scientific reports

Check for updates

OPEN

Composable security of CV-MDI-QKD with secret key rate and data processing

Panagiotis Papanastasiou✉, Alexander G. Mountogiannakis & Stefano Pirandola

We provide a rigorous security proof of continuous-variable measurement-device-independent quantum key distribution which incorporates finite-size effects and composable terms. In order to use realistic and optimized parameters and be able to derive results close to experimental expectations, we run protocol simulations supported by a Python library, including all the protocol operations, from simulating the quantum communication till the extraction of the final key.

Quantum key distribution (QKD) uses a quantum channel for the transmission of signals between two distant legitimate parties to create a shared secret key[1–3]. The secret key can be later utilized for the symmetric encryption of confidential messages exchanged between the parties. In particular, based on the laws of quantum mechanics, QKD allows for the detection of the presence of an eavesdropper in the quantum channel and the quantification of the compromised amount of information[4,5]. Depending on this amount, the shared data after the quantum communication can be compressed into a shorter shared key, about which the eavesdropper possesses negligible knowledge. This leads to quantum-safe applications, i.e., applications safe against attacks by large quantum computers.

In the beginning, QKD protocols were based on a discrete-variable (DV) encoding[6–8], such as the polarization of a photon. The security of such protocols has been thoroughly investigated. More recently, protocols that exploit continuous degrees of freedom, such as the position and momentum of the electromagnetic field[9] have been developed[10–12]. These are called "continuous-variable" (CV) QKD protocols. CV-QKD is highly compatible with the current telecommunications and, consequently, promises simpler and cost-effective practical implementations. Furthermore, it produces high rates, which approach the capacity limit of repeaterless quantum communications, also known as PLOB bound[13]. Their performance with respect to larger distances has improved significantly[14,15].

Crucial improvements have also been demonstrated in their security level. We have different levels of security (on top of the levels listed below, the security is characterized also by the level of attacks, i.e, individual, collective, or coherent ones[9]) according to the assumptions taken into consideration when one calculates the secret key rate (secret bits per channel use). The first is the asymptotic security which assumes an infinite number of signals. The finite-size security[16] refers to the practical use of a finite number of signals. And finally, the composable framework[17] considers all the post-processing subroutines in the evaluation of the security of the protocol.

A standard QKD protocol provides security against channel attacks, where the eavesdropper interacts with the quantum signals propagating through the channel. However, equivalently crucial, if not more dangerous, are the attacks connected with the preparation or detection processes, where the eavesdropper has direct access to the labs of the two legitimate parties. These attacks are known as side-channel attacks[1]. MDI-QKD[18,19] and CV-MDI-QKD[20–24] have the intrinsic property of relieving the parties from any detection obligation. In fact, it uses an intermediate relay, which is responsible for the detection part of the protocol. The relay can be considered part of the channel, i.e., under the control of the eavesdropper. The outcomes of this detection are classically broadcast to the parties, who utilize them to build correlations between their data strings. This configuration can be used as a basis for constructing multi-user applications[25,26] (see[27], Appendix VII) that can be extended to QKD networks[28]. Experimental implementations have also taken place recently[29,30].

Here, we focus on a simulation analysis similar to Ref.[31,32] but for the CV-MDI protocol[20,21]. Its finite-size security analysis has been presented in Ref.[33], with a first composable study discussed in Ref.[34]. In "Protocol and asymptotic secret key rate" section, we give a detailed summary of the protocol and the calculation of its asymptotic key rate. Then, we assume finite-size effects and describe the postprocessing subroutines. In "Composable security" section, we adapt the composable proof of Ref.[17] to the CV-MDI protocol. This proof removes an issue from a previous treatment[34] (see also[27], Appendix VI). In "Privacy amplification" section, we explain how the parties apply the appropriate amount of compression to the data to extract a secret key, according to the previous

Department of Computer Science, University of York, York YO10 5GH, UK. ✉email: papkpan@gmail.com

analysis. We present all the results of the simulation with the help of a developed Python library in "Simulation and results" section. Conclusions are in "Conclusion" section.

Security analysis

In this section, we investigate the quantum communication part of the protocol (considering the classical post-processing part ideal). We focus on the potential to build strong correlations secret to the eavesdropper considering an infinite number of signals between the parties. We present this analysis here because, as we show later, the asymptotic secret key rate is an integral part of the composable secret key rate, along with the correction terms because of the non-ideal character of the classical postprocessing procedures.

Protocol and asymptotic secret key rate. Alice and Bob prepare coherent states $|\alpha\rangle$ and $|\beta\rangle$ with amplitudes $\alpha = (1/2)(Q_A + \mathrm{i}P_A)$ and $\beta = (1/2)(Q_B + \mathrm{i}P_B)$, carried by modes A and B respectively. In particular, they encode the real vectorial variables $\boldsymbol{\alpha} = (Q_A, P_A)$ and $\boldsymbol{\beta} = (Q_B, P_B)$ following the Gaussian distributions

$$G(\boldsymbol{\alpha}) = \frac{\exp\left[-\frac{1}{2}(Q_A^2 + P_A^2)/\sigma_A^2\right]}{2\pi\sigma_A^2}, \tag{1}$$

$$G(\boldsymbol{\beta}) = \frac{\exp\left[-\frac{1}{2}(Q_B^2 + P_B^2)/\sigma_B^2\right]}{2\pi\sigma_B^2}, \tag{2}$$

with variances σ_A^2 and σ_B^2 respectively. The two bosonic modes travel to an intermediate relay, where a Bell measurement is applied to them with outcome $\gamma = (1/2)(Q_R + \mathrm{i}P_R)$. We also use the notation $\boldsymbol{\gamma} = (Q_R, P_R)$.

Eve interacts with the traveling modes via a two-mode attack where mode E_1 is mixed with mode A through a beam splitter with transmissivity T_A and mode E_2 with mode B through a beam splitter with transmissivity T_B (see Fig. 1). The CM of Eve's modes is given by

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega_A\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B\mathbf{I} \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \tag{3}$$

where the bona fide conditions for g and g' are given in Ref.[21]. In fact, given the previous description (These attacks are collective Gaussian two mode attacks and represent the entangling cloner attack[35,36] counterpart of a channel comprised of two links.), the best attacks are those with $g < 0$ and $g' > 0$. Taking into consideration this area of values, one can see that as $|g|$ and $|g'|$ become larger, the modes become more quickly and more strongly correlated (entangled). Then, one can choose $g_{\max} = \max\{|g|, |g'|\}$ and assume the attack with

$$\mathbf{G}_{\max} = \begin{pmatrix} -g_{\max} & 0 \\ 0 & g_{\max} \end{pmatrix}, \tag{4}$$

as the worst-case scenario. In such a case, the quadratures can be treated equivalently, as they follow the same probability distribution.

