Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks

Panagiotis Papanastasiou and Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, United Kingdom

We consider continuous-variable quantum key distribution with discrete-alphabet encodings. In particular, we study protocols where information is encoded in the phase of displaced coherent (or thermal) states, even though the results can be directly extended to any protocol based on finite constellations of displaced Gaussian states. In this setting, we provide a composable security analysis in the finite-size regime assuming the realistic but restrictive hypothesis of collective Gaussian attacks. Under this assumption, we can efficiently estimate the parameters of the channel via maximum likelihood estimators and bound the corresponding error in the final secret key rate.

I. INTRODUCTION

Quantum key distribution (QKD) [1–4] allows two remote authenticated parties to establish a shared secret key without any assumption on the computational power of the eavesdropper, the security being based on fundamental laws of quantum mechanics, such as the no-cloning theorem [5, 6]. The first QKD protocols were based on the use of discrete variables (DVs), i.e., discrete degrees of freedom of the electromagnetic field, such as polarization or time bins. Later, at the end of the 90s and beginning of 2000, QKD was extended to continuous-variables (CVs) [7, 8] by the work of Ralph [9] and other authors [10–12], culminating in the seminal GG02 protocol [13] based on Gaussian modulation of coherent states. This seminal work also introduced the notion of reverse reconciliation that allowed experimental CV-QKD to reach long distances and led to the theoretical introduction of the reverse coherent information of a bosonic channel [15, 16]. Ref. [16] was the first exploration of the ultimate limits of point-to-point (i.e., repeaterless) QKD, culminating in 2015 with the discovery of the PLOB bound [17] (see Ref. [4, 18] for more details on the historical developments).

Other theoretical advances in CV-QKD were the introduction of thermal-state protocols [19–23] (where Refs. [21, 22] specifically studied the extension to longer wavelengths, down to the microwaves), two-way quantum communication protocols [24, 25], one-dimensional protocols [26, 27] and CV measurement-device independent (MDI) QKD [28]. Last but not least, there was the important development of CV-QKD with discrete-alphabet encoding. This idea was first introduced in the post-selection protocol of Ref. [29] and later developed in a number of works [30–38]. In particular, Refs. [29–32] considered binary and ternary alphabets of displaced coherent states. Ref. [33] considered four coherent states and, later, other words studied alphabets with the discovery number of states under pure-loss [34] and thermal-loss [35] attacks. All these security proofs were limited to the asymptotic case of infinite signal exchanged by the parties. In particular, the security of discrete-alphabet CV QKD has been proven asymptotically under general collective attacks using decoy-like states [36] or a suitable Gaussian bound [37].

In this work, we provide a finite-size composable proof of the security of discrete-alphabet CV-QKD protocols, under the assumption of collective Gaussian attacks [39] (and, in particular, collective entangling cloner attacks [4, 10] which result into a realistic thermal-loss channel between the remote parties). While the general arguments apply to any discrete alphabet, we focus on the case of phase-encoded coherent (or thermal) states, so that they are displaced in the phase-space to create regular constellations at fixed distance from the vacuum state. Our techniques combine tools from Refs. [40–42]. The asymptotic Gaussian assumption is used for the purpose of parameter estimation, for which we follow the approach of Refs. [43, 44]. The composable proof is then obtained by adapting the methods developed in Refs. [43, 44] for protocols with Gaussian modulation. In particular, we adapt an expression developed for CV-MDI-QKD [44] to the case of one-way QKD protocols.

The manuscript is organized as follows. In Sec. II we describe the discrete-alphabet (phase-encoded) QKD protocol, for which we discuss the asymptotic security analysis. In Sec. III we discuss parameter estimation in the presence of finite-size effects and, in Sec. IV we provide the key rate of the protocol in the composable security framework. Sec. V is for conclusions.

