Received: 8 April 2024 | Revised: 29 May 2024 | Accepted: 3 July 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12103

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Classical channel bandwidth requirements in continuous variable quantum key distribution systems

Margarida Almeida[1,2] | Daniel Pereira[1,2] | Armando N. Pinto[1,2] | Nuno A. Silva[1]

[1]Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, Aveiro, Portugal

[2]Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, Aveiro, Portugal

Correspondence
Margarida Almeida.
Email: mralmeida@ua.pt

Present address
Daniel Pereira, Austrian Institute of Technology, Giefinggasse, Austria

Funding information
European Defence Industrial Development Programme, Grant/Award Number: Project DISCRETION (S12.858093); Fundação para a Ciência e a Tecnologia, Grant/Award Numbers: PhD Grant SFRH/BD/139867/2018, PhD Grant UI/BD/153377/2022, Project QuantaGenomics (QuantERA/0001/2021), Project QuantumPrime (PTDC/EEI-TEL/8017/2020)

Abstract

The reconciliation method for continuous variable quantum key distribution systems is usually chosen based on its reconciliation efficiency. Nonetheless, one must also consider the requirements of each reconciliation method in terms of the amount of information transmitted on the classical channel. Such may limit the achievable key rates. For instance, multidimensional reconciliation of dimension 8 demands a classical channel bandwidth 43 times greater than that of the quantum channel baud rate. Decreasing the dimension to 4 halves the required bandwidth, allowing for higher quantum channel baud rates and higher key rates for shorter transmission distances, despite the lesser reconciliation performance.

KEYWORDS
quantum communication, quantum cryptography

1 | INTRODUCTION

Continuous variables quantum key distribution (CV-QKD) allows the distribution of symmetric keys between two distant parties [1]. To achieve that, the transmitter and the receiver use a quantum channel to exchange coherent states, and an authenticated classical channel for the post-processing procedure to generate a secret key. The classical channel plays a pivotal role in the information reconciliation process that significantly impacts the achievable key rate [2–4]. Moreover, different reconciliation methods require different information to be shared, imposing minimum bandwidth requirements on the classical channel. The cost-effective and widespread deployment of CV-QKD systems using existing optical networks poses unique challenges, being imperative to account for the limitations of the existing infrastructure. By properly maximising the key rates and comparing different reconciliation methods considering their requirements in terms of the classical channel's bandwidth, we can pave the way for the widespread use of CV-QKD technology.

CV-QKD can be implemented using both Gaussian modulation (GM) and discrete modulation (DM) [5, 6]. GM is theoretically optimal [7], but poses practical challenges, due to the finite extinction ratio of the electro–optic modulators [8]. DM provides a simpler practical implementation, at the cost of lower key rates [9, 10]. Nevertheless, the use of higher-order constellations opens the door to key rates of the order of the ones obtained with GM [11–14]. For instance, constellations such as M-symbol Quadrature and Amplitude Modulation (M-QAM) and M-symbol Amplitude and Phase Shift Keying (M-APSK) have been studied, with both modulation formats showing performances close to that of GM [11, 12]. Moreover, 64- [15], 256- [13, 15], and 1024-QAM [16] and 128-APSK [14] have been experimentally implemented in CV-QKD systems, and their performance was assessed in terms of

secret key rate. Nonetheless, those experimental validations do not consider the required classical channel bandwidth for post-processing of the secret keys, namely information reconciliation and privacy amplification. This disregards the effect that the information reconciliation method may have on the extraction key rate, especially when the modulation variance is chosen without taking it into account [4].

The reconciliation method first proposed for low-cardinality DM-CV-QKD systems [17] was a variation of the sign reconciliation (SR) method applied to GM [2, 18]. For GM-CV-QKD systems, multidimensional reconciliation or slice reconciliation are usually applied [2, 19–23]. Multidimensional reconciliation is based on a transformation step, while slice reconciliation is based on a quantisation step [24]. Multidimensional reconciliation is usually considered for low signal-to-noise ratios (SNRs) since the lossless rotation makes the method more efficient [19, 25, 26]. Slice reconciliation allows the distillation of more than 1 bit per symbol per quadrature measured, showing higher efficiency for SNRs higher than 0.5 [19, 22]. Different reconciliation methods demand different information to be exchanged in the classical channel to assist the reconciliation step. Nonetheless, the bandwidth of optical links comes with an associated cost, and the use of already deployed optical links for CV-QKD may impose limitations in terms of available bandwidth. Therefore, it is of utmost importance to minimise the bandwidth requirements over the classical channel for a cost-effective implementation of a CV-QKD network. In that sense, it is fundamental to quantify the bandwidth consumed by all post-processing steps for key extraction.

