UNIVERSITY of York

This is a repository copy of *Continuous-Variable Quantum Key Distribution with Composable Security and Tight Error Correction Bound for Constrained Devices*.

White Rose Research Online URL for this paper: <u>https://eprints.whiterose.ac.uk/225430/</u>

# **Preprint:**

Papanastasiou, Panagiotis, Ottaviani, Carlo orcid.org/0000-0002-0032-3999, Pirandola, Stefano orcid.org/0000-0001-6165-5615 et al. (2 more authors) (2025) Continuous-Variable Quantum Key Distribution with Composable Security and Tight Error Correction Bound for Constrained Devices. [Preprint]

# Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

# Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



eprints@whiterose.ac.uk https://eprints.whiterose.ac.uk/

# arXiv:2504.06384v1 [quant-ph] 8 Apr 2025

# Continuous-Variable Quantum Key Distribution with Composable Security and Tight Error Correction Bound for Constrained Devices

Panagiotis Papanastasiou<sup>1,3</sup>, Carlo Ottaviani<sup>2,3</sup>, Stefano Pirandola<sup>2</sup>, Poonam Yadav<sup>2</sup>, and Marco Lucamarini<sup>1,3</sup>

<sup>1</sup>School of Physics, Engineering & Technology, University of York, YO10 5FT York, U.K.

<sup>2</sup>Department of Computer Science, University of York, YO10 5GH York, U.K. and

<sup>3</sup> York Centre for Quantum Technologies, University of York, YO10 5FT York, U.K.

Constrained devices, such as smart sensors, wearable devices, and Internet of Things nodes, are increasingly prevalent in society and rely on secure communications to function properly. These devices often operate autonomously, exchanging sensitive data or commands over short distances, such as within a room, house, or warehouse. In this context, continuous-variable quantum key distribution (CV-QKD) offers the highest secure key rate and the greatest versatility for integration into existing infrastructure. A key challenge in this setting, where devices have limited storage and processing capacity, is obtaining a realistic and tight estimate of the CV-QKD secure key rate within a composable security framework, with error correction (EC) consuming most of the storage and computational power. To address this, we focus on low-density parity-check (LDPC) codes with non-binary alphabets, which optimise mutual information and are particularly suited for short-distance communications. We develop a security framework to derive finite-size secret keys near the optimal EC leakage limit and model the related memory requirements for the encoding process in one-way error correction. This analysis facilitates the practical deployment of CV-QKD, particularly in constrained devices with limited storage and computational resources.

# I. INTRODUCTION

Quantum key distribution (QKD) [1] allows two parties to establish a common secret key, which can later be used in symmetric cryptographic primitives. Its security relies on the fundamental principles of quantum physics rather than computational complexity conjectures [2– 5] and constitutes, along with post-quantum cryptography [6], the leading candidate for countering quantum threats, such as an eavesdropper equipped with a quantum computer.

Initially, QKD was developed for discrete-variable (DV) systems, which use discrete degrees of freedom, such as the polarization of the electromagnetic field. Later, protocols based on continuous degrees of freedom, such as the quadratures of the electromagnetic field, i.e., continuous-variable (CV) systems [7], emerged, offering high performance in the asymptotic regime and over short distances, as well as compatibility with existing technological infrastructure. Recent studies have advanced both the security [8, 9] and the experimental performance [10, 11] of CV-QKD, bringing it close to the repeaterless PLOB bound [12] and making it comparable to DV-QKD.

The most common and earliest CV-QKD protocols employ Gaussian modulation of coherent states (GMCS), utilising homodyne detection [13] or heterodyne detection [14] in direct or reverse reconciliation (RR) [15]. CV-QKD has also been extended to protocols using different frequencies (thermal states), two-way communication [16–20], and network settings [21–32]. There also have been considered schemes with post-selection [33–35] and discrete modulation [37–41].

In this study, we focus on the GMCS protocol, which is particularly effective in short- to moderate-loss regimes, and precisely quantify the demands of postprocessing, especially error correction (EC), which can significantly impact the protocol's performance [42–49]. More specifically, we adopt the analysis from Ref. [9], which imposes strict bounds on the secret key length, to evaluate the protocol's performance under composable security with finite-size effects.

Furthermore, we adapt the tight one-way EC bound from Ref. [50] to non-binary low-density parity-check (LDPC) codes [51–53] to compute secret key rates with near-optimal performance. This allows us to estimate the storage requirements of the encoder during EC. Although this represents only half of the complete EC procedure, it provides valuable insight in scenarios where there is a strong asymmetry in computational resources between the CV-QKD transmitter and receiver. Specifically, the transmitter, which performs the encoding, can be lightweight and agile, while the receiver, responsible for decoding, may be bulkier and better suited for computationally intensive tasks. This scenario arises in networks of small sensors transmitting to a central processing unit, as seen in smart home sensors, wearable devices, IoT systems [54–59], or drones [60]. These devices play a crucial role in modern society, supporting the technological infrastructure by enabling automation, real-time monitoring, and critical decision making. As they become increasingly integrated into daily life, cyber threats targeting them pose significant risks to public safety. We suggest feasible cases where CV-QKD can be used to safeguard from these threats.

In Sec. II A, we introduce the composable secret key length bound. In Sec. II B, we derive the information leakage in one-way EC for nonbinary LDPC codes. In Sec. II C, we present the final formula for the secret key rate, and in Sec. III, we introduce one-way EC with nonbinary LDPC codes. Finally, we link these results to an estimate of the storage required for the encoding of the EC procedure to achieve near-optimal performance.