II. ASYMPTOTIC SECURITY OF A PHASE-ENCODED PROTOCOL

In a generic phase-encoded CV-QKD protocol with $N$ states, Alice randomly chooses between $N$ coherent states $|\alpha \exp(i2k\pi N^{-1})\rangle$ with $\alpha \geq 0$ and $k = 1, \ldots, N - 1$ (so that the classical label $k$ is chosen with probability $P_k = N^{-1}$). More generally, she prepares her mode $A$ in one of $N$ displaced thermal states $\rho_{A|k}$ with amplitudes $\alpha_k := \alpha \exp(i2k\pi N^{-1})$, each with a fixed mean number of photons $\bar{n}_k$. In terms of quadrature operators $\hat{x}_A := (\hat{q}_A, \hat{p}_A)^T$, Alice’s conditional thermal state has mean value

$$\bar{x}_{A|k} := \text{Tr}[\hat{x}_A \rho_k] = \alpha \begin{pmatrix} \cos(2k\pi N^{-1}) \\ \sin(2k\pi N^{-1}) \end{pmatrix}$$

(1)
and covariance matrix (CM) $V_{A|k} = (\nu_{th} + 1) I$, where $\nu_{th} = 2\tau_{th}$ and $I$ is the bidimensional identity matrix.

The signal state $\rho_{A|k}$ is travelling through a Gaussian (thermal-loss) channel which is under the full control of Eve. This is described by transmissivity $\tau$ and injected thermal noise $\omega \geq 1$. This channel can always be dilated into an entangling cloner attack [39], where Eve has a two-mode squeezed-vacuum (TMSV) state $\rho_{E}$ with zero mean $x_{E} = (0, 0, 0, 0)$ and CM

$$V_{E} = \begin{pmatrix} \omega I & \sqrt{\omega^2 - 1} I \\ \sqrt{\omega^2 - 1} I & \omega I \end{pmatrix}.$$  \hspace{1cm} (2)

In particular, mode $E$ is mixed with Alice’s travelling mode $A$ in a beam-splitter with transmissivity $\tau$ described by the symplectic matrix

$$B(\tau) = \begin{pmatrix} \sqrt{1-\tau} I & \sqrt{1-\tau} I \\ -\sqrt{1-\tau} I & \sqrt{1-\tau} I \end{pmatrix}.$$  \hspace{1cm} (3)

After the interaction, modes $E'$ and $e$ are kept in a quantum memory for an optimal final measurement taking into consideration of all the classical communication between the parties. For each use of the channel, Eve’s and Bob’s conditional output state $\rho_{E' e|k}$ has mean and CM given by

$$\begin{align*}
\bar{x}_{E' e|k} &= [B(\tau) \otimes I] (\bar{x}_{A|k} \otimes \bar{x}_{E}) = \bar{x}_{B|k} \otimes \bar{x}_{E'} \\
V_{E' e|k} &= [B(\tau) \otimes I] (V_{A|k} \otimes V_{E}|E) [B(\tau)^T \otimes I] \\
&= \begin{pmatrix} B & C \\ C^T & 0 \end{pmatrix} V_{E'}.
\end{align*}$$  \hspace{1cm} (4)

At the output, assume that Bob applies heterodyne measurement with outcome $(q_B, p_B)$ (the analysis can be easily adapted to considering the case of switching homodyne detections). Then, Eve’s doubly-conditional state $\rho_{E' e|k q_B p_B}$ has CM $46$ $48$

$$V_{E' e|k q_B p_B} = V_{E'} - C^T (B + I)^{-1} C$$  \hspace{1cm} (5)

while the probability of the outcome is given by

$$P_{q_B p_B|k} = \frac{e^{-\frac{(q_B - \bar{x}_{B|k} - \sqrt{\tau} \sigma_{E} \cos(2k + N - 1) p_B)^2}{2\Omega}}}{2\Omega},$$  \hspace{1cm} (6)

with $\Omega := 2 + \tau\nu_{th} + (1 - \tau)(\omega - 1)$. Setting

$q_B + iP_B = \beta e^{i(2k + N - 1) + \theta},$  \hspace{1cm} (7)

with $\beta \geq 0$ and $\theta \in [-\pi N - 1, \pi N - 1]$, we obtain

$$P_{\beta \theta|k} = \frac{1}{2\Omega} e^{-\frac{[\beta \sigma_{E} \cos(2k + N - 1) + \theta - \sqrt{\tau} \sigma_{E} \cos(2k + N - 1)]^2}{2\Omega}} \times e^{-\frac{[\beta \sigma_{E} \sin(2k + N - 1) + \theta - \sqrt{\tau} \sigma_{E} \sin(2k + N - 1)]^2}{2\Omega}}.$$  \hspace{1cm} (8)