The outputs Q_R and P_R are dependent on the variables Q_A, P_A and Q_B, P_B according to the following equations:

$$Q_R = \tau_B Q_B - \tau_A Q_A + Q_z, \tag{5}$$

$$P_R = \tau_B P_B + \tau_A P_A + P_z, \tag{6}$$

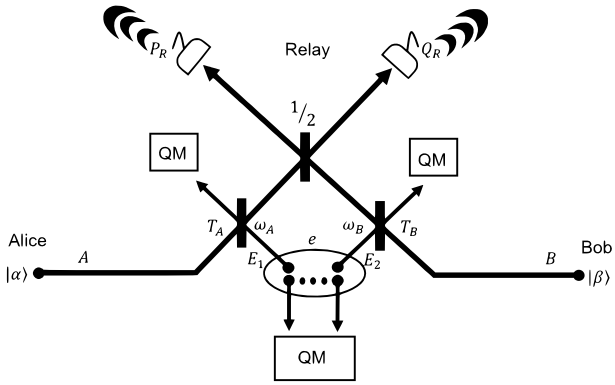

Figure 1. Alice and Bob send coherent states $|\alpha\rangle$ and $|\beta\rangle$ with modes A and B to the intermediate relay. Eve's modes E_1 and E_2 interact with the traveling modes via beam splitters with transmissivities T_A and T_B respectively. Eve's two-mode attack is characterized by thermal noise parameters ω_1 and ω_2 (see Eq. 3). Eve's modes are stored in a quantum memory waiting for an optimal measurement after the communication between the parties.

where τ_A and τ_B are rescaling parameters connected to the overall attenuation via

$$\tau_A = \sqrt{\eta_{\text{eff}} T_A/2}, \tag{7}$$

$$\tau_B = \sqrt{\eta_{\text{eff}} T_B/2}, \tag{8}$$

and the noise variables Q_z and P_z have variance σ_z^2 such that

$$\sigma_z^2 = \Xi + \nu_{\text{el}} + 1, \tag{9}$$

where η_{eff} and ν_{el} are the calibrated detection efficiency and electronic noise of the detectors respectively. In Supplementary Appendix V, we show the details of the calibrated noise attack and its connection to the uncalibrated one (see Supplementary Appendix IV). Subsequently, we obtain

$$\begin{aligned}\Xi = \frac{\eta_{\text{eff}}}{2}\Big((1-T_A)(\omega_A-1)+(1-T_B)(\omega_B-1)\Big)\\ +\eta_{\text{eff}} g_{\max}\sqrt{(1-T_A)(1-T_B)},\end{aligned} \tag{10}$$

with

$$g_{\max} = \max\{\sqrt{(\omega_A-1)(\omega_B+1)}, \sqrt{(\omega_B-1)(\omega_A+1)}\}. \tag{11}$$

In the EB representation, one introduces additional modes a and b in two-mode squeezed-vacuum (TMSV) states with modes A and B, respectively. These states have variances $\mu_A = \sigma_A^2 + 1$ and $\mu_B = \sigma_B^2 + 1$, respectively. Then, the encoding process is simulated by a heterodyne measurement on modes a and b with corresponding measurement outcomes $\tilde{\boldsymbol{\alpha}}$ and $\tilde{\boldsymbol{\beta}}$. The initial CM of the systems is given by

$$\mathbf{V}_{aABbE_1E_2} = \mathbf{V}_{aA} \oplus \mathbf{V}_{Bb} \oplus \mathbf{V}_{E_1E_2}, \tag{12}$$

with $\mathbf{V}_{aA}(\mu_A)$ and $\mathbf{V}_{Bb}(\mu_B)$ being CMs of a TMSV state

$$\mathbf{V}_{\text{TMSV}}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I}\end{pmatrix}, \tag{13}$$

and $\mathbf{Z} = \text{diag}\{1,-1\}$. The attack corresponds to applying a beam splitter with transmissivity T_A between the modes A and E_1 and a beam splitter of transmissivity T_B between modes B and E_2. The beam splitter symplectic operation with transmissivity T is given by

$$\mathcal{BS}(T) = \begin{pmatrix} \sqrt{T}\mathbf{I} & \sqrt{1-T}\mathbf{I} \\ -\sqrt{1-T}\mathbf{I} & \sqrt{T}\mathbf{I}\end{pmatrix}. \tag{14}$$

After the beam splitters, Alice's and Bob's modes A' and B' are mixed in a balanced beam splitter (i.e., $T = 1/2$) and conjugate homodyne measurements are applied to the output modes with outcomes grouped in the variable $\boldsymbol{\gamma}$. In fact, starting from a CM with the following general form

$$\mathbf{V}_{FM} = \begin{pmatrix} \mathbf{F} & \mathbf{C} \\ \mathbf{C}^{\mathsf{T}} & \mathbf{M}\end{pmatrix}, \tag{15}$$

if we apply a homodyne measurement to mode M with outcome x_M, the CM after the measurement will be given by

$$\mathbf{V}_{F|x_M} = \mathbf{F} - \mathbf{C}(\mathbf{\Pi}\mathbf{M}\mathbf{\Pi})^{-1}\mathbf{C}^{\mathsf{T}}, \tag{16}$$

with $\mathbf{\Pi} = \text{diag}\{1,0\}$ ($\mathbf{\Pi} = \text{diag}\{0,1\}$) for a $Q(P)$-measurement and $(.)^{-1}$ being the pseudo-inverse operation.

In this description, the CM after the relay measurements is given by

$$\mathbf{V}_{ab|\boldsymbol{\gamma}} = \begin{pmatrix} \phi\mathbf{I} & \eta\mathbf{Z} \\ \eta\mathbf{Z} & \theta\mathbf{I}\end{pmatrix}, \tag{17}$$

where

$$\phi = 1 + \sigma_A^2 - \frac{\tau_A^2\sigma_A^2(\sigma_A^2+2)}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2}, \tag{18}$$

$$\theta = 1 + \sigma_B^2 - \frac{\tau_B^2\sigma_B^2(\sigma_B^2+2)}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2}, \tag{19}$$

$$\eta = \frac{\tau_A \tau_B \sqrt{\sigma_A^2(\sigma_A^2+2)\sigma_B^2(\sigma_B^2+2)}}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2}. \tag{20}$$

The conditional CM after the heterodyne measurement of mode b with outcome $\tilde{\boldsymbol{\beta}}$ is given by

$$\mathbf{V}_{a|\boldsymbol{\gamma}\tilde{\boldsymbol{\beta}}} = \left(\phi - \frac{\eta^2}{\theta+1}\right)\mathbf{I}. \tag{21}$$