# II. COMPOSABLE SECURITY RATE WITH TIGHT LEAKAGE BOUND

# A. Secret key length with composable terms

The secret-key length is upper-bounded by the following expression (see also Ref. [9, Eq. (36)])

$$s_n^{\epsilon_{\rm cor}+\epsilon_{\rm h}+\epsilon_{\rm s}} \le nR_{\infty} - \sqrt{n}\Delta_{\rm aep}^{\epsilon_{\rm s}}(h) + \theta,$$
 (1)

obtained assuming that the protocol did not abort, the extracted key is correct, with probability larger than  $1 - \epsilon_{\rm cor}$ , and secret with probability larger than  $1 - \epsilon_{\rm sec}$ . The  $\epsilon_{\rm sec} = \epsilon_{\rm s} + \epsilon_{\rm h}$ , where  $\epsilon_{\rm s}$  is the smoothing parameter and  $\epsilon_{\rm h}$  is the probability of failure of Privacy Amplification (PA). The asymptotic key-rate  $R_{\infty}$  in Eq. (1) is given by

$$R_{\infty} = H(\mathsf{k}) - \chi(\mathsf{k}:E) - n^{-1} \text{leak}_{\text{ec}}.$$
 (2)

The quantity  $\Delta_{aep}^{\epsilon_s}$ , given by the expression

$$\Delta_{\rm aep}^{\epsilon_{\rm s}}(h) \simeq 4\log_2\left(\sqrt{2^{hd}} + 2\right)\sqrt{\log_2(2/\epsilon_{\rm s}^2)},\qquad(3)$$

accounts for the penalty due to finite-size effects, while

$$\theta = \log_2(2\epsilon_{\rm h}^2\epsilon_{\rm cor}) \tag{4}$$

is the penalty paid for non-ideal verification and Privacy Amplification while n is the block size of the raw key after channel parameter estimation (PE) and leak<sub>ec</sub> is the error correction (EC) leakage.

The quantity H(k), in Eq. (2), is the Shannon entropy of the key variable k and  $\chi(k : E)$  is Eve's Holevo information. The key variable k takes values from the alphabet  $\mathcal{K} = \{0, 1, \ldots, 2^{hd} - 1\}$  for *d*-bit digitization of the normalized quadrature results, according to refs. [9, 47, 48]. In this description, the dummy variable  $h = \{1, 2\}$  distinguishes between homodyne (h = 1) and heterodyne detection (h = 2). More specifically, for heterodyne protocol, the digitized outcomes are in the vectorial form  $(k_q, k_p)$ , that can be concatenated as

$$\mathbf{k} = k_q 2^d + k_p, \tag{5}$$

without loss of any information because the mapping  $(k_q, k_p) \leftrightarrow \mathbf{k}$  is one-to-one, and with Shannon entropies related by the following mathematical expression  $H(\mathbf{k}) = 2H(k)$  (see Appendix A for details). For error correction the parties may now decide to use the vectorial form  $\{k_q^{(1)}, k_p^{(1)}, k_q^{(2)}, k_p^{(2)}, \dots, k_q^{(n)}, k_p^{(n)}\}$ . From here, we apply the procedure given in [9,

From here, we apply the procedure given in [9, Eq. (48)], to write Eq. (2) as

$$R_{\infty} = hH(k) - \chi(x:E) - n^{-1} \text{leak}_{\text{ec}}, \qquad (6)$$

where variable x is the continuous-variable version of k. Note that for the homodyne protocol k and k are equivalent forms of the key variable. The steps to obtain the Holevo bound for the RR protocol have been detailed in Ref. [9], hence we give only the final expression for the CM for the DR protocol in Appendix B.

We can now calculate the secret-key rate after parameter estimation, replacing in the Holevo bound the channel parameters with their worse-case scenario values for transmissivity  $\tau^{\epsilon_{pe}}$  and excess noise  $\xi^{\epsilon_{pe}}$ , obtaining the expression below

$$R^{\epsilon_{\rm pe}}_{\infty} = hH(k) - n^{-1} \text{leak}_{\rm ec} - \chi(x:E)|_{\tau^{\epsilon_{\rm pe}}, \xi^{\epsilon_{\rm pe}}}, \quad (7)$$

which can replace  $R_{\infty}$  in Eq. (1).

# B. Theoretical estimation of EC leakage

In case of one-way reconciliation, where low-density parity-check (LDPC) codes [51, 52] are used (see also Sec. III), the EC leakage term can be upper-bounded by the number of syndrome bits, given by

$$\operatorname{leak}_{\operatorname{ec}} \le \log_2 |\mathcal{M}|, \tag{8}$$

where  $\mathcal{M}$  is the alphabet of the syndrome strings. One may calculate the size of the alphabet  $|\mathcal{M}|$  via EC simulations, as done in Ref. [46] for asymptotic security analysis and in Refs. [28, 47, 48] for composable security analysis.

However, in a complete theoretical analysis, one may use the asymptotic bound (Slepian-Wolf coding [61]) stating that

$$\log_2 |\mathcal{M}| - nhH(k|y) \ge 0,\tag{9}$$

where H(k|y) is the conditional Shannon entropy of k conditioned on the continuous variable y of the other party. In fact, when considering finite-size effects one can use a more rigorous bound [50] providing a tighter estimate of the performance of information reconciliation. Such a bound is given by

$$\log_2 |\mathcal{M}| - nhH(k|y) - \sqrt{n\Delta_{\text{leak}}^{\epsilon_{\text{ec}}}(h)} \le \delta(n), \quad (10)$$

where

$$\Delta_{\text{leak}}^{\epsilon_{\text{ec}}}(h) = \sqrt{hV(k|y)}\Phi^{-1}(1-\epsilon_{\text{ec}})$$
(11)

with  $\Phi$  being the cumulative normal distribution. The right-hand side of Eq. (10) is given by

$$\delta(n) = \frac{1}{2}\log_2 hn + \mathcal{O}(1) \tag{12}$$

while the conditional entropy and the conditional entropy variance are given by

$$H(k|y) = \mathbb{E}\left[-\log_2 p(k|y)\right], \ V(k|y) = \operatorname{Var}\left[-\log_2 p(k|y)\right].$$
(13)

We now extend the calculation of Eq. (10) to nonbinary alphabets (i.e., d > 1) using the expression of p(k|y) given in Eq. (68) of Ref.[47]. That allows the parties to achieve higher mutual information at short distances, because when d increases, the entropy of digitized variables approach that of their continuous-variable counterpart.