Integrating over $\beta$ and for $\theta$, we derive

$$P_{l|k} = \int_{0, -\pi N - 1}^{\infty, \pi N - 1} \beta P_{\beta \theta|k} d\beta d\theta,$$  \hspace{1cm} (9)

which can be calculated numerically. Here $l$ is Bob’s estimator of Alice’s encoding variable $k$. Using Bayes’ formula we may write

$$P_{k|l} = \frac{P_{l|k} P_k}{\sum_{k=0}^{N-1} P_l P_{l|k}},$$  \hspace{1cm} (10)

and compute the residual entropy

$$H(k|l) = \sum_{l} \sum_{k} (-P_{k|l} \log P_{k|l}).$$  \hspace{1cm} (11)

The mutual information between the variables $k$ and $l$ is given by

$$I(k : l) = H(k) - H(k|l) = \log_2 N - H(k|l).$$  \hspace{1cm} (12)

In reverse reconciliation (RR), Eve’s information on $l$ is bounded by the Holevo quantity

$$\chi(E' : l) = S(\rho_{E'|e}) - \sum_{l} P_l S(\rho_{E'|e|l}),$$  \hspace{1cm} (13)

where $\rho_{E'|e} := \sum_{l} P_l \rho_{E'|e|l}$ is non-Gaussian, and the conditional state $\rho_{E'|e|l}$ is calculated by replacing of Eq. (3) in the Gaussian state $\rho_{E'|e|k q_B p_B}$ and averaging over the probability $P_{k, \beta, \theta|l}$, i.e., we have

$$\rho_{E'|e|l} = \sum_{k, \beta, \theta|l} \int_{\Omega} \rho_{E'|e|k \theta \beta} d\beta d\theta.$$  \hspace{1cm} (14)

Thus, the asymptotic secret key rate in RR is given by

$$R = \xi I(k : l) - \chi(E' : l),$$  \hspace{1cm} (15)

where $\xi$ is the reconciliation efficiency.

Note that some simplifications may be employed to compute the Holevo quantity of Eq. (13). Using the optimality of Gaussian states, we can replace $S(\rho_{E'|e}) \leq S(\rho_{E'|e}')$ where $\rho_{E'|e}'$ is a Gaussian state with the same CM as $\rho_{E'|e}$. Then, we could also use the concavity of the von Neumann entropy $S(\sum x P_x \rho_x) \geq \sum x P_x S(\rho_x)$ holding for any ensemble of states $\{P_x, \rho_x\}$. In this way, from Eq. (15), we see that we can bound the conditional entropic term as follows

$$S(\rho_{E'|e|l}) \geq \sum_{k, \beta, \theta|l} \int_{\Omega} P_{\beta \theta|k} S(\rho_{E'|e|k \theta \beta}) d\beta d\theta.$$  \hspace{1cm} (16)

Because the CM of the Gaussian state $\rho_{E'|e|k \theta \beta}$ does not depend on the variables $\beta, \theta, k$, while the mean value does, from Eq. (17) we then have $S(\rho_{E'|e|l}) \geq S(\rho_{E'|e|k \beta \theta})$ and finally $\sum_{l} P_l S(\rho_{E'|e|l}) \geq S(\rho_{E'|e|k \beta \theta})$. The entropy of $\rho_{E'|e|k \beta \theta}$ can be computed by the symplectic spectrum of its CM $V_{E'|e|k \beta \theta}$. Also note that the CM $V_{E'|e}$ of the average state $\rho_{E'|e}$ can be computed from the statistical moments $x_{E'|e|k \beta \theta}$ and $V_{E'|e|k \beta \theta}$ (see Appendix A for more details).
III. CHANNEL PARAMETER ESTIMATION