From the matrices

$$\mathbf{V}_{a|\boldsymbol{\gamma}} = \phi\mathbf{I}, \tag{22}$$

and $\mathbf{V}_{a|\boldsymbol{\gamma}\tilde{\boldsymbol{\beta}}}$, we can calculate the mutual information between $\tilde{\boldsymbol{\beta}}$ and Alice's outcome $\tilde{\boldsymbol{\alpha}}$ which is

$$I(\tilde{\boldsymbol{\alpha}} : \tilde{\boldsymbol{\beta}}|\gamma) = \frac{1}{2}\log_2 \frac{\det \mathbf{V}_{a|\boldsymbol{\gamma}} + \operatorname{tr} \mathbf{V}_{a|\boldsymbol{\gamma}} + 1}{\det \mathbf{V}_{a|\boldsymbol{\gamma}\tilde{\boldsymbol{\beta}}} + \operatorname{tr} \mathbf{V}_{a|\boldsymbol{\gamma}\tilde{\boldsymbol{\beta}}} + 1}. \tag{23}$$

One may also calculate, from the CM in Eq. (17), Eve's Holevo information

$$\chi(E : \tilde{\boldsymbol{\beta}}|\boldsymbol{\gamma}) = H(E|\boldsymbol{\gamma}) - H(E|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}), \tag{24}$$

$$= \int p(\boldsymbol{\gamma}) H(\rho_{E|\boldsymbol{\gamma}})\, \mathrm{d}^2\boldsymbol{\gamma} - \int p(\tilde{\boldsymbol{\beta}}, \boldsymbol{\gamma}) H(\rho_{E|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}})\, \mathrm{d}^2\boldsymbol{\gamma}\, \mathrm{d}^2\tilde{\boldsymbol{\beta}}, \tag{25}$$

$$= H(\rho_{ab|\boldsymbol{\gamma}}) - H(\rho_{a|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}}), \tag{26}$$

which is expressed in terms of conditional von Neumann entropies. Then by the assumption that Eve's systems $E = E_1' E_2' e$ purify the whole output state, we have that the von Neumann entropy of the state $\rho_{E|\boldsymbol{\gamma}}$ equals that of $\rho_{ab|\boldsymbol{\gamma}}$, and similar equivalence holds between $\rho_{E|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}}$ and $\rho_{a|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}}$. These entropies are not dependent on the outcomes $\tilde{\boldsymbol{\beta}}$ and $\boldsymbol{\gamma}$ and can be expressed in terms of the symplectic eigenspectra $\{\nu_\pm\}$ and $\tilde{\nu}$ of of the CMs $\mathbf{V}_{ab|\boldsymbol{\gamma}}$ and $\mathbf{V}_{a|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}}$ respectively, so that

$$H(\rho_{ab|\boldsymbol{\gamma}}) - H(\rho_{a|\tilde{\boldsymbol{\beta}}\boldsymbol{\gamma}}) = h(\nu_+) + h(\nu_-) - h(\tilde{\nu}), \tag{27}$$

with

$$h(\nu) := \frac{\nu+1}{2}\log_2\frac{\nu+1}{2} - \frac{\nu-1}{2}\log_2\frac{\nu-1}{2}. \tag{28}$$

In terms of mutual information, the measurement variables $\tilde{\boldsymbol{\alpha}}$ and $\tilde{\boldsymbol{\beta}}$ in the EB scheme are equivalent to the rescaled P&M variables, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Then the conditioning on $\boldsymbol{\gamma}$ is equivalent to a displacement on the variables $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ so that key-extraction variables, $\mathbf{x} = (Q_x, P_x)$ and $\mathbf{y} = (Q_y, P_y)$, need to be suitably constructed. In fact, the parties use the following relations

$$Q_x = Q_A - u_Q Q_R, \tag{29}$$

$$P_x = P_A - u_P P_R, \tag{30}$$

$$Q_y = Q_B - v_Q Q_R, \tag{31}$$

$$P_y = P_B - v_P P_R. \tag{32}$$

An optimal option for the parameters u and v is given by assuming a minimal correlation between the new variables, $\mathbf{x}$ and $\mathbf{y}$, and the relay outputs. This is explained by the fact that Eve should know as less as possible about $\mathbf{x}$ and $\mathbf{y}$ by knowing $\boldsymbol{\gamma}$. Therefore, we impose

$$\langle Q_y Q_R\rangle = \langle Q_x Q_R\rangle = 0, \quad \langle P_y P_R\rangle = \langle P_x P_R\rangle = 0, \tag{33}$$

so to obtain (These are the regression coefficients. Given a bipartition of a multivariate Gaussian distribution $\{\mathbf{x}_1, \mathbf{x}_2\}$ with CM $\boldsymbol{\Sigma}$, the regression coefficients are given by the matrix $\boldsymbol{\Sigma}_{12}\boldsymbol{\Sigma}_{22}^{-1}$. One may write that $\mathbf{y} = \mathbf{x}_1|\mathbf{x}_2 = \mathbf{x}_1 - \boldsymbol{\Sigma}_{12}\boldsymbol{\Sigma}_{22}^{-1}\mathbf{x}_2$.)

$$u_Q = \frac{\langle Q_A Q_R\rangle}{\langle Q_R^2\rangle} = \frac{-\tau_A\sigma_A^2}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2}, \tag{34}$$

$$u_P = \frac{\langle P_A P_R \rangle}{\langle P_R^2 \rangle} = -u_Q, \tag{35}$$

$$v_Q = \frac{\langle Q_B Q_R \rangle}{\langle Q_R^2 \rangle} = \frac{\tau_B \sigma_B^2}{\tau_B^2 \sigma_B^2 + \tau_A^2 \sigma_A^2 + \sigma_z^2}, \tag{36}$$

$$v_P = \frac{\langle P_B P_R \rangle}{\langle P_R^2 \rangle} = v_Q. \tag{37}$$

Therefore, one may write

$$I(\mathbf{x} : \mathbf{y}) = I(\boldsymbol{\alpha} : \boldsymbol{\beta}|\boldsymbol{\gamma}) = I(\tilde{\boldsymbol{\alpha}} : \tilde{\boldsymbol{\beta}}|\boldsymbol{\gamma}), \tag{38}$$

where the first equality is proven in Ref.[27], Appendix I.