We study the bandwidth requirements of each post-processing step in a DM-CV-QKD system regarding the communication on the classical channel, considering both sign and multidimensional reconciliation. The link direction from Bob to Alice requires more information flow due to the exchange of the side information for reconciliation, imposing minimum bandwidth requirements on the classical channel. This minimum bandwidth requirement is proportional to the baud rate on the quantum channel. Multidimensional reconciliation of dimension 8 demands the highest bandwidth on the classical channel for the same quantum channel baud rate, while SR allows the lowest. Accounting for both the reconciliation efficiency and with the frame error rate (FER) in the system, a constrained bandwidth on the classical channel results in a higher key rate for multidimensional reconciliation with dimension 4 at low transmission distances than multidimensional reconciliation with dimension 8, by allowing for a higher baud rate in the quantum channel, and a higher number of states to be considered for the finite-size effects, despite showing lower performance in terms of reconciliation.

The paper is organised as follows. Section 2 contains the theoretical description of a CV-QKD system. In Section 3 both sign and multidimensional reconciliation are briefly described, and the information to be exchanged in the classical channel is enumerated. Section 4 accounts for the analysis of the extraction key rate and of the requirements in the classical and quantum channels. Finally, in Section 5 we conclude our analysis.

2 | THEORETICAL DESCRIPTION

A CV-QKD system can be divided into two main parts: the physical layer and the post-processing layer. In the physical layer, Alice and Bob exchange quantum states. The post-processing layer comprises the parameter estimation, information reconciliation, and privacy amplification steps.

When considering DM, the quantum states exchanged between Alice and Bob are given by coherent states following a specific geometric and probabilistic shaping. Here, we consider the 64-QAM constellation following the Boltzmann–Maxwell distribution for probabilistic shaping, since it closely approximates the performance of GM in terms of secret key rate [11, 15, 27]. The 64-QAM constellation has eight amplitude levels in each quadrature, defined by $|\alpha_{k,l}| = (k + il)\sqrt{(V_A)/\left(2\sum_{k,l}P_{k,l}\sqrt{k^2+l^2}\right)}$ with k, l equidistant values between -1 and 1; V_A, the modulation variance of Alice's states; and $P_{k,l} = \exp\left(-\nu\left(k^2+l^2\right)\right)\Big/\sum_{k,l}P_{k,l}$, the probability of the states considering the Boltzmann–Maxwell distribution. In this work, the ν parameter is optimised through the maximisation of the secret key rate. Despite the ν parameter being optimised in the results presented, the details of the optimisation and its analysis will not be presented in the current work.

The length of the key that Alice and Bob can extract from the quantum states exchanged between them is measured by the extraction key rate, K, which is given by the following equation:

$$K = \frac{n}{N}(1 - \mathrm{FER})\left[\beta I_{BA} - \chi_{BE} - \Delta(n)\right], \tag{1}$$

where I_{BA} is the mutual information between Bob and Alice computed considering DM [28], and χ_{BE} is the Holevo bound between Bob and Eve. Reverse reconciliation is considered, since it allows the extraction of secret keys for higher transmission distances. For collective Gaussian attacks, the Holevo bound between Bob and Eve [29] is computed by properly defining the Z parameter, which is given by the following equation [11]:

$$Z = 2\sqrt{T_{\mathrm{ch}}}\,\mathrm{Tr}\left(\tau^{1/2}\hat{a}\tau^{1/2}\hat{a}^{\dagger}\right) - \sqrt{2T_{\mathrm{ch}}\xi W}, \tag{2}$$