The asymptotic rate in Eq. (16) is a function of Alice’s encoding parameters, i.e., \( \alpha, N \) and \( \nu_k \), together with the channel parameters, i.e., \( \tau \) and \( \omega \), or equivalently \( \tau \) and \( \varepsilon \), where \( \varepsilon := \tau^{-1}[(1 - \tau)(\omega - 1)] \) is the excess noise. In order to estimate the parameters of the channel, Alice and Bob sacrifice \( m \) signal states (note that the parameter estimation can also post-poned after the error correction stage, in which case the parties can use almost all their data for both parameter estimation and key generation). By communicating their outcomes for these \( m \) signals, Alice and Bob can compute estimators for \( \tau \) and \( V_{\varepsilon} := \tau \varepsilon \) and corresponding confidence intervals. They can choose worst-case parameters to be used in the computation of the key rate in Eq. (16).

Therefore, assume that Alice reveals the encoding \( k \) of \( m \) signal states out of a block of \( M = m + n \) signal states. For \( m \) sufficiently large, we have that \( m/N \) can be chosen to be an integer. Bob will have samples \( B_{ki} \) for \( i = 1 \ldots m/N \) associated to a specific Alice’s encoding \( k \). Because we assume heterodyne detection, the discussion of the \( q \) and \( p \) quadratures is symmetric. In the \( q \) quadrature, Bob’s sampled \( q \)-quadratures \( B_{qi} \) can be described by the following stochastic variable

\[
q_{B_k} = \frac{\tau}{2} \alpha \cos(2k\pi/N) + q_{no},
\]

and variance

\[
E(q_{B_k}) = \frac{\tau}{2} \alpha \cos(2k\pi/N) \quad \text{and variance} \quad V_{no} = \frac{1}{2} \Omega = \frac{1}{2}(\tau \nu_k + \nu_k + 1) \quad \text{and variance} \quad V_{no} = \frac{1}{2} \Omega = \frac{1}{2}(\tau \nu_k + \nu_k + 1).
\]

We can then create maximum likelihood estimators for the mean value and variance of \( q_{B_k} \) starting from the samples \( B_{ki} \). In fact, we may write

\[
\hat{q}_{B_k} = \frac{N}{m} \sum_{i=1}^{m/N} B_{ki}, \quad \hat{V}_{no} = \frac{N}{m} \sum_{i=1}^{m/N} (B_{ki} - \hat{q}_{B_k})^2.
\]

The mean value and variance of the estimator \( \hat{q}_{B_k} \) are given by

\[
E(\hat{q}_{B_k}) = \frac{N}{m} \sum_{i=1}^{m/N} E(B_{ki}) = E(q_{B_k}),
\]

and

\[
Var(\hat{q}_{B_k}) = \frac{N^2}{m^2} \sum_{i=1}^{m/N} Var(B_{ki}) = \frac{N}{m} V_{no}.
\]

since \( B_{ki} \) can be considered to be i.i.d. variables (in a collective Gaussian attack).

Note that the estimator \( \hat{q}_{B_k} \) can be replaced by its expected value \( E(q_{B_k}) \) due to the fact that its variance in Eq. (24) vanishes for \( m \gg 1 \). Thus, we can write the variance estimator \( \hat{V}_{no} \) in Eq. (22) as

\[
\hat{V}_{no} = V_{no} \frac{N}{m} \sum_{i=1}^{m/N} \left( B_{ki} - E(q_{B_k}) \right)^2.
\]

