p_x)^2}{2(u+1/2)}}. \tag{E2}$$

From this, we obtain the probability density of measuring $\beta = (q + ip)/\sqrt{2}$ by ideal heterodyne detection,

$$\frac{1}{\pi}\langle\beta|\rho_B(x)|\beta\rangle = \frac{1}{2\pi(u+1)}\, e^{-\frac{(q-\sqrt{\eta}\,q_x)^2 + (p-\sqrt{\eta}\,p_x)^2}{2(u+1)}}, \tag{E3}$$

and, in turn, the probability of measuring $\beta \in \mathcal{I}_{jk}$,

$$P_{jk|x} = \frac{1}{\pi}\int_{\beta\in\mathcal{I}_{jk}} d^2\beta \langle\beta|\rho_B(x)|\beta\rangle = P_{j|x}\, P_{k|x}, \tag{E4}$$

where

$$P_{j|x} = \frac{1}{2}\mathrm{erf}\left[\frac{(2+d-2j)R + d\sqrt{\eta}\,q_x}{d\sqrt{2(u+1)}}\right] - \frac{1}{2}\mathrm{erf}\left[\frac{(d-2j)R + d\sqrt{\eta}\,q_x}{d\sqrt{2(u+1)}}\right]. \tag{E5}$$

For QPSK encoding, the conditional mutual information then reads (log in base 2)

$$H(Y|X) = -\frac{1}{4}\sum_{x=0}^{3}\sum_{j,k=1}^{d} P_{jk|x}\log P_{jk|x}. \tag{E6}$$

The probability distribution of Y is obtained by averaging over X, $P_{jk} = 1/4\sum_{x=0}^{3} P_{jk|x}$ and the entropy of Y is

$$H(Y) = -\sum_{j,k=1}^{d} P_{jk}\log P_{jk}. \tag{E7}$$

Similarly, we compute the expected values for the estimated parameters v and c. We obtain

$$\mathrm{Tr}(\mathcal{C}\rho_{AB}) = \frac{1}{4}\sum_{x=0}^{3}\sum_{j,k=1}^{d}\frac{q_x q_j + p_x p_k}{2} P_{jk|x} \tag{E8}$$

$$\mathrm{Tr}(\mathcal{V}\rho_B) = \sum_{j,k=1}^{d}\frac{q_j^2 + p_k^2}{2} P_{jk}. \tag{E9}$$

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proc. IEEE Int. Conf. Comput., Syst. Signal Process., Bangalore, India, 10–12 December, 1984; 175, p. 8.
[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).
[3] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).
[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. Leverrier and P. Grangier, Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, Phys. Rev. A **83**, 042312 (2011).
[6] 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).

[7] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Finite-size security of continuous-variable quantum key distribution with digital signal processing, Nat. Commun. **12**, 252 (2021).

[8] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Napoli, 2005).

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

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

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

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

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

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

[15] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. Solar Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, Practical continuous-variable quantum key distribution with composable security (2021), ArXiv:2110.09262.

[16] A. Denys, P. Brown, and A. Leverrier, Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation, Quantum **5**, 540 (2021).

[17] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X **9**, 021059 (2019).

[18] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution, Phys. Rev. X **9**, 041064 (2019).

[19] R. Canetti, Universally composable security: A new paradigm for cryptographic protocols, Proceedings 42nd IEEE Symposium on Foundations of Computer Science, pages 136-145 (2001).

[20] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols, PRX Quantum **2**, 020325 (2021).

[21] M. Christandl, R. König, and R. Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

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

[23] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. Lond. A **461**, 207 (2005).

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

[25] A. Winter, Coding theorem and strong converse for quantum channels, IEEE Trans. Inf. Theory **45**, 2481 (1999).

[26] M. E. Shirokov, Tight uniform continuity bounds for the quantum conditional mutual information, for the Holevo quantity, and for capacities of quantum channels, J. Math. Phys. **58**, 102202 (2017).

[27] M. Tomamichel, C. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[28] M. Tomamichel, A Framework for Non-Asymptotic Quantum Information Theory, Ph.D. thesis, Department of Physics, Swiss Federal Institute of Technology (ETH) Zurich, 2012 (2012), ArXiv:1203.2142.

[29] 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).

[30] C. Lupo, Towards practical security of continuous-variable quantum key distribution, Phys. Rev. A **102**, 022623 (2020).

[31] E. Kaur, S. Guha, and M. M. Wilde, Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution, Phys. Rev. A **103**, 012412 (2021).

[32] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information, Nat. Commun. **12**, 605 (2021).

[33] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[34] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).