The quantum mutual information between Eve's system $E = E_1' E_2' e$ and Bob's key-extraction variable $\mathbf{y}$ when she has access to the variable $\boldsymbol{\gamma}$ is given by[37], Lemma 7.4.4

$$I(E\boldsymbol{\gamma} : \mathbf{y}) = \cancelto{0}{I(\boldsymbol{\gamma} : \boldsymbol{\gamma})} + I(E : \mathbf{y}|\boldsymbol{\gamma}) = \chi(E : \mathbf{y}|\boldsymbol{\gamma}) \tag{39}$$

and it is equal to the Holevo information $\chi(E : \mathbf{y}|\boldsymbol{\gamma})$ since $\mathbf{y}$ is a classical variable. In particular, we have that, given $\boldsymbol{\gamma}$, there is a function $\mathbf{y} = f(\boldsymbol{\beta})$ determined by the relations in Eqs. (31) and (32) such that $\boldsymbol{\beta} = f^{-1}(\mathbf{y})$. This allows us to apply the data processing inequality in both directions with respect to y and β and obtain

$$\chi(E : \mathbf{y}|\boldsymbol{\gamma}) = \chi(E : \boldsymbol{\beta}|\boldsymbol{\gamma}). \tag{40}$$

At this point, one may define the asymptotic key rate

$$R_{\text{asy}} = \zeta I(\mathbf{x} : \mathbf{y}) - \chi(E : \mathbf{y}|\boldsymbol{\gamma}), \tag{41}$$

$$= \zeta I(\boldsymbol{\alpha} : \boldsymbol{\beta}|\boldsymbol{\gamma}) - \chi(E : \boldsymbol{\beta}|\boldsymbol{\gamma}), \tag{42}$$

$$= R(\zeta, \sigma_A^2, \sigma_B^2, \eta, \upsilon_{\text{el}}, T_A, T_B, \Xi), \tag{43}$$

which is calculated starting from the CM in Eq. (17) as in Ref.[21]. Note that ζ is the reconciliation parameter defined later in Eq. (70). This parameter accounts for the proportion of mutual information given to Eve during the public channel communication of the parties performing a non-ideal reconciliation process.

Parameter estimation. Here we follow the PE proposed in Ref.[33]. An alternative way is described in[27], Appendix II.B based on extra simplifying assumptions. In particular, based on m samples $[Q_A]_i$, $[Q_B]_i$, $[Q_R]_i$, for $i = 1, \ldots, m$, the parties calculate the maximum likelihood estimators (MLEs) of the covariances $\text{Cov}(Q_A, Q_R) = \langle Q_A Q_R \rangle = -\tau_A \sigma_A^2$ and $\text{Cov}(Q_B, Q_R) = \langle Q_B Q_R \rangle = \tau_B \sigma_B^2$. These estimators are given by

$$\widehat{C}_{Q_A Q_R} = \frac{1}{m} \sum_{i=1}^{m} [Q_A]_i [Q_R]_i, \tag{44}$$

$$\widehat{C}_{Q_B Q_R} = \frac{1}{m} \sum_{i=1}^{m} [Q_B]_i [Q_R]_i, \tag{45}$$

$$\widehat{C}_{P_A P_R} = \frac{1}{m} \sum_{i=1}^{m} [P_A]_i [P_R]_i, \tag{46}$$

$$\widehat{C}_{P_B P_R} = \frac{1}{m} \sum_{i=1}^{m} [P_B]_i [P_R]_i. \tag{47}$$

From these, they define estimators for T_A and T_B, i.e.,

$$\widehat{T}_A = \frac{2}{\eta_{\text{eff}} (\sigma_A^2)^2} \min\{|\widehat{C}_{Q_A Q_R}|^2, |\widehat{C}_{P_A P_R}|^2\}, \tag{48}$$

$$\widehat{T}_B = \frac{2}{\eta_{\text{eff}} (\sigma_B^2)^2} \min\{|\widehat{C}_{Q_B Q_R}|^2, |\widehat{C}_{P_B P_R}|^2\}. \tag{49}$$

Then they define an estimator for σ_z^2. This estimator is given by

$$\widehat{\sigma}_z^2 = \max\left\{\frac{1}{m}\sum_{i=1}^{m}\left([Q_R]_i + \widehat{\tau}_A[Q_A]_i - \widehat{\tau}_B[Q_B]_i\right)^2, \frac{1}{m}\sum_{i=1}^{m}\left([P_R]_i - \widehat{\tau}_A[P_A]_i - \widehat{\tau}_B[P_B]_i\right)^2\right\}, \tag{50}$$

with

$$\widehat{\tau}_A = \sqrt{\eta_{\text{eff}}\widehat{T}_A/2}, \tag{51}$$

$$\widehat{\tau}_B = \sqrt{\eta_{\text{eff}}\widehat{T}_B/2}, \tag{52}$$

and obtain the associated variances[27], Appendix II.A

$$\sigma^2_{\widehat{T}_A} \simeq \frac{4\widehat{T}_A}{m}\left[\widehat{T}_A + \frac{\widehat{T}_B}{2}\frac{\sigma_B^2}{\sigma_A^2}\right]\left(2 + \frac{2\widehat{\sigma}_z^2/\eta_{\text{eff}}}{\widehat{T}_A\sigma_A^2 + \frac{\widehat{T}_B}{2}\sigma_B^2}\right), \tag{53}$$

$$\sigma^2_{\widehat{T}_B} \simeq \frac{4\widehat{T}_B}{m}\left[\widehat{T}_B + \frac{\widehat{T}_A}{2}\frac{\sigma_A^2}{\sigma_B^2}\right]\left(2 + \frac{2\widehat{\sigma}_z^2/\eta_{\text{eff}}}{\widehat{T}_B\sigma_B^2 + \frac{\widehat{T}_A}{2}\sigma_A^2}\right), \tag{54}$$

$$V_z \simeq \frac{2(\widehat{\sigma}_z^2)^2}{m}. \tag{55}$$

Based on $\widehat{\sigma}_z^2$ they find an estimator for Ξ given by

$$\widehat{\Xi} = \widehat{\sigma}_z^2 - v_{\text{el}} - 1, \tag{56}$$

with variance equal to

$$\sigma^2_{\widehat{\Xi}} := V_z. \tag{57}$$

Finally, worst-case scenario values can be derived given the PE error ϵ_{PE}. These values are

$$\widetilde{T}_A = \widehat{T}_A - w\sigma_{\widehat{T}_A}, \tag{58}$$

$$\widetilde{T}_B = \widehat{T}_B - w\sigma_{\widehat{T}_B}, \tag{59}$$

$$\widetilde{\Xi} = \widehat{\Xi} + w\sigma_{\widehat{\Xi}}, \tag{60}$$

where

$$w = \sqrt{2}\text{erf}^{-1}(1 - \epsilon_{\text{PE}}). \tag{61}$$

Using the previous values, the parties can compute a secret key rate with an overestimated Holevo information

$$R_m := \zeta I(\mathbf{x}:\mathbf{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}} - \chi(E:\mathbf{y}|\boldsymbol{\gamma})|_{\widetilde{T}_A,\widetilde{T}_B,\widetilde{\Xi}}. \tag{62}$$

Note here that $m = N - n$ where N is the number of signals sent through the channel and n is the number of signals devoted to secret key extraction for each block. In a practical situation, where the transmission can be assumed stable over a large number of blocks n_{bks}, one can use m signals on average from each block in order to estimate the channel parameters. Thus the parties sacrifice $M = mn_{\text{bks}}$ for PE and the corresponding rate is given by

$$R_m \to R_M := \left[\zeta I(\mathbf{x}:\mathbf{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}} - \chi(E:\mathbf{y}|\boldsymbol{\gamma})|_{\widetilde{T}_A,\widetilde{T}_B,\widetilde{\Xi}}\right]_{m=M}. \tag{63}$$

The mutual information and the correlation between the two variables $\mathbf{x}$ and $\mathbf{y}$ are connected as follows[38], Eq. (8.56) (see also[27], Eq. (2)):

$$I(\mathbf{x}:\mathbf{y}) = \log_2[1 + \text{SNR}] = \log_2\left[(1 - \rho^2_{\mathbf{xy}})^{-1}\right]. \tag{64}$$

One may derive the estimator for the correlation between the variables by replacing with the MLEs of the transmissivities and noise into the mutual information, namely,

$$\widehat{\rho}_{\mathbf{xy}} = \sqrt{1 - 2^{-I(\mathbf{x}:\mathbf{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}}}}, \tag{65}$$

which helps in the calculation of the *a priori* probabilities for the initialization step of the decoding sum-product algorithm of the error correction step[31,32].