The term inside the brackets follows a standard normal distribution with zero mean and unit variance. Therefore, the sum term follows a chi-squared distribution with zero mean and unit variance. Consequently, for the mean and variance of the estimator \( \hat{V}_{no} \) we obtain

\[
E(\hat{V}_{no}) = V_{no} \frac{N}{m} \sum_{i=1}^{m/N} E \left( \left( B_{ki} - E(q_{B_k}) \right)^2 \right) = V_{no},
\]

and

\[
Var(\hat{V}_{no}) = V_{no}^2 \frac{2}{m} \sum_{i=1}^{m/N} Var \left( \left( B_{ki} - E(q_{B_k}) \right)^2 \right) = 2 \frac{N}{m} V_{no}^2.
\]

Based on the estimator \( \hat{q}_{B_k} \), we can build an estimator for the transmissivity

\[
\hat{\tau}_k = 2 \alpha^{-2} \cos^{-2}(2k\pi/N) \left( \hat{q}_{B_k} \right)^2
\]

The estimator \( \hat{q}_{B_k} \) is the sample mean of \( B_{ki} \) and as such follows a Gaussian distribution. We then can express the above equation with the help of the chi-squared variable \( \left( \sqrt{\frac{N}{m}} \hat{q}_{B_k} \right)^2 \) with mean 1 and variance \( \left( \frac{2}{m} \right) \) as follows

\[
\hat{\tau}_k = \frac{V_{no}}{\alpha \cos(2k\pi/N)} \sqrt{\frac{N}{m}} \left( \frac{m}{N} \hat{q}_{B_k} \right)^2.
\]

This estimator of the transmissivity has mean and variance equal to

\[
E(\hat{\tau}_k) = \frac{2V_{no}N}{m \alpha^2 \cos^2(2k\pi/N)} \times \left( 1 + \frac{m}{N} \frac{\tau \alpha \cos(2k\pi/N)}{2V_{no}} \right)
\]

and

\[
Var(\hat{\tau}_k) = \frac{\sigma_k^2}{m} = \left( \frac{2V_{no}N}{m \alpha^2 \cos^2(2k\pi/N)} \right) \times 2 \left( 1 + \frac{m}{N} \frac{\tau \alpha \cos(2k\pi/N)}{2V_{no}} \right)
\]

and

\[
= 8 \tau \frac{N}{m} \frac{V_{no}}{\alpha^2 \cos^2(2k\pi/N)} + O(1/m^2). \]
Since there will other estimators corresponding to the other values of Alice’s encoding $k$ we can create an optimal linear combination of them with variance [42]

$$\sigma_q^2 = \left[ \sum_{k=0}^{N-1} (\sigma_k^2)^{-1} \right]^{-1}$$

$$= \frac{8}{m} \frac{V_{\text{no}}}{\alpha^2} \left[ \sum_{k=0}^{N-1} \cos(2k \pi / N) \right]^{-1}$$

$$= \frac{16}{m} \frac{V_{\text{no}}}{\alpha^2}. \quad (32)$$

So far, we have used only samples from the $q$-quadrature of Bob’s outcomes. Similar relations will hold for the $p$-quadrature. Combining all the available $q$- and $p$-samples, the optimal linear estimator $\hat{\tau}$ of the transmissivity will have variance

$$\sigma^2 = \frac{8}{m} \frac{V_{\text{no}}}{\alpha^2}. \quad (33)$$

In fact, for large $m$, we can approximate all the $2N$ estimators $\hat{\tau}_k$ to have Gaussian distributions with the same mean and variance $\sigma_p^2 = \sigma_q^2$. As a result, the global estimator $\hat{\tau}$ is a Gaussian variable with the same mean and variance equal to $\sigma^2$. Now, assuming an error $\epsilon_{\text{CPE}} = 10^{-10}$ for channel parameter estimation (CPE), we have to consider a 6.5 standard deviation interval for $\tau$. This means that the worst-case value for the transmissivity is equal to

$$\tau_{\text{CPE}} = \tau - 6.5 \sqrt{\tau \frac{8}{m} \frac{V_{\text{no}}}{\alpha^2}}. \quad (34)$$

Starting from $\hat{V}_{\text{no}}$, we may also define an estimator for the excess noise. Solving Eq. (21) with respect to $V_\epsilon$, we obtain

$$\hat{V}_\epsilon = 2\hat{V}_{\text{no}} - \hat{\tau}_\text{th} - 2. \quad (35)$$