To minimize the probability of errors in the final key string, the parties apply the verification step: one party sends the syndrome and a hash of the raw key  $k^{hn}$  with collision probability  $\epsilon_{\rm cor}$ . The other party will compare this with the hash of the guessed string  $\hat{k}^{hn}$  and, if they match, then the protocol can continue with probability  $p_{\rm ec}$  and conditional probability of error  $P[\hat{k}^n \neq k^n | p_{\rm ec}] \leq \epsilon_{\rm cor}$ , otherwise they will abort. This means that

$$P[\hat{k}^n \neq k^n] = 1 - p_{\text{ec}} \left[ 1 - P[\hat{k}^n \neq k^n | p_{\text{ec}}] \right]$$
$$\leq 1 - p_{\text{ec}} \left[ 1 - \epsilon_{\text{cor}} \right] := \epsilon_{\text{ec}} \qquad (14)$$

We then replace Eq. (10) into Eq. (7) and obtain

$$R_{\infty}^{\epsilon_{\rm pe}+\epsilon_{\rm ec}} = hI(k:y) - \chi(x:E)_{\tau^{\epsilon_{\rm pe}},\xi^{\epsilon_{\rm pe}}} - \frac{\Delta_{\rm leak}^{\epsilon_{\rm ec}}(h)}{\sqrt{n}}$$
(15)

where the  $\mathcal{O}\left(\frac{\log_2 n}{n}\right)$  terms are omitted and I(k:y) = H(k) - H(k|y) is the mutual information between k and y.

We now can group the mutual information and  $\Delta_{\text{leak}}$  term in Eq. (15), to define the quantities

$$\zeta_{\text{leak}} hI(k:y) := hI(k:y) - \Delta_{\text{leak}}^{\epsilon_{\text{ec}}}(h) / \sqrt{n}$$
(16)

and

$$\zeta_{\text{digit}} := hI(k:y)/I(x:y), \qquad (17)$$

where the mutual information I(x : y) refers to the Gaussian variables as described in [9, Eq. (83)].

Then using Eq. (16) and (17) into Eq. (15), we can rewrite the asymptotic rate as follows

$$R_{\infty}^{\epsilon_{\rm pe}+\epsilon_{\rm ec}} = \zeta I\left(x:y\right) - \chi(x:E)_{\tau^{\epsilon_{\rm pe}},\xi^{\epsilon_{\rm pe}}},\qquad(18)$$

where

$$\zeta = \zeta_{\text{digit}} \zeta_{\text{leak}}.$$
 (19)

# C. Secret key rate with tight estimation of EC performance

Replacing  $R_{\infty}^{\epsilon_{\text{pe}}}$  of Eq. (7) with  $R_{\infty}^{\epsilon_{\text{pe}}+\epsilon_{\text{ec}}}$  from either Eq. (15) or (18), we obtain

$$s_n^{\epsilon}/n \le r_n^{\epsilon} := R_{\infty}^{\epsilon_{\mathrm{pe}}+\epsilon_{\mathrm{ec}}} - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}(h)}{\sqrt{n}} + \frac{\theta}{n} - \mathcal{O}(\log_2(n)/n).$$

This gives the highest number of bits per signal that can be extracted with security  $\epsilon$  and a tight estimation of EC leakage, and it can be used to compute the final secret key rate,

$$R := p_{\rm ec}(n/N)r_n^{\epsilon},\tag{20}$$

where N is the number of the total signals in the block.

# III. LDPC CODES FOR NON-BINARY VARIABLES AND STORAGE REQUIREMENTS

In this section we connect practical schemes of EC with (nonbinary) LDPC codes with the previous theoretical bound of Eq. (10). This will further allow us to connect the secret key performance with predictions for the storage requirements of the devices that handle the EC procedure and especially the encoding phase. The encoder obtains a string  $k^{hn}$  and computes the syndrome  $\mathbf{H}k^{hn} = s^r$  where **H** is a  $r \times Dn$  parity-check matrix. In general, every element of the matrix belongs to the Galois field  $k = \mathcal{GF} = 0, 1, \dots, 2^d - 1$ . More specifically, the matrix is a representation of a Tanner graph with hn message nodes and r parity check nodes. When a message  $i = 1, \ldots, hn$  is included in a parity check  $j = 1, \ldots, r$ , there is an edge between the corresponding message node and parity-check node while the entry  $H_{ii}$ of the associated parity-check matrix in this intersection is chosen randomly from  $k = 1, \ldots, 2^d - 1$ .

One then may calculate the corresponding code rate

$$R_{\rm code} = \frac{hn - r}{hn} = 1 - R_{\rm synd} \tag{21}$$

The code is usually designed by assuming that each message participates in  $d_v$  (column weight) checks and every check contains  $d_c$  (row weight) messages. Then the number of edges must follow  $nd_v = rd_c$  (for sparse matrices, i.e.,  $d_v < d_c \ll r < Dn$ ). Therefore, by replacing  $r := hn\frac{d_v}{d}$  in Eq. (21), we obtain the design rate

$$R_{\rm design} = 1 - \frac{d_{\rm v}}{d_{\rm c}},\tag{22}$$

where we usually set  $d_v = 2$  as it gives the best performance in decoding. This means that the design code rates for regular LDPCs are given by

$$R_{\rm design} = 0.333, 0.5, 0.6, 0.666, 0.714, 0.75, \dots, 0.777, 0.8\dots$$

On the other hand, irregular LDPC codes can be designed where the column and row weights are not constant. Through the probability distributions of the weights, one defines their means  $\bar{d}_c$  and  $\bar{d}_v$ , respectively. Therefore, we have

$$R_{\rm design} = 1 - \frac{\bar{d}_{\rm v}}{\bar{d}_{\rm c}} \tag{23}$$

which allows for more flexible values than before. However, the performance of these codes is not particularly stable, i.e., different structures with the same  $R_{\text{design}}$  respond very differently in terms of correcting different levels of SNRs or in terms of probability of successful EC. Then from Eq. (8), we have that

$$\operatorname{leak}_{\operatorname{ec}} \le \log_2 |\mathcal{M}| = qr = hndR_{\operatorname{synd}}.$$
 (24)

One then may define a tight approximation for the optimal  $R_{\text{synd}}$  by Eq. (10), where

$$R_{\rm synd}^* = H(k|y)/d + \Delta_{\rm leak}^{\epsilon_{\rm ec}}(h)/(dh\sqrt{n}) + \delta(n)/(dhn).$$
(25)