Data reconciliation. The parties apply the transformations of Eqs. (29)–(32) based on the quantities in Eqs. (34)–(37) calculated via the MLEs of the previous section. Bob and Alice combine their data from the Q and P quadratures into one variable. In particular, Alice and Bob apply the following mapping to their data:

$$[x]_{2i-1} = [Q_x]_i, \tag{66}$$

$$[x]_{2i} = [P_x]_i, \tag{67}$$

$$[y]_{2i-1} = [Q_y]_i, \tag{68}$$

$$[y]_{2i} = [P_y]_i, \tag{69}$$

in order to obtain $2n$ samples from each block. Afterwards, the parties apply the EC procedure using non-binary LDPC codes following Ref.[32], Sect. III.B (for extra details see also Ref.[31]). More specifically, they define the worst-case estimator (up to an error probability ϵ_{ent}) for the reconciliation parameter ζ appearing in Eq. (43) which is given by

$$\hat{\zeta} = 2\frac{\widehat{H}(\mathsf{I}) + R_{\text{code}}q - p - \delta_{\text{ent}}}{I(\mathbf{x}:\mathbf{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}}}, \tag{70}$$

where $2(\widehat{H}(\mathsf{I}) - \delta_{\text{ent}})$ is the worst-case scenario entropy of the raw-key string described by I, the normalized and discretized version of y. In particular, $2\widehat{H}(\mathsf{I})$ is the estimator of the previous entropy, $-R_{\text{code}}q + p$ is the maximum data exchanged for reconciliation per channel use when one uses a non-binary LDPC code with the rate R_{code} associated with the Galois filed $\mathcal{G}(2^q)$ and discretization of p bits. We take into consideration here that Bob applies the LDPC encoding only to the q bits of I while the rest $p - q$ bits are entirely sent through the public channel. $I(\mathbf{x}:\mathbf{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}}$ is the ideal mutual information between the parties according to the data (i.e., after parameter estimation) which appears in Eq. (63). In fact by replacing ζ in the previous equation, one obtains the practical key rate

$$R_M^{\text{EC}} = 2[\widehat{H}(\mathsf{I}) + R_{\text{code}}q - p - \delta_{\text{ent}}] - \chi(E:\mathbf{y}|\boldsymbol{\gamma})|_{\widetilde{T}_A,\widetilde{T}_B,\widetilde{\Xi}}. \tag{71}$$

The parties started with two different sequences of n_{bks} blocks each with $2N$ initial samples and, in the process (after PE and EC), these are reduced to two indistinguishable binary sequences (with probability $1 - \epsilon_{\text{EC}}$) that consist of $p_{\text{EC}}n_{\text{bks}}$ blocks each carrying $2np$ bits:

$$\mathsf{I}_{\text{bin}} := \bar{\mathsf{I}}^n_{\text{bin}}\mathsf{I}^n_{\text{bin}} \simeq \tilde{\mathsf{I}}_{\text{bin}} := \widehat{\mathsf{I}}^n_{\text{bin}}\mathsf{I}^n_{\text{bin}}. \tag{72}$$

Note that $\bar{\mathsf{I}}^n_{\text{bin}}$ corresponds to the part of the original variable I in binary form that has been sent through the public channel using the LDPC encoding, $\mathsf{I}^n_{\text{bin}}$ is the part in binary form that has been sent unchanged through the public channel, and $\widehat{\mathsf{I}}^n_{\text{bin}}$ is the binary form of the successfully decoded and verified part with probability p_{EC}. The parties need to apply on these sequences the appropriate amount of compression during the PA step so that the previous raw-data strings become a secret key. This is determined by the composable key rate calculated below. Concatenating appropriately the previous parts, the parties end up with the raw data sequences I_{bin} for Bob and $\tilde{\mathsf{I}}_{\text{bin}}$ for Alice in binary form.

Composable security. We adopt the composable framework security analysis presented in Ref.[17], Appendix G to the requirements of the CV-MDI-QKD protocol. More specifically, the secret key is characterized by certain properties stemming from certain post-processing procedures, and there is an overall probability ϵ that the key fails to possess at least one of these properties.

According to the previous analysis, one may write for the length of the secret key[17], Eq. (G12):

$$\begin{aligned} s_n \geq\ & nH(l|E\boldsymbol{\gamma})_\rho - \sqrt{n}\Delta_{\text{AEP}}(p_{\text{EC}}\epsilon_{\text{s}}^2/3, 2^{2p}) \\ & + \log_2\left[p_{\text{EC}}(1-\epsilon_{\text{s}}^2/3)\right] + 2\log_2\sqrt{2}\epsilon_{\text{h}} - \text{leak}_{\text{EC}}, \end{aligned} \tag{73}$$

where l is defined according to the bidirectional mapping

$$l = \mathsf{I}_Q 2^p + \mathsf{I}_P, \tag{74}$$

where $\mathsf{I}_Q(\mathsf{I}_P)$ is the I instance corresponding to the $q(p)$-quadrature. Note that here we have used a virtual concatenation assumption (see Appendix A of [32]) to pass from a description based on the single-quadrature variable I (normalized and discetized) to one based on the vectorial variable l. One may also observe that, in this case, Eve's system is described by the group of modes E plus the classical variable $\boldsymbol{\gamma}$. In particular, $H(l|E\boldsymbol{\gamma})$ is the conditional von Neumann entropy of the variable l conditioned on E and $\boldsymbol{\gamma}$, and[39], Eq. (61)

$$\Delta_{\rm AEP}(\epsilon_{\rm s},|\mathcal{L}|)=4\log_2(\sqrt{|\mathcal{L}|}+2)\sqrt{\log_2(2/\epsilon_s^2)},\tag{75}$$

with $|\mathcal{L}|$ being the cardinality of the discretized variable l, which in our case is 2^{2p}. Note that, for the conditional mutual information, we have [37], Def. 7.4.1

$$I(l:E|\boldsymbol{\gamma})_{\rho_l}=H(l|\boldsymbol{\gamma})-H(l|E\boldsymbol{\gamma})_{\rho_l}.\tag{76}$$