Then the mean and variance of this estimator are given by

$$\mathbb{E} \left[ \hat{V}_\epsilon \right] = 2V_{\text{no}} - \tau \nu_{\text{th}} - 2,$$

$$\text{Var} \left[ \hat{V}_\epsilon \right] := s^2_k = \frac{8}{m} \frac{V_{\text{no}}^2 + \sigma^2 \nu_{\text{th}}}{m}. \quad (36)$$

The variance of the optimal linear combination $\hat{V}_\epsilon$ of all the estimators $\hat{V}_k$ (also considering the $p$-quadrature) is given by

$$s^2 = \frac{V_{\text{no}}}{m} + \frac{\sigma^2 \nu_{\text{th}}}{2N}. \quad (37)$$

Based on the assumption of large $m$, we approximate the distribution of each $\hat{V}_{\text{no}}$ to be Gaussian. As a result, the distribution of $\hat{V}_\epsilon$ is Gaussian with the same mean and variance given by $s^2$ above. Assuming an error $\epsilon_{\text{CPE}} = 10^{-10}$, we obtain the 6.5 confidence intervals for $\hat{V}_\epsilon$. Therefore, the worst-case value is give by

$$\hat{V}_\epsilon = V_\epsilon + 6.5 \sqrt{\frac{V_{\text{no}}^2}{m} + \frac{\sigma^2 \nu_{\text{th}}}{2N}}. \quad (38)$$

Using the worst-case values $\tau_{\text{CPE}}$ and $\hat{V}_\epsilon$, we can write a finite-size expression of the key rate $R = R(\tau, V_\epsilon)$ of Eq. (16) which accounts for the imperfect parameter estimation and the reduced number of signals. This is give by replacing

$$R(\tau, V_\epsilon) \rightarrow \frac{n}{M} R(\tau_{\text{CPE}}, \hat{V}_\epsilon) := \frac{n}{M} R^\text{CPE}. \quad (40)$$

IV. COMPOSABLE SECURITY

Our approach for the composable security of the protocol is based on tools of Ref. [43, 44]. Let us suppose that the block size is $M = n + m$, where $n$ signals are used for key generation and $m$ signals for parameter estimation. The total number of secret key bits that can be extracted from Bob’s variable $l$ are given by

$$s_{n,l}^{\epsilon_{\text{EC}}} \geq H_{\text{min}}(l|E')_{\rho_{E'E}} - \text{leak}_{\text{EC}}(n, \epsilon_{\text{EC}}) + 2 \log(2e),$$

where $H_{\text{min}}(l|E')_{\rho_{E'E}}$ is the smooth min-entropy of Bob’s variable $l$ conditioned on Eve’s quantum systems $E'$, which are described by the global state $\rho_{E'E}$ in Eve’s hands after successful error correction (EC). The term leak$_{\text{EC}}(n, \epsilon_{\text{EC}})$ accounts for the bits that are lost during the reconciliation process. Parameter $\epsilon$ is related to the probability that the protocol is not secure, while $\epsilon_s$ is the smoothing parameter, and $\epsilon_{\text{EC}}$ is associated with the error in the EC routine.

Under a collective attack, Eve’s state before EC can be considered to be a tensor product state $\rho_{E'E}$. However, this is no longer true after EC. In fact, if the EC routine is successful (with probability $p$), Eve’s state undergoes the transformation

$$\rho_{E'E} \rightarrow \rho_{E'E} = p^{-1} \Pi_{\text{EC}}\rho_{E'E}^\text{no}\Pi_{\text{EC}},$$

where $\Pi_{\text{EC}}$ is a suitable projector. Assuming that the protocol is not aborted (with probability $1 - p$), it is then secure with probability $\epsilon/p$. Theorem 1 in Ref. [44] states that we can still bound the number of secret bits by computing the smooth min-entropy over the tensor product state $\rho_{E'E}^\text{no}$ (before EC) proviso that we replace the smoothing parameter as $\epsilon_s \rightarrow \frac{\epsilon}{2} \epsilon_{\text{EC}}$ and we reduce the number of bits by $\log_2(p - \frac{\epsilon}{2} \epsilon_{\text{EC}})$.