where T_{ch} is the channel's transmission, ξ is the excess noise, $\mathrm{Tr}(\cdot)$ is the trace of $\cdot$, $\tau = \sum_{k,l}P_{k,l}|\alpha_{k,l}\rangle\langle\alpha_{k,l}|$ is the density matrix describing the average state sent by Alice, $W = \sum_{k,l}P_{k,l}\left(\langle\alpha_{k,l}|\hat{a}_{\tau}\dagger\hat{a}_{\tau}|\alpha_{k,l}\rangle - |\langle\alpha_{k,l}|\hat{a}_{\tau}|\alpha_{k,l}\rangle|^2\right)$, $\hat{a}_{\tau} = \tau^{1/2}\hat{a}\tau^{-1/2}$, and $\hat{a}$ and $\hat{a}^{\dagger}$ are the annihilation and creation operators on Alice's system, respectively. The $\Delta(n)$ parameter accounts for the finite-size effects of exchanging only a finite number of states between Alice and Bob, which is given by the following equation [30]:

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PA}), \tag{3}$$

where $\bar{\epsilon}$ is a *smoothing* parameter and ϵ_{PA} is the failure probability of the privacy amplification procedure [30]. Due to the finite-size effects, the value of T_{ch} and ξ is changed to their lower and upper bounds with a probability of at least $1 - \epsilon_{PE}$, respectively [30]. Moreover, the β parameter corresponding to the reconciliation efficiency guarantees that the system only extracts the allowed number of bits . Additionally, related to the information reconciliation step is the FER, which gives the ratio of uncorrected frames after the information reconciliation step. Finally, the ratio $\frac{n}{N}$ accounts for the fact that only n of the N states shared between Alice and Bob are used to extract the final key. The remaining $N - n$ states are used to estimate the channel's transmission and excess noise. To account for the finite-size effects on the computation of the extraction key rate, given by Equation (1), we take into account the close approximation of the 64-QAM modulation format to GM [16]. Moreover, we compute β, I_{BA} and χ_{BE} in Equation (1) considering that Bob uses heterodyne detection [31], thus being able to measure both quadratures of the received signal.

3 | POST-PROCESSING AND BANDWIDTH REQUIREMENTS

We compute the extraction key rate assuming that the reconciliation efficiency is given by $\beta = \frac{R}{C}$, where R is the code rate for reconciliation and C is the classical capacity of the quantum channel [25]. Since Bob uses heterodyne detection, $C = \frac{1}{2}I_{BA}$, and, as such, $\beta = \frac{2R}{I_{BA}}$. Once again, note that, by using heterodyne detection, Bob can measure both quadratures of the receiving signal. The FER is only obtained after the information reconciliation method has been applied. Nonetheless, we can estimate the FER of the system through the knowledge of its SNR, given by $\frac{\eta T_{\text{ch}} V_A}{\eta T_{\text{ch}}\xi + 2 + 2\xi_{\text{thermal}}}$ for heterodyne detection, where η is the detection's efficiency and ξ_{thermal} is the thermal noise intrinsic to the receiver's setup. The FER estimation was provided by simulating the CV-QKD system for different SNR values. For the information reconciliation step we employed multidimensional and SR, focusing on the low SNR regime. Moreover, we considered the use of multi-edge type low-density parity check (LDPC) codes, which are a generalisation of irregular LDPC codes and approximate the Shannon's limit for low SNRs [25]. Through the FER estimation, one can find the trade-off between the modulation variance, the reconciliation efficiency, and the FER of the system, such that the extraction key rate is maximised [4].

In SR [17], Bob's binary sequence $\mathbf{u}^{\text{SR}}$ is given by $\mathbf{u}^{\text{SR}} = \frac{\mathbf{y}}{|\mathbf{y}|}$, where $\mathbf{y}$ are Bob's measurements of Alice's sent states [17]. The binary sequence for the raw binary key, $\mathbf{m}^{\text{SR}}$, is such that $m_i^{\text{SR}} = 1$ if $u_i^{\text{SR}} = 1$ and $m_i^{\text{SR}} = 0$ if $u_i^{\text{SR}} = -1$, with i the indices of the sequences. Bob then sends the side information $\mathbf{t} = |\mathbf{y}|$ to Alice through the classical channel [17]. From the knowledge of the side information $\mathbf{t}$, Alice computes the noisy version of $\mathbf{u}^{\text{SR}}$, $\mathbf{v}^{\text{SR}} = \frac{\mathbf{x}}{|\mathbf{x}|}\mathbf{t}$, where $\mathbf{x}$ are Alice's sent states. For SR, the log-likelihood of the priori message probabilities of the sum–product algorithm is given by $r_i^{\text{SR}} = 2v_i^{\text{SR}}/\sigma^2$, where $\sigma^2 = \frac{\eta T_{\text{ch}}}{2}\xi + 1 + \xi_{\text{thermal}}$ is the noise associated to Bob's measured states.