In particular, this mutual information is between a classical variable l and a quantum system E (conditioned on another classical variable $\boldsymbol{\gamma}$). This is therefore the Holevo information $\chi(E:l|\boldsymbol{\gamma})$, i.e., an upper bound for the accessible information on l given that Eve possesses E (and knows the variable $\boldsymbol{\gamma}$). Therefore, by reversing Eq. (76), one may write

$$H(l|E\boldsymbol{\gamma})_{\rho_l}=H(l|\boldsymbol{\gamma})-\chi(E:l|\boldsymbol{\gamma})_{\rho_l},\tag{77}$$

where $H(l|\boldsymbol{\gamma})=H(l)$ (see Eq. 33) is the Shannon entropy of l. In more detail, using the data processing inequality, we manipulate Eve's Holevo bound as follows

$$\chi(E:l|\boldsymbol{\gamma})_{\rho_l}\leq\chi(E:Q_y,P_y|\boldsymbol{\gamma})=\chi(E:\mathbf{y}|\boldsymbol{\gamma}).\tag{78}$$

Therefore we have

$$H(l|E\boldsymbol{\gamma})_{\rho_l}\geq H(l)-\chi(E:\mathbf{y}|\boldsymbol{\gamma}).\tag{79}$$

We may replace Eq. (79) in Eq. (73) and then set

$$\zeta I(\mathbf{x}:\mathbf{y})=H(l)-n^{-1}{\rm leak}_{\rm EC}.\tag{80}$$

In this way, we derive

$$\begin{aligned}s_n\geq\;&nR_{\rm asy}-\sqrt{n}\Delta_{\rm AEP}(p_{\rm EC}\epsilon_{\rm s}^2/3,2^{2p})\\&+\log_2[p_{\rm EC}(1-\epsilon_{\rm s}^2/3)]+2\log_2\sqrt{2}\epsilon_{\rm h},\end{aligned}\tag{81}$$

where we include the asymptotic secret key rate of Eq. (43). One may replace $R_{\rm asy}$ with $R_M^{\rm EC}$ of Eq. (71) into Eq. (81) to obtain (see also[17,32,39])

$$R=\frac{np_{\rm EC}}{N}\tilde{R},\;\tilde{R}:=\left(R_M^{\rm EC}-\frac{\Delta_{\rm AEP}}{\sqrt{n}}+\frac{\Theta}{n}\right),\tag{82}$$

with composable terms

$$\Delta_{\rm AEP}:=4\log_2\left(2^p+2\right)\sqrt{\log_2\left(\frac{18}{p_{\rm EC}^2\epsilon_{\rm s}^4}\right)},\tag{83}$$

$$\Theta:=\log_2[p_{\rm EC}(1-\epsilon_{\rm s}^2/3)]+2\log_2\sqrt{2}\epsilon_{\rm h}.\tag{84}$$

The overall security parameter is equal to

$$\epsilon=\epsilon_{\rm cor}+\epsilon_{\rm h}+\epsilon_{\rm s}+p_{\rm EC}(3\epsilon_{\rm PE}+\epsilon_{\rm ent}),\tag{85}$$

where we note that the factor 3 is due to the fact the $\epsilon_{\rm PE}$ is defined per parameter.

One may also derive an approximate key rate, which is not based on the data postprocessing

$$R_{\rm theo}=\frac{np_{\rm EC}}{N}R^{\star},\;R^{\star}:=\bar{R}_M-\frac{\Delta_{\rm AEP}}{\sqrt{n}}+\frac{\Theta}{n},\tag{86}$$

where $\bar{R}_M$ is the rate in Eq. (63) but where the estimators are approximated using the initial values of the simulation (see, e.g., the steps in Sects. III.B.1 and III.B.2 in Ref.[31]). In fact, one may define $\bar{R}_M$ from Eq. (63) but where the following substitutions have been made:

$$\widehat{T}_A\to\mathbb{E}(\widehat{T}_A)\simeq T_A+\mathcal{O}(1/M),\tag{87}$$

$$\widehat{T}_B\to\mathbb{E}(\widehat{T}_B)\simeq T_B+\mathcal{O}(1/M),\tag{88}$$

$$\widehat{\Xi}\to\mathbb{E}(\widehat{\Xi})\simeq\Xi,\tag{89}$$

and

$$\widetilde{T}_A\to T_A-w\sigma_{T_A},\tag{90}$$

μ_A, μ_B	ζ (%)	R_{code}	SNR	R
45	90	0.833	10.019	0.00452259
46	92.15	0.846	10.252	0.06346475
47	91.35	0.846	10.485	0.04397952
48	90.62	0.846	10.718	0.01369927
49	92.35	0.857	10.951	0.06547397
50	91.64	0.857	11.189	0.04992091

Table 1. Composable secret key rate R (bits/use) versus Alice's and Bob's signal variances μ_A and μ_B. The rightmost column displays the average value for R, which is obtained after 5 simulations. Here we use $N = 5 \times 10^5$ and $n_{\text{bks}} = 100$. All simulations have achieved $p_{\text{EC}} \geq 0.95$. Parameters not listed here are taken as in Table 2.

$$\widetilde{T}_B \to T_B - w\sigma_{T_B}, \tag{91}$$

$$\widetilde{\Xi} \to \Xi + w\sigma_{\Xi}, \tag{92}$$

where $\sigma_{T_A}, \sigma_{T_B}$, and σ_{Ξ} have been calculated through Eqs. (53), (54), and (57), respectively, after replacing T_A, T_B, and σ_z^2 in those formulas. Note that the rates presented in this section do not rely on the conjecture mentioned in[27], Appendix VI.

Privacy amplification. Now the parties are ready to apply the appropriate amount of compression indicated by Eq. (82) on their binary strings in Eq. (72) to create a secret key through the PA step. To achieve this, they compress them via universal hashing. More specifically, they apply a modified Toeplitz matrix $\mathbf{G}(\mathbf{I}_r|\mathbf{T}_{r,2np-r})$ to their sequences in order to extract the secret key[40]

$$K = \mathbf{G}S = \mathbf{I}_r|_{\text{bin}}^{r} \oplus \mathbf{T}_{r,2np-r}|_{\text{bin}}^{2np-r}, \tag{93}$$

where $r = 2np\tilde{R}$, the Toeplitz matrix $\mathbf{T}_{r,2np-r}$ is of $r \times 2np - r$ dimensions and $\mathbf{I}_r$ is the $r \times r$ identity matrix, with $|_{\text{bin}}^{r}$ we denote the first r bits of the raw key string and with $|_{\text{bin}}^{2np-r}$ the rest.