Then, we can also use the conditional von Neuman entropy of $\rho_{E'}$, instead of the conditional smooth min-entropy of $\rho_{E'E}^\text{no}$ to approximate the previous bound. This is based on the asymptotic equipartition property (AEP) stating that the conditional smooth min-entropy
of $\rho_{E'}^{n}$ is larger or equal to $n$ times the conditional von Neumann entropy of $\rho_{E'}$, minus a correction term $\sqrt{n} \Delta_{\text{AEP}}$ [49]. This term depends on the smoothing parameter $\epsilon_{s}$ and the number of phase-encoded signals $N$; it can be bounded by

$$\Delta_{\text{AEP}} \leq 4 \left( \frac{1}{2} \log_{2} N + 1 \right) \sqrt{\log_{2}(2/e^{\xi})}. \quad (43)$$

In turn, the conditional von Neumann entropy can be written in terms of the von Neumann entropy and the quantum mutual information, with further simplifications in the presence of a classical variable $l$. In fact, we have

$$S(l | E')_{\rho_{E'}^{n}} = S(l)_{\rho_{E'}^{n}} - I(E' : l)_{\rho_{E'}^{n}} = H(l) - \chi(E' : l), \quad (44)$$

where $H(l)$ is the Shannon entropy and $\chi(E' : l)$ is the Holevo bound.

We then can make the following replacement

$$H(l) - \frac{1}{n} \text{leak}_{\text{EC}}(n, \text{EC}) = \xi I(k : l), \quad (45)$$

in terms of the mutual information $I(k : l)$ and the reconciliation parameter $\xi \in (0, 1)$. Thanks to this manipulations, the expression of the asymptotic secret key rate $R = \xi I(k : l) - \chi(E' : l)$ appears in the bound of Eq. (44). We explicitly have

$$s_{n}^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}} \geq nR + \sqrt{n} \Delta_{\text{AEP}} \left( \frac{2}{3} \rho_{s} \right) + 2 \log_{2}(p - \frac{2}{3} \rho_{s}) + 2 \log_{2}(2e). \quad (46)$$

Finally, we replace with the worst-case value of the rate $R^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}}$ from Eq. (44), which comes from the fact that the channel parameters are estimated as in Sec. IIII with associated error $\epsilon_{\text{CPE}}$. Accounting for this and the ratio $n/M$ due to parameter estimation, we write the rate

$$R^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}} = \frac{n}{M} R^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}} - \frac{\sqrt{n}}{M} \Delta_{\text{AEP}} \left( \frac{2}{3} \rho_{s} \right) + \frac{1}{M} \log_{2}(p - \frac{2}{3} \rho_{s}) + \frac{2}{M} \log_{2}(2e). \quad (47)$$

V. CONCLUSION AND DISCUSSION

In this work, we have studied the finite-size composable security of a discrete-alphabet CV-QKD protocol under the assumption of collective Gaussian attacks. This assumption is realistic because the standard model of loss and noise in optical quantum communications is the memoryless thermal-loss channel, which is dilated into a collective entangling cloner attack, i.e., a specific type of collective Gaussian attack. Our analysis extends previous asymptotic analysis under collective attacks to the finite-size and composable regime, but simultaneously pays the price to be restricted to Gaussian attacks. Removing this assumption is the subject of future investigations.