$N(10^{5})$	$n(10^5)$	$R^*_{\rm code}$	$M^*_{\rm sparse}({\rm MB})$	$R_{\rm code}$	$M_{\rm sparse}({\rm MB})$
1	0.676	0.78	0.389	0.777	0.464
2	1.6	0.78	0.95	0.777	1.1
4	3.2	0.7949	2	0.8	2.3

TABLE I: We have chosen block sizes  $1 - 4 \times 10^5$  and found the associated  $R^*_{\text{code}}$  and  $M^*_{\text{sparse}}$  from Fig. 3. Then with the associated parameters, we have created parity-check matrices in the CSR format in Python with  $R_{\text{code}} \approx R^*_{\text{code}}$ , using regular non-binary LDPC codes. We finally calculated the actual storage needed for these cases and listed the results under the  $M_{\text{sparse}}$  column. These points have been depicted in the bottom panel of Fig. 3 with red ink following the predicted performance.

Then, one may find values for the  $R_{\rm code}$  that perform closely to the previous tight bound in terms of leakage (the corresponding structure of the codes needs to be optimized to achieve a certain probability of successful EC for a specific SNR). These are given through Eq. (21) by

$$R_{\rm code}^* = 1 - R_{\rm synd}^* \tag{26}$$

where by  $n \to \infty$  we arrive at the asymptotic expression

$$R_{\text{code}}^*|_{n \to \infty} = 1 - d^{-1}H(k|y).$$

Then, we can calculate the required memory to store the parity check matrix  $\mathbf{H}$  as

$$M_{\text{code}} := hn \times \log_2 |\mathcal{M}| = hndr = n^2 h^2 dR_{\text{synd}} \quad (27)$$

For example, for a protocol using homodyne detection, with a block size of the raw key equal to  $n = 10^5$  and  $dR^*_{\text{synd}} = 4 \times 0.667$  we obtain the parity-check matrix storage to be around 3.34 GBs while for a protocol using heterodyne detection it will be 4 times larger.

In the CRS format [49, Sec. 6.3], one will need  $\bar{d}_v \times hn \times d$  bits for storing the non-zero elements of the paritycheck matrix,  $\bar{d}_v \times hn \times \lceil \log_2(hn) \rceil$  bits for storing the column indices, and  $\left(\frac{\log_2|\mathcal{M}|}{d}+1\right) \times \lceil \log_2(\bar{d}_v hn) \rceil$  bits for the row pointers. Gathering all these terms, one may calculate the sparse matrix representation storage as

$$M_{\text{sparse}} = \bar{d}_{v} hnd + \bar{d}_{v} hn \lceil \log_{2}(hn) \rceil + (hnR_{\text{synd}} + 1) \lceil \log_{2}\left(\bar{d}_{v}hn\right) \rceil$$
(28)

For a protocol using homodyne detection with  $\bar{d}_v = 2$ ,  $nR_{\rm synd} = 0.667 \times 10^5$ , d = 4, and  $n = 10^5$ , we have that the sparse matrix storage will be approximately equal to 0.67 MB while for a protocol using heterodyne detection 2 times larger.

Note here that Eqs. (29) and (30) calculate the practical storage associated with the parity-check matrix of a code with rate  $R_{\text{code}} = 1 - R_{\text{synd}}$ . Theoretically, one may compute tight bounds for these quantities through

ξ	0.01
$\eta_d$	0.8
$u_{\rm el}$	0.01
au	$10^{-\mathrm{dB}/10}$
$\epsilon_{\rm h}$	$2^{-32}$
$\epsilon_{\rm cor}$	$2^{-32}$
$\epsilon_{\rm pe}$	$2^{-32}$
$\epsilon_{\rm s}$	$2^{-32}$

TABLE II: Here we present the common parameters used to plot the secret key rate of Eqs. (20) in all figures.

Eq. (10) and obtain an approximate prediction for them. Thus, we may write

$$M_{\rm code}^* = (hn)^2 dR_{\rm synd}^* \tag{29}$$

$$M_{\text{sparse}}^* = \bar{d}_{v} hn(q + \lceil \log_2(hn) \rceil) + (hnR_{\text{synd}}^* + 1) \lceil \log_2(\bar{d}_{v}hn) \rceil$$
(30)

The most accurate estimation for these quantities is to simulate the results, i.e., create parity check matrices for different block sizes (see Table I) with similar parameters and store them in CRS format. We have done this using the EC encoding script developed in the simulation library for the GMCS protocol with heterodyne detection [62]. This may give different results due to a particular choice of the type of variables in the script or other software parameters used to describe the parity check matrix in the specific format that may add an overhead, which is not included in Eq. (30). Although this formula cannot give very accurate results, it is quite simple and can provide key insights for the encoding function.

## IV. RESULTS

In this section, we connect the previous theoretical results with the practical implications for the protocol operations and especially the data post-processing part. We focus on the protocol with homodyne detection. In Fig. 1, we plot the secret key rate of Eq. (20) against the loss in dB, where we have optimized over V and the PE ratio 1 - (n/N). We also plot the changes in terms of  $\zeta$  or leakage and the associated SNR for the optimized rate value. These correspond to the values of V and n presented in the same figure. The rest of the parameters used for this plot are summarized in Table II.

In Fig. 2, we plot the corresponding RR secret key rate, where it is clear that the performance has increased in terms of loss tolerance. This is expected due to the 3 dB loss limit of the direct reconciliation protocol in the asymptotic regime, which degrades when one assumes finite-size effects. Clearly, the RR protocol is robust against higher losses (see Fig. 11) especially when one uses a large block size. This is not achievable by the DR protocol. We also include plots for the correspond-



FIG. 1: In the top panel, we plot the secret key rate of Eq. (20) (black line) of the Gaussian modulation protocol with coherent states and homodyne detection in direct reconciliation against the loss in dB. We have optimized over the Gaussian modulation variance V (grey thin line) and the PE ratio of sacrificed channel uses. We have assumed  $N = 2 \times 10^5$ , d = 4, and  $p_{ec} = 0.9$ . The rest of the parameters are given in Table II. We plot also the corresponding SNR (gray dasheddotted line). In the second panel, we plot the corresponding values of the reconciliation efficiency  $\zeta$  (black line), which follow the same pattern as the Gaussian modulation variance values. However, we can see that for a constant value of Vthe reconciliation efficiency increases linearly with the loss in dB. Subsequently, we plot the associated  $R^*_{\rm code}$  (black dashdotted line). In the third panel, we plot the corresponding block size (gray dashed line) after optimizing the number of sacrificed channel uses during PE. We plot also the associated leakage (black line). In the last panel, we plot Eq. (30) for the corresponding values of the secret key rate and loss in dB.

ing  $R^*_{\text{code}}$  that is needed to achieve the specific performance for the given SNR and, similarly, the corresponding  $M^*_{\text{sparse}}$ .