Simulation and results

In our simulations, the attack is handled by initially defining values for the excess noise of Alice's (ξ_A) and Bob's (ξ_B) channels. These values, along with the transmissivity of each channel, constitute the thermal noise ω for each channel respectively as follows:

$$\omega_A = \frac{T_A \xi_A}{1 - T_A} + 1, \tag{94}$$

$$\omega_B = \frac{T_B \xi_B}{1 - T_B} + 1. \tag{95}$$

Using Alice's thermal noise value, we can estimate the correlation parameter g from Eq. (11). We now have all components to find the excess noise variance Ξ, which is shown in Eq. (10). Finally, the noise variance σ_z^2 is calculated through Eq. (9).

The parameters used to execute the simulations are listed in Table 2. To begin with, the symmetric version of the protocol is examined, which means that the signal variance and the channel parameters will be the same between Alice and Bob, i.e. $\mu_A = \mu_B$, $T_A = T_B$ and $\xi_A = \xi_B$.

To find a signal variance range, for which the composable rate R becomes positive, the asymptotic rate R_{asy} was maximized using a modulation variance optimization function. Table 1 shows that a positive R can be achieved, when $45 \leq \mu_A, \mu_B \leq 50$. Under these conditions, the SNR spans from approximately 10 to 11.89. As presented in the Table, the choice of the reconciliation efficiency is important, when trying to maximize the value of R. It is important to note that neither the asymptotic nor the composable rate will further grow, as the signal variances increase. This means that, at some point, the rates will saturate and eventually become negative again.

Knowing the variables, for which the composable rate becomes positive, we can now identify what is the maximum tolerable excess noise in the system. For this purpose, $\mu_A = \mu_B = 46$ is chosen, in order to produce a high rate (and therefore tolerate more excess noise), while performing a faster EC procedure (when compared to that for $\mu_A = \mu_B = 49$). Therefore, in Fig. 2, the symmetric case of the protocol is considered again, with $\mu_A = \mu_B = 46$ and with the excess noise being variable. As observed from the plot, ξ can take values up to 0.008, before the protocol is deemed unsafe for key distribution.

Next, we investigate the asymmetric version of the protocol, where the channel parameters, as well as the signal variances, are different between Alice and Bob. Here, two cases are examined: Fig. 3 shows the behaviour of Alice's transmissivity against the composable key rate and Fig. 4 displays the maximum tolerable values for Alice's excess noise. Regarding the former case, it is possible for Alice's channel to reach transmissivity values of

Parameter	Value (Table 1)	Value (Fig. 2)	Value (Fig. 3)	Value (Fig. 4)
T_A	0.98	0.98	Variable	0.96
T_B	0.98	0.98	0.985	0.985
ξ_A	0.005	Variable	0.006	Variable
ξ_B	0.005	Variable	0.004	0.004
η	0.98	0.98	0.98	0.98
υ_{el}	0.01	0.01	0.01	0.01
n_{bks}	100	100	100	100
N	5×10^5	5×10^5	5.88×10^5	5.88×10^5
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	$0.15 n_{\text{bks}} N$	$0.15 n_{\text{bks}} N$
p	6	6	7	7
q	4	4	4	4
α	7	7	7	7
$\text{iter}_{\max}$	200	200	100	100
$\epsilon_{\text{PE,s,h,corr}}$	2^{-32}	2^{-32}	2^{-32}	2^{-32}
μ_A	Variable	46	60	60
μ_B	Variable	46	50	50

Table 2. The input parameters for the simulations.

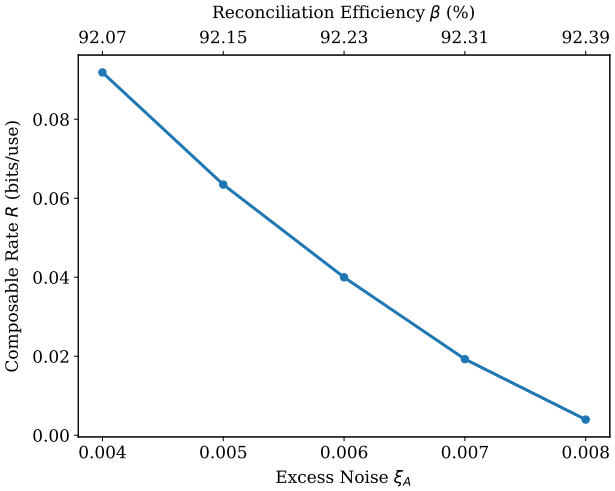

Figure 2. Composable secret key rate R (bits/use) versus Alice's and Bob's excess noise values $\xi = \xi_A = \xi_B$. Every point represents the average value of R, which is obtained after 5 simulations. Here we use $N = 5 \times 10^5$ and $n_{\text{bks}} = 100$. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant and equal ($\mu_A = \mu_B = 46$). The values of the reconciliation efficiency ζ are shown on the top axis. Other parameters are taken as in Table 2.

about $T_A = 0.94$, which translates to a fiber length of 1.34 km. The latter case shows that it is feasible to achieve a positive R under relatively high values for the excess noise, which can be extended to $\xi_A = 0.01$. To ensure a positive composable rate is positive under harsher noise settings, it is possible to employ a larger LDPC matrix with a block length very close to the order of 10^6 (The use of non-binary LDPC codes allows for block sizes under 10^6. A fair comparison with existing research (using binary LDPC codes) would be to multiply the current block sizes with the Galois field component q. Note that the stable channel assumption (see Eq. 63) and the use of high SNR in our study contribute, as well, to obtaining rates with these block size values.) and $R_{\text{code}} = 0.875$ for the task. Because of the finite-size effect, a larger LDPC block size leads to higher values for the reconciliation efficiency, when all other values remain the same.

Conclusion

In this study, we give a rigorous proof for the composable security of the Gaussian-modulated CV-MDI protocol and we calculate its rate. Depending on this rate, the appropriate amount of compression is applied, in order to extract a secret key. We simulate the quantum communication step and we apply all the classical postprocessing steps on the generated data. All of these procedures are performed by means of an associated Python library.

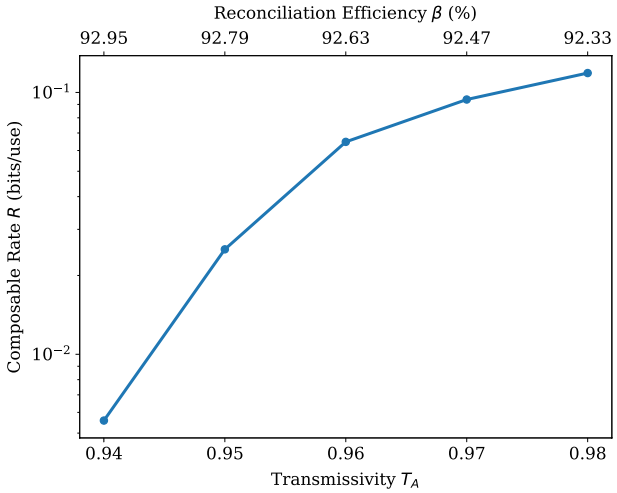

Figure 3. Composable secret key rate R (bits/use) versus Alice's transmissivity T_A. Every point represents the average value of R, which is obtained after 5 simulations. Here we use $N = 5.88 \times 10^5$ and $n_{\text{bks}} = 100$. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant ($\mu_A = 60$, $\mu_B = 50$). The values of the reconciliation efficiency ζ are shown on the top axis. Other parameters are taken as in Table 2.