In multidimensional reconciliation, Alice and Bob first divide their non-uniform and, approximately, Gaussian distributed variables, $\mathbf{x}$ and $\mathbf{y}$, prior to demodulation, into consecutive d dimensional vectors, $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_d)$, respectively. Here, d is the dimension of multidimensional reconciliation, which can only take the values of 1, 2, 4 and 8, as shown in ref. [20]. Usually, d is chosen to be eight for improved performances [20, 24]. Bob then generates a binary random sequence, $\mathbf{m}^{\text{MR}} = (m_1^{\text{MR}}, m_2^{\text{MR}}, \ldots, m_d^{\text{MR}})$, and his d-dimensional sequence $\mathbf{u}^{\text{MR}} = (u_1^{\text{MR}}, u_2^{\text{MR}}, \ldots, u_d^{\text{MR}})$ by doing $\mathbf{u}^{\text{MR}} = \frac{1}{\sqrt{d}}\left[(-1)^{m_1^{\text{MR}}}, (-1)^{m_2^{\text{MR}}}, \ldots, (-1)^{m_d^{\text{MR}}}\right]$. Bob then maps $\mathbf{y}$ to $\mathbf{u}^{\text{MR}}$ by the operation $M_R(\mathbf{y}, \mathbf{u}^{\text{MR}})\mathbf{y} = \mathbf{u}^{\text{MR}}$, where $M_R(\mathbf{y}, \mathbf{u}^{\text{MR}})$ is a rotation matrix obtained by $M_R(\mathbf{y}, \mathbf{u}^{\text{MR}}) = \sum_{i=1}^{d}\alpha_i(\mathbf{y}, \mathbf{u}^{\text{MR}})\mathbf{Q}_i$, where $\alpha_i(\mathbf{y}, \mathbf{u}^{\text{MR}})$ are the coordinates of $\mathbf{u}^{\text{MR}}$ on the orthogonal basis $[\mathbf{Q}_1\mathbf{y}, \mathbf{Q}_2\mathbf{y}, \ldots, \mathbf{Q}_d\mathbf{y}]$, and $\{\mathbf{Q}_1, \mathbf{Q}_2, \ldots, \mathbf{Q}_d\}$ is a non-unique family of d orthogonal matrices of $\mathbb{R}^{d\times d}$ such that $\mathbf{Q}_1 = \mathbb{I}_d$, and for $i, j > 1$ the anti-commutator of $\mathbf{Q}_i$ and $\mathbf{Q}_j$ is $-\delta_{i,j}\mathbb{I}_d$ [17]. The $\mathbf{Q}_i$ matrices used are the ones available in ref. [17]. $\alpha_i(\mathbf{y}, \mathbf{u}^{\text{MR}})$ can be obtained by doing $\alpha_i(\mathbf{y}, \mathbf{u}^{\text{MR}}) = \left[\mathbf{T}^{-1}\mathbf{u}^{\text{MR}}\right]_i$, where $\mathbf{T}$ is a matrix whose columns are given by $[\mathbf{Q}_1 \cdot \mathbf{y}, \mathbf{Q}_2 \cdot \mathbf{y}, \ldots, \mathbf{Q}_d \cdot \mathbf{y}]$. Finally, Bob sends $M_R(\mathbf{y}, \mathbf{u}^{\text{MR}})$ to Alice, who is now able to compute the noisy version of $\mathbf{u}^{\text{MR}}$, $\mathbf{v}^{\text{MR}}$, by doing $\mathbf{v}^{\text{MR}} = M_R(\mathbf{y}, \mathbf{u}^{\text{MR}})\mathbf{x}$. In the case of multidimensional reconciliation, the log likelihood of the priori message probabilities of the sum–product algorithm is given by the following equation [24]:

$$r_i^{\text{MR}} = -\frac{d+1}{2}\log\left[\frac{d + \left(v_i^{\text{MR}} - 1\right)^2}{d + \left(v_i^{\text{MR}} + 1\right)^2}\right]. \tag{4}$$