By contrast, in Figs. 3 and 4, we plot the secret key rates for the DR and RR protocols, respectively, against the block size. We set the loss to 0.02 dB and choose the other parameters in the same way. We mainly observe that the DR protocol is advantageous in this regime of losses: we can achieve high rates by using smaller bock-



FIG. 2: In the top panel, we plot the secret key rate of Eq. (20) (black line) of the Gaussian modulation protocol with coherent states and homodyne detection in RR against the loss in dB. The rest of the parameters and settings have been considered the same as in Fig. 1. Here we observe a better performance in terms of tolerable loss compared with the direct reconciliation protocol in Fig. 1. This is expected due to the known 3 dB loss limit of the DR protocol in the ideal asymptotic regime which decreases even more when one considers finite-size effects and channel noise.

size. Here, we consider a moderate block size roughly  $10^5 - 10^6$ . This is because we would like to investigate regimes of operation where the high-rate performance in long distance is not a priority. These regimes are described by fast sharing of small keys assuming the smallest requirements of hardware equipment, either because of space constraints or cost-effective implementations. For example, this can be described by QKD implementations over networks of small sensor devices, Internet of Things (IoT) nodes, wearable devices, or drones operating inside a building, outside, connected with fiber or with free-space links [63, 64].

Apart from the limitations due to the communication links such as the noise and the losses, one should take into account as a priority the hardware requirements of the classical data post-processing. This can be done effectively, in the finite-size regime, using composable terms connected to every performance aspect. Therefore, we



FIG. 3: In the first panel, we plot the secret key rate of Eq. (20) (black line) for the Gaussian modulation protocol with coherent states and homodyne detection in direct reconciliation against N. We set dB = 0.02. We have optimized over V and n/N. The rest of the parameters, settings and lines are the same as in Fig. 1. With red ink, we plot the points included in Table I of the corresponding  $M_{\text{sparse}}$ , i.e., the actual storage needed for these sparse matrices after creating them in CRS format using the GMCS simulation library in [62].

combine tools developed in previous studies to characterize the requirements in storage during one-way EC and especially the encoding part which is executed by one of the parties. Note that the DR protocol is advantageous in this regime because it can give higher rates for smaller block size and can support lightweight and agile transmitters responsible for the EC encoding while the bulkier receivers can be better suited for computationally intensive tasks such as the EC decoding in an assymetric scenario: for example, a network of small sensors transmitting to a central processing unit.

The syndrome creation, i.e., encoding process, is the less difficult part of the one-way EC with LDPC codes. In contrast, the decoding process is rather demanding and can be effectively handled by larger stations rather than a constrained device. In such an asymmetric scenario in terms of computational power, for an appropriate loss tolerance, the party operating through the constrained



FIG. 4: In the first panel, we plot the secret key rate of Eq. (20) (black line) for the Gaussian modulation protocol with coherent states and homodyne detection in RR against N. We have set the loss to 0.02 dB. The rest of the parameters, settings and lines are the same as in Fig. 1. We observe here, that we need a larger block size in order to obtain a secret key rate compared to the DR protocol in Fig. 3. This is because the DR protocol offers higher rates than the RR protocol in the low loss regime.

device is the transmitter and also the encoder during EC. This describes the DR protocol. In this setting, one can exploit the trade-off between limitations in robustness against losses with the mitigation of computationalpower requirements.

Then, one still needs to check the compatibility with storage requirements for the parity check matrix as the main aspect of the EC encoding procedure. In particular, the amount of leakage calculated in Eq. (10) that achieves a specific performance in terms of secret key rate in Eqs. (20) can be mapped to the associated LDPC code rate in Eq. (26) and, in turn, to the dimensions of the related parity-check matrices that give the associated leakage. Then we can predict the related storage requirements by Eq. (30).

In Fig. 3, we can see the behaviour of  $M^*_{\text{sparse}}$  against the block-size. For specific block sizes, we have created the parity check matrices for the corresponding encoding process in EC and stored them in sparse form. The details of these parity check matrices are presented in Table I while, for the sake of comparison, the storage for each matrix is described by the red points in the bottom panel. We see that the results are very close to the predicted values for  $M_{\rm sparse}$ . Finally, in Appendix C, we examine the behaviour of the protocols in terms of losses when one considers different values for block size, successful EC probability, and digitization.

# V. CONCLUSION

Small device detectors and IoT device networks play a crucial role in modern society, enabling real-time monitoring, automation, and seamless connectivity across various sectors, including healthcare, smart cities, industrial automation, and environmental monitoring. Their ability to collect and process vast amounts of data enhances efficiency, reduces human intervention, and supports decision-making in critical applications. However, as these devices become deeply integrated into daily life, their security is of paramount importance. Cyber threats targeting IoT networks can lead to privacy breaches, unauthorized surveillance, or even large-scale disruptions in infrastructure, posing risks to public safety and economic stability.

It is paramount then to search for robust solutions against cyber threats for these devices: one of the main candidates is QKD offering an information-theoretic security advantage. Since these devices operate at short distances, such as within a room, a house, or a warehouse, CV-QKD which has an advantage in this regime and especially the GMCS protocols can provide higher secret key rates. In particular, by using non-binary LDPC codes in a practical implementation of such a protocol, the parties exploit the high mutual information between their continuous variables.