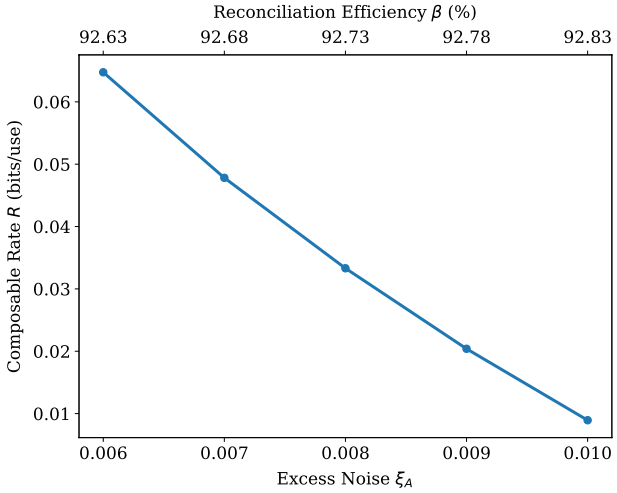

Figure 4. Composable secret key rate (bits/use) versus Alice's excess noise value ξ_A. Every point represents the average value of R, which is obtained after 5 simulations. Here we use $N = 5.88 \times 10^5$ and $n_{\text{bks}} = 100$. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant ($\mu_A = 60$, $\mu_B = 50$). The values of the reconciliation efficiency ζ are shown on the top axis. Other parameters are taken as in Table 2.

This library allows us to calibrate and optimize all the relevant parameters with direct benefits for experimental implementations.

Data availability

The datasets and the Python library used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Received: 14 October 2022; Accepted: 26 June 2023
Published online: 19 July 2023

References

1. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

3. Cao, Y. *et al.* The evolution of quantum key distribution networks: On the road to the Qinternet. *IEEE Commun. Surv. Tutor.* https://doi.org/10.1109/COMST.2022.3144219 (2022).
4. Park, J. The concept of transition in quantum mechanics. *Found. Phys.* **1**, 23–33 (1970).
5. Wootters, W. & Zurek, W. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
6. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India* 175–179 (1984).
7. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
8. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
9. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
10. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
11. Weedbrook, C. *et al.* Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
12. Usenko, V. C. & Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **92**, 062337 (2015).
13. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
14. Zhang, Y. *et al.* Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
15. Zhou, C. *et al.* Continuous-variable quantum key distribution with rateless reconciliation protocol. *Phys. Rev. Appl.* **12**, 054013 (2019).
16. Ruppert, L., Usenko, V. C. & Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **90**, 062310 (2014).
17. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).
18. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
19. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
20. Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C. & Braunstein, S. L. Continuous-variable quantum cryptography with untrusted relays. Preprint at http://arxiv.org/abs/1312.4104v1 (2013).
21. Pirandola, S. *et al.* High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **9**, 397–402 (2015).
22. Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M. & Liang, L.-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 042335 (2014).
23. Li, Z., Zhang, Y.-C., Xu, F., Peng, X. & Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052301 (2014).
24. Tian, Y. *et al.* Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. *Optica* **9**, 492–500 (2022).
25. Papanastasiou, P., Weedbrook, C. & Pirandola, S. Continuous-variable quantum key distribution in fast fading channels. *Phys. Rev. A* **97**, 032311 (2018).
26. Ottaviani, C., Lupo, C., Laurenza, R. & Pirandola, S. Modular network for high-rate quantum conferencing. *Commun. Phys.* **2**, 118 (2019).
27. Papanastasiou, P., Mountogiannakis, A. G. & Pirandola, S. *Supplementary Material: Composable Security of CV-MDI-QKD: Secret Key Rate and Data Processing*.
28. Ghalaii, M., Papanastasiou, P. & Pirandola, S. Composable end-to-end security of Gaussian quantum networks with untrusted nodes. http://arxiv.org/abs/2203.11969v1.
29. Liao, Q., Wang, Y., Huang, D. & Guo, Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express* **26**, 19907–19920 (2018).
30. Hajomer, A. A. E., Andersen, U. L. & Gehring, T. Real-world data encryption with continuous-variable measurement device-independent quantum key distribution. http://arxiv.org/abs/2303.01611.
31. Mountogiannakis, A. G., Papanastasiou, P., Braverman, B. & Pirandola, S. Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution. *Phys. Rev. Res.* **4**, 013099 (2022).
32. Mountogiannakis, A. G., Papanastasiou, P. & Pirandola, S. Data post-processing for the one-way heterodyne protocol under composable finite-size security. *Phys. Rev. A* **106**, 042606 (2022).
33. Papanastasiou, P., Ottaviani, C. & Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **96**, 042332 (2017).
34. Lupo, C., Ottaviani, C., Papanastasiou, P. & Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **97**, 052327 (2018).
35. Papanastasiou, P., Ottaviani, C. & Pirandola, S. Security of continuous-variable quantum key distribution against canonical attacks. *Int. Conf. Comput. Commun. Netw.* **2021**, 1–6. https://doi.org/10.1109/ICCCN52240.2021.9522349 (2021).
36. Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).
37. Renner, R. *Quantum Information Theory, Lecture Notes* (2013).
38. Cover, T. M. & Thomas, J. A. *Elements of Information Theory* (Wiley, 2012).
39. Pirandola, S. Composable security for continuous-variable quantum key distribution: Trust levels and practical key rates in wired and wireless. *Phys. Rev. Res.* **3**, 043014 (2021).
40. Tang, B., Liu, B., Zhai, Y., Wu, C. & Yu, W. High-speed and large-scale privacy amplification scheme for quantum key distribution. *Sci. Rep.* **9**, 15733 (2019).

Acknowledgements

A. M. was supported by the Engineering and Physical Science Research Council (EPSRC) via a Doctoral Training Partnership EP/R513386/1. S. P. was supported by the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No. 862644 (FET-OPEN project: Quantum readout techniques and technologies, QUARTET).

Author contributions

P.P. adapted the simulation steps and the composable theory proof to the CV-MDI-QKD setting. A.M. Created the simulation the code and the results and plots of this study. S.P. organized and supervised the previous tasks and proposed the main idea of this study. All participated equally in creating the document.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-023-37699-5.

Correspondence and requests for materials should be addressed to P.P.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.