Through reconciliation, Alice's goal is to obtain the best estimate of the binary random sequence $\mathbf{m}^{\text{SR}}$, $\hat{\mathbf{m}}$SR, for SR and $\mathbf{m}^{\text{MR}}$, $\hat{\mathbf{m}}$MR, for multidimensional reconciliation, known only by Bob.

Assuming that the post-processing of the raw data for key extraction functions in real-time, the bandwidth of the classical channel must be at least sufficient to assure the classical communication for post-processing. The amount of data required to be exchanged through the classical channel during post-processing is directly proportional to the baud rate of the quantum channel. Depending on the quantum channel's baud rate, the bit rate required in the classical channel for real-time operation may limit the wide-scale deployment of CV-QKD systems. Since different information reconciliation methods have different demands in terms of information to be exchanged in the classical channel, it is important to

acknowledge the bandwidth requirements on the classical channel for the different reconciliation methods and understand how these requirements may affect the extraction key rate of CV-QKD systems. The bit rate unit is considered to characterise the classical channel instead of the baud rate unit for simplicity. Moreover, we consider the classical channel to be bidirectional.

The information exchanged between Alice and Bob in the classical channel can be divided in three types: (1) real data, such as the extraction key rate; (2) binary data, such as the syndromes for the reconciliation step; and (3) the identifiers of the information transmitted and the acknowledgements of the received data. Here, we assume that the real data (1) is composed of 64 bits per real value, except for the real data for the side information, which is composed of 16 bits per real value. The binary data (2) is composed of 1 bit per binary value. The identifiers and the acknowledgements (3) give information of the specific data that was exchanged, and as such we assume them to be composed of 32 bits. We could assume the identifiers to not be transmitted and the acknowledgments of receipt to be composed by only 1 bit. However, considering both to be exchanged using 32 bits has an insignificant effect on the bandwidth demand, consuming no more than 0.03% of the total bandwidth demand, and allows for a better practical implementation. Moreover, we consider that during two stages of the operating time, Alice and Bob are not sharing any states, as Bob uses this time to estimate his receiver's thermal and shot noise [32]. In the remaining third stage of the operating time, half of the exchanged states is used to estimate the parameters of the channel, namely, the channel's transmission and the excess noise, while the other half is used for key extraction. For simplification purposes, we assume that each of these stages takes one third of the operation time. The use of a locally generated local oscillator allows the estimation of the shot and thermal noises while being shielded to shot-noise calibration attacks under the trusted-noise model [33].

Regarding the finite-size effects, we define N as the number of states exchanged between Alice and Bob for parameter estimation and key extraction, meaning that keys are extracted for each 3N states exchanged between Alice and Bob. The information exchanged during parameter estimation, information reconciliation, and privacy amplification is discriminated in Table 1 for the communication between Alice and Bob and in Table 2 for the communication between Bob and Alice.

During parameter estimation, Bob sends to Alice the position of the states used to estimate the receiver's noise, thermal noise, and shot noise. Therefore, Bob only needs to inform Alice of the starting positions of the respective measurements for each 3N states that Alice transmits to Bob through the quantum channel. Both positions are given by a real value composed of 64 bits, thus consuming a bit rate on the classical channel of $2 \cdot 64 \frac{B_{QC}}{3N} = 128 \frac{B_{QC}}{3N}$ bit/s, where B_{QC} is the baud rate of the quantum channel. Note that each set of 3N states exchanged between Alice and Bob in the quantum channel is exchanged at a rate of $\frac{B_{QC}}{3N}$. Moreover, for each 3N states transmitted in the quantum channel, Bob sends through the classical channel one identifier regarding the position of the states used to estimate the receiver's noise. This identifier is composed of 32 bits, consuming $32 \frac{B_{QC}}{3N}$ bit/s. Alice acknowledges this information by sending a message of receipt composed of 32 bits each 3N states transmitted in the quantum channel, $32 \frac{B_{QC}}{3N}$ bit/s.