However, this is quite challenging due to the increased requirements of the data post-processing stage in computational power or storage, not to mention implementing a QKD protocol on such constrained devices in the first place. Therefore, in order to investigate the performance under those circumstances, one needs to develop rigorous theoretical tools. Here we have combined a composable security proof taking into account the main stages of the data post-processing of a QKD protocol with a tight bound for EC adapting it to the non-binary LDPC regime.

This allows us to predict optimal secret key performance in terms of reconciliation efficiency and leakage and match this performance to operational code rates for given signal-to-noise ratios and error correction success probabilities. Based on this, we developed a tool that models the encoding storage requirements for a nonbinary LDPC EC associated with the given secret key rate performance.

We combined a composable security framework for the secret key rate of the GMCS protocols with a finite-size tight bound for one-way EC leakage of non-binary LDPC dependent on the given SNR and successful EC probability. Through this tool, one can theoretically calculate the code rate for close to optimum performance and the dimensions of the associated parity-check matrix. In turn, one may calculate the storage requirements of the EC encoding process, which is crucial, for example, for the implementation of CV-QKD with constraint devices. Note here that optimum leakage means optimum value for storage.

# CODE AND NUMERICAL IMPLEMENTATION

The majority of the numerical results and plots in this manuscript were produced using custom Python code developed for the calculation of tight leakage bounds in the context of non-binary LDPC codes. This code represents a central technical contribution of the present work and is publicly available at: eqclabs/tight\_bound\_leakage. The three red data points in Fig. 3 were obtained using an independent implementation, as referenced in the main text. All simulations were performed on nodes of the Viking High Performance Computing cluster at the University of York, equipped with a 2-core AMD EPYC3 7643 processor and 12 GB of memory. All repositories are released under the Apache License 2.0 and include documentation to support reproducibility.

# ACKNOWLEDGEMENTS

P.P. thanks Juan Vieira Giestinhas and Alex Mountogiannakis for insightful discussions, and the high performance compute facility, the Viking cluster, of the University of York. This work is supported, in part, by EPSRC and DSIT TMF-uplift: CHEDDAR: Communications Hub For Empowering Distributed ClouD Computing Applications And Research (EP/X040518/l), and (EP/Y037421/l). S.P. acknowledges support from EP-SRC and UKRI, via the Integrated Quantum Networks (IQN) Research Hub (EP/Z533208/1).

 C. H. Bennett and G. Brassard, Quantum cryptog- raphy: Public key distribution and coin tossing, Int. Conf. on Computers, Systems & Signal Processing, Ban- galore, India, Dec 9-12, 1984. Also at Theor. Comput. Sci. 560, 7 (2014).

- [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum Cryptography, Rev. Mod. Phys. 74, 145 (2002).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M.

- [4] 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. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in quantum cryptography*, Adv. Opt. Photon. **12**, 1012 (2020).
- [5] V. C. Usenko, A. Acín, R. Alléaume, U. L. Andersen, E. Diamanti, T. Gehring, A. A.E. Hajomer, F. Kanitschar, C. Pacher, S. Pirandola, V. Pruneri, *Continuous-variable quantum communication*, arXiv:2501.12801v1.
- [6] Y. Liu and D. Moody, Post-quantum cryptography and the quantum future of cybersecurity, Phys. Rev. Applied 21, 040501 (2024).
- [7] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, Rev. Mod. Phys. 84, 621 (2012).
- [8] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduc- tion, Phys. Rev. Lett. 118, 200501 (2017).
- [9] S. Pirandola and P. Papanastasiou, *Improved composable key rates for CV-QKD*, Phys. Rev. Research 6, 023321 (2024).
- [10] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, et al., *Continuous-variable QKD over 50km commercial fiber*, Quantum Sci. Technol. 4, 035006 (2019).
- [11] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, *High key rate continuous-variable quan*tum key distirbution with a real local oscillator, Opt. Express 26, 2794 (2018).
- [12] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, Fundamental Limits of Repeaterless Quantum Communications, Nature Comm. 8, 15043 (2017).
- [13] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. 88, 057902 (2002).
- [14] 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).
- [15] F. Grosshans and P. Grangier, Reverse reconciliation protocols for quantum cryptography with continuous variables, arXiv preprint quant-ph/0204127 (2002).
- [16] R. Filip, Continuous-variable quantum key distribution with noisy coherent states, Phys. Rev. A 77, 022310 (2008).
- [17] S. Pirandola, S. Mancini, S. Lloyd, S. L. Braunstein, Continuous Variable Quantum Cryptography using Two-Way Quantum Communication, Nat. Phys. 4, 726 (2008).
- [18] C. Weedbrook, C. Ottaviani, S. Pirandola, *Two-way quantum cryptography at different wavelengths*, Phys. Rev. A 89, 012309 (2014).
- [19] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Gaussian one-way thermal quantum cryptography with finitesize effects, Phys. Rev. A 98, 032314 (2018).
- [20] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, *Terahertz quantum cryptography*, arXiv preprint quantph/1805.03514v1 (2018).
- [21] S. Pirandola, C. Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen and Ulrik L. An-

dersen, *High-rate quantum cryptography in untrusted networks*, Nature Photon. **9**, 397 (2015). See also preprint arXiv:1312.4104 (2013).