Since our analysis applies not only to displaced coherent states but also to displaced thermal states, it can be useful for studying the security of phase-encoded protocols at frequencies lower than the optical. It is also worth to stress that our derivation, described for phase-encoded signals, can immediately be extended to any configuration or constellation of displaced Gaussian states (e.g., coherent, thermal or squeezed), besides the fact that it also applies to CV-QKD protocols based on the Gaussian modulation of the amplitudes of Gaussian states (e.g., coherent, thermal or squeezed). As a matter of fact, the formalism of Sec. IV does not change. This is heavily based on Ref. [43] and the following simplification [44] originally developed for CV-MDI-QKD, that we have suitably adapted to the case of one-way QKD protocols. The most crucial part is the finite-size rate $R^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}}$ which can always be estimated, under the assumption of collective Gaussian attacks, by using maximum likelihood estimators and their confidence intervals, i.e., adopting simple variations of the technique in Sec. IIII. In this way, the finite-size rate $R^{\epsilon_{s} + \epsilon_{\text{EC}} + \epsilon_{\text{CPE}}}$ can always be expressed in terms of the asymptotic key rate $R$ of the specific protocol under consideration via the transformation in Eq. (44).

Acknowledgements. This work has been sponsored by the EPSRC Quantum Communications Hub (Grant No. EP/T001011/1) and the European Union via “Continuous Variable Quantum Communications” (CiViQ, Grant agreement No 820466).

[1] C. H. Bennett and G. Brassard, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175, 8 (1984).
[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992).
[4] 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, arXiv:1906.01645 (2019).
[5] W. Wootters, and W. Zurek, Nature 299, 802 (1982).
[6] J. Park, Found. Phys. 1, 23 (1970).
[7] S. L. Braunstein and P. van Loock Rev. Mod. Phys. 77, 513 (2005).
[8] Ch. Weedbrook, S. Pirandola, R. Garc-a-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. 84, 621 (2012).
[9] T. C. Ralph, Rev. A 61, 010303 (1999).
[10] M. Hillery, Phys. Rev. A 61, 022309 (2000).
Consider the generic quadrature
\[ \hat{x}_i \in \{\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n\} \] (A1)

of a non-mode bosonic system. Given a state \( \rho_A \), we have a vectorial mean value \( \bar{x}_A \), with generic element
\[ \bar{x}^i_A := \langle \hat{x}^i \rangle_{\rho_A} = \text{tr}(\hat{x}_i \rho_A), \] (A2)

and a CM \( V_A \), with generic element
\[ [V^i_A]_{ij} := \frac{1}{2} \langle [\Delta \hat{x}^i, \Delta \hat{x}^j] \rangle_{\rho_A} \] (A3)
\[ = \frac{1}{2} \text{tr} (\hat{x}_i \hat{x}_j + \hat{x}_j \hat{x}_i) \rho_A - \text{tr}(\hat{x}_i \rho_A) \text{tr}(\hat{x}_j \rho_A). \]

Let us assume that
\[ \rho_A = \sum_k P_k \rho_{A|k} \] (A4)
where \( \rho_{A|k} \) are Gaussian states with CM \( V_{A|k} \) and mean value \( \bar{x}_{A|k} \), chosen with probability \( P_k \). By using the linearity of the trace operation, the CM of the average state \( \rho_A \) will be given by
\[ [V_A]_{ij} = \frac{1}{2} \sum_k P_k \text{tr} \left( [\hat{x}_i \hat{x}_j + \hat{x}_j \hat{x}_i] \rho_{A|k} \right) - \sum_l \sum_m P_m P_l \text{tr}(\hat{x}_j \rho_{A|m}) \] (A5)

For the component \( \rho_{A|k} \), we may write
\[ \frac{1}{2} \text{tr} \left( [\hat{x}_i \hat{x}_j + \hat{x}_j \hat{x}_i] \rho_{A|k} \right) = [V_{A|k}]_{ij} + \text{tr}(\hat{x}_i \rho_{A|k}) \text{tr}(\hat{x}_j \rho_{A|k}), \] (A6)

and replace in Eq. (A5), so that we find
\[ [V_A]_{ij} = [V_{A|k}]_{ij} + \sum_k P_k \bar{x}^i_{A|k} \bar{x}^j_{A|k} \] (A7)
\[ - \sum_{l,m} P_m P_l \bar{x}^i_{A|m} \bar{x}^j_{A|l}, \]

which expresses the CM of the average state \( \rho_A \) in terms of the statistical moments of its components \( \rho_{A|k} \).