- [22] Z. Li, Y. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-Variable Measurement-Device- Independent Quantum Key Distribution, Phys. Rev. A 89, 052301 (2014).
- [23] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration, Phys. Rev. A 91, 022320 (2015).
- [24] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Finitesize analysis of measurement-device- independent quantum cryptography with continuous variables, Phys. Rev. A 96, 042332 (2017).
- [25] X. Zhang, Y.-C. Zhang, Y. Zhao, X. Wang, S. Yu, H. Guo, *Finite-size analysis of continuous-variable measurement-device-independent quantum key distri- bu*tion, Phys. Rev. A **96**, 042334 (2017).
- [26] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **120**, 220505 (2018).
- [27] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, *Continuous-variable measurement-deviceindependent quantum key distribution: Composable security against coherent attacks*, Phys. Rev. A **97**, 052327 (2018).
- [28] P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, *Composable security of CV-MDI-QKD with secret* key rate and data processing, Sci Rep 13, 11636 (2023).
- [29] A. I. Fletcher, C. Harney, M. Ghalaii, P. Papanastasiou, A. Mountogiannakis, G. Spedalieri, A. A. E. Hajomer, T. Gehring, and S. Pirandola, An Overview of CV-MDI-QKD, arXiv:2501.09818v1.
- [30] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, Comm. Phys. 2(1), 118 (2019). See also High-rate secure quantum conferencing, preprint arXiv:1709.06988 (2017).
- [31] P. Papanastasiou, C. Weedbrook, and S. Pirandola, Continuous-variable quantum key distribution in fast fading channels, Phys. Rev. A 97, 032311 (2018).
- [32] M. Ghalaii, P. Papanastasiou, and Stefano Pirandola, Composable end-to-end security of Gaussian quantum networks with untrusted relays, npj Quantum Information 8, 105 (2022).
- [33] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, *Experimental* demonstration of post-selection-based continuous- variable quantum key distribution in the presence of Gaussian noise, Phys. Rev. A 76, 030303(R) (2007).
- [34] K. N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, and S. Pirandola, Long-distance continuousvariable measurement-device-independent quantum key distribution with postselection, Phys. Rev. Research 2, 033424 (2020).
- [35] N. Hosseinidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, *Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection*, Phys. Rev. A **101**, 052335 (2020).
- [36] A. Leverrier and P. Grangier, Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, Phys. Rev. A 83, 042312 (2011).

- [37] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermalloss channels, Phys. Rev. A 98, 012340 (2018).
- [38] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic security of continuous-variable quantum key distribution with a discrete modulation, preprint arXiv:1902.01317 (2019).
- [39] P. Papanastasiou and S. Pirandola, Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks, Phys. Rev. Research 3, 013047 (2021).
- [40] S. Bäuml, C. Pascual-García, V. Wright, O. Fawzi, A. Acín, Security of discrete-modulated continuous-variable quantum key distribution, Quantum 8, 1418 (2024).
- [41] A.A.E. Hajomer, F. Kanitschar, N. Jain, M. Hentschel, R. Zhang, N. Lütkenhaus, U.L. Andersen, C. Pacher, T. Gehring, Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography, arXiv:2410.13702v1.
- [42] X. Wang, Y. Zhang, S. Yu, and H. Guo, High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code, Sci. Rep. 8, 10543 (2018).
- [43] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, *Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography*, npj Quantum Information 4, 21 (2017).
- [44] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental demonstration of long*distance continuous-variable quantum key distribution, Nat. Photon. 7, 378, (2013).
- [45] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. 6, 19201 (2016).
- [46] C. Pacher, J. Martinez-Mateo, J. Duhme, T. Gehring, and F. Furrer, Information Reconciliation for Continuous-Variable Quantum Key Distribution using Non-Binary Low-Density Parity-Check Codes, arXiv:1602.09140.
- [47] A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution, Phys. Rev. Research 4, 013099 (2022).
- [48] Alexander G. Mountogiannakis, Panagiotis Papanastasiou, and Stefano Pirandola, *Data postprocessing for the* one-way heterodyne protocol under composable finite-size security, Phys. Rev. A **106**, 042606 (2022).
- [49] W. Weerasinghe, Practical, High-Speed, Gaussian Modulated Coherent State Continuous Variable Quantum Key Distribution with Real-Time Post Processing, PhD Thesis, University of Cambridge (2024).
- [50] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, Fundamental finite key limits for one-way information reconciliation in quantum key distribution, Quantum Inf Process 16, 280 (2017).
- [51] D. J. C. Mackay, Good error-correcting codes based on very sparse matrices, IEEE Trans. Inform. Theory 45, 399–431 (1999).
- [52] M. C. Davey and D. MacKay, *Low-density parity check codes over GF(q)*, IEEE Communications Letters 2, 165–167 (1998).
- [53] J. Martinez-Mateo and D. Elkouss, Efficient Reconciliation of Continuous Variable Quantum Key Distribution

with Multiplicatively Repeated Non-Binary LDPC Codes, arXiv:2501.11009v1.

- [54] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey, J. Netw. Comput. Appl. 88, 10–28 (2017).
- [55] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, Securing the Future Internet of Things with Post-Quantum Cryptography, Security and Privacy 5(2), e200 (2022).
- [56] A. Shafique, S. A. A. Naqvi, A. Raza, M. Ghalaii, P. Papanastasiou, J. McCann, Q. H. Abbasi, and M. A. Imran, A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks, Scientific Reports 14, 31054 (2024).
- [57] E. Zadobrischi, The Concept regarding Vehicular Communications Based on Visible Light Communication and the IoT, Electronics 26, 1359 (2023).
- [58] M. Asif, W. U. Khan, H. M. R. Afzal, J. Nebhen, I. Ullah, A. U. Rehman, M. K. A. Kabar, *Reduced-Complexity LDPC Decoding for Next-Generation IoT Networks*, Wireless Communications and Mobile Computing, 2029560, (2021).
- [59] J. Tang, H. Wen, H. -H. Song, L. Jiao and K. Zeng, Sharing Secrets via Wireless Broadcasting: A New Efficient Physical Layer Group Secret Key Generation for Multiple IoT Devices, IEEE Internet of Things Journal 9, 15228-15239 (2022).
- [60] X. Tian, R. Yang, H. Liu, P. Fan, J. Zhang, C. Gu, M. Chen, M. Hu, F. Lu et al., Experimental Demonstration of Drone-Based Quantum Key Distribution Phys. Rev. Lett. 133, 200801 (2024).
- [61] D. S. Slepian and J. K. Wolf, Noiseless Coding of Correlated Information Sources, IEEE Trans. Inf. Theory 19, 471–480 (1973).
- [62] github.com/softquanta/homCVQKD
- [63] O. Elmabrok and M. Razavi, Wireless quantum key distribution in indoor environments, J. Opt. Soc. Am. B 35, 197-207 (2018).
- [64] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Research 3, 013279, (2021).

## Appendix A: Virtual concatenation

After digitization, one may apply the concatenation step useful only on the protocols using heterodyne detection. This is a virtual step that results in a common description of the GMCS protocols using either homodyne or heterodyne detection. This is summarised by

$$\mathbf{k} = k \tag{A1}$$

for the case of homodyne detection and

$$\mathbf{k} = k_q 2^d + k_p \tag{A2}$$

for the case of heterodyne detection. We observe that

$$p(\mathbf{k}) = p(k_q, k_p) = p(k_q)p(k_p), \quad k_q = k_p = k$$
  
$$\Rightarrow \quad p(k_q) = p(k_p) \tag{A3}$$





FIG. 5: We present similar plots to Fig. 1. All the parameters are the same, apart from  $p_{\rm ec} = 0.4$ . We observe that the secret key rate is lower than the corresponding one in the previous figure. However, the achievable loss has been slightly improved. We see also very similar performance in terms of the other parameters  $\beta$ ,  $R_{\rm code}^*$ , leakage, and  $M_{\rm sparse}$ .

FIG. 7: We present similar plots to Fig. 1. All the parameters are the same, apart from assuming a doubled value for block size  $N = 4 \times 10^5$ . We observe that the secret key rate takes higher values and the achievable loss has been significantly increased. The leakage level and n has been increased in the same manner (almost doubled) and similarly  $M_{\rm sparse}^*$ . The other parameters have remained in similar levels as before.





FIG. 6: We present similar plots to Fig. 2. All the parameters are the same, apart from  $p_{\rm ec} = 0.4$ . We observe similar behaviour for the rate as in Fig. 5.

FIG. 8: We present similar plots to Fig. 2. All the parameters are the same, apart from assuming a doubled value for block size  $N = 4 \times 10^5$ . We observe similar behaviour for the rate as in Fig. 7.



FIG. 9: We present similar plots to Fig. 1. All the parameters are the same, apart from assuming a digitization of d = 6. We observe that the secret key rate takes higher values and the achievable loss has been significantly increased. The improvement is better compared to increasing the block size as in the case of Fig. 7. By increasing the digitization, we allow the choice for larger optimal values for the Gaussian modulation variance which leads to higher SNRs and very high reconciliation efficiency.

Therefore,

$$H(\mathbf{k}) = H(k_q, k_p) = -\sum_{k_q, k_p} p(k_q, k_p) \log_2 p(k_q, k_p)$$
  
=  $-\sum_{k_q, k_p} p(k_q, k_p) \log_2 p(k_q) - \sum_{k_q, k_p} p(k_q, k_p) \log_2 p(k_p)$   
=  $-\sum_{k_q} p(k_q) \log_2 p(k_q) - \sum_{k_p} p(k_p) \log_2 p(k_p)$   
=  $-\sum_k p(k) \log_2 p(k) - \sum_k p(k) \log_2 p(k) = 2H(k).$   
(A4)

# Appendix B: Conditional Covariance Matrices for Direct Reconciliation

For the case of direct reconciliation and homodyne detection, the associated conditional CM is given by

$$\mathbf{V}_{E|x} = \begin{pmatrix} \operatorname{diag}\{\phi_0, \phi\} & \psi \mathbf{Z} \\ \psi \mathbf{Z} & \omega \mathbf{I} \end{pmatrix}, \quad (B1)$$



FIG. 10: We present similar plots to Fig. 2. All the parameters are the same, apart from assuming a digitization of q = 6. We observe similar behaviour for the rate as in Fig. 9.



FIG. 11: We present similar plots to Fig. 4. All the parameters are the same, apart from dB = 2. We observe that the RR protocol can operate in higher losses given an increased block size above  $4 \times 10^5$ .

where

$$\phi_0 = \tau \omega + (1 - \tau), \tag{B2}$$

$$\phi = \tau \omega + (1 - \tau)(V + 1), \tag{B3}$$

$$\psi = \sqrt{\tau(\omega^2 - 1)},\tag{B4}$$

where  $\omega$  is Eve's noise variance, V is the Gaussian classical modulation,  $\tau$  is the transmissivity of the channel. For the case of direct reconciliation and heterodyne detection, the associated conditional CM is given by

$$\mathbf{V}_{E|x} = \begin{pmatrix} \phi_0 \mathbf{I} & \psi \mathbf{Z} \\ \psi \mathbf{Z} & \omega \mathbf{I} \end{pmatrix}.$$
 (B5)

# Appendix C: Other results

We now investigate the behaviour of the protocols, in terms of the secret key rate against losses, assuming either a different successful EC probability, block size, or digitization parameter. For example, we see that changing the  $p_{\rm ec}$  from 0.9 to 0.4 affects the performance of both reconciliation directions: in Figs. 5 and 6, we see a considerable drop in terms of the rate but a minimal improvement in loss tolerance compared to Figs. 1 and 2, respectively.

In Figs. 7 and 8, we doubled the block size to  $4 \times 10^5$  compared to Figs. 1 and 2, respectively. Here we see an

improvement in the performance and loss tolerance: we obtain rates almost in the 3/2 amount or more of loss in both cases compared to Figs. 1 and 2, respectively. However, the amount of  $M^*_{\rm sparse}$  required is almost doubled as expected by the linear dependence of  $M^*_{\rm sparse}$  on block size.

When one increases the digitization parameter (here from d = 4 to 6), the performance also increases along with the loss tolerance. We show this tendency in Figs. 9 and 10 for both protocols, respectively. In particular, the tolerable loss is larger than the double in Figs. 1 and 2. In addition, the leakage and  $M_{\text{sparse}}^*$  increase slightly. This means that by increasing the digitization parameter, we can obtain similar performance as by increasing the block size avoiding large storage requirements.

Increasing the digitization means that  $\zeta_{\text{digit}}$  approaches 1. In other words, the parties can exploit almost the whole amount of the CV mutual information available to them. This is why CV are advantageous especially for small loss. However, the terms  $\Delta_{\text{aep}}^{\epsilon_{\text{s}}}$  and  $\Delta_{\text{leak}}^{\epsilon_{\text{cc}}}$  (also expressed through  $\zeta_{\text{leak}}$ ) increase with larger digitization parameters. This will lead to a saturation point for the secret key rate performance and loss tolerance.

Finally, in Fig. 11, we plot the secret key rate for the RR protocol against the block size for dB = 2. We observe that the RR protocol can tolerate higher losses.