TABLE 1 Information exchanged from Alice to Bob during parameter estimation, information reconciliation and privacy amplification.

Parameter estimation
Acknowledgement of receipt of the position of the states used to estimate the receiver's noise: $32 \frac{B_{QC}}{3N}$ bit/s
Position of the states used for parameter estimation: $\frac{B_{QC}}{3}$ bit/s
Identifier for the position of the states used for parameter estimation: $32 \frac{B_{QC}}{3N}$ bit/s
Value of the states used for parameter estimation: $\log_2 M \cdot \frac{B_{QC}}{6}$ bit/s
Identifier for the value of the states used for parameter estimation: $32 \frac{B_{QC}}{3N}$ bit/s
Information reconciliation
Acknowledgement of receipt of the side information: $32 \frac{B_{QC}}{3N}$ bit/s both for multidimensional reconciliation and for sign reconciliation
Acknowledgement of receipt of the syndromes for the sum-product algorithm: $32 \frac{B_{QC}}{3L}$ bit/s
Information of corrected and uncorrected frames: $\frac{B_{QC}}{3L}$ bit/s
Identifier of the information of corrected and uncorrected frames: $32 \frac{B_{QC}}{3L}$ bit/s
Subset of the extracted key for comparison: $R_{\text{comp},IR}(1 - \text{FER}) \frac{B_{QC}}{3}$ bit/s
Identifier of the subset of the extracted key for comparison: $32 \frac{B_{QC}}{3N}$ bit/s
Acknowledgement of the receipt of the result of the comparison: $32 \frac{B_{QC}}{3N}$ bit/s
Frame error rate obtained during the information reconciliation: $64 \frac{B_{QC}}{3N}$ bit/s
Identifier of the frame error rate obtained during the information reconciliation: $32 \frac{B_{QC}}{3N}$ bit/s
Acknowledgement of the receipt of the estimation of the extraction key rate: $32 \frac{B_{QC}}{3N}$ bit/s
Privacy amplification
Seed for privacy amplification: $\frac{B_{QC}}{3} \cdot \left(1 + K \cdot \frac{N}{n(1-\text{FER})}\right) \cdot (1 - R_{\text{comp},IR}) \cdot (1 - \text{FER})$ bit/s
Identifier of the seed for privacy amplification: $32 \frac{B_{QC}}{3N}$ bit/s
Subset of the extracted key for comparison: $R_{\text{comp},PA} \cdot \frac{B_{QC}}{3} \cdot (1 - R_{\text{comp},IR}) \cdot K \cdot \frac{N}{n}$ bit/s
Identifier of the subset of the extracted key for comparison: $32 \frac{B_{QC}}{3N}$ bit/s
Acknowledgement of the receipt of the result of the comparison: $32 \frac{B_{QC}}{3N}$ bit/s

Abbreviations: 3N, number of states exchanged between Alice and Bob for receiver's noise estimation, channel's noise estimation and key extraction; B_{QC}, baud rate of the quantum channel; FER, frame error rate; L, length of the MET-LDPC code; M, number of points in the constellation; $R_{\text{comp},IR}$, rate of bits for comparison after information reconciliation; $R_{\text{comp},PA}$, rate of bits for comparison after privacy amplification.

TABLE 2 Information exchanged from Bob to Alice during parameter estimation, information reconciliation and privacy amplification.

Parameter estimation
Position of the states used to estimate the receiver's noise: $128\frac{B_{QC}}{3N}$ bit/s
Identifier of the position of the states used to estimate the receiver's noise: $32\frac{B_{QC}}{3N}$ bit/s
Acknowledgement of receipt for the position of the states used for parameter estimation: $32\frac{B_{QC}}{3N}$ bit/s
Acknowledgement of receipt for the value of the states used for parameter estimation: $32\frac{B_{QC}}{3N}$ bit/s
Information reconciliation
Side information: $16 \cdot d \cdot \frac{B_{QC}}{3}$ bit/s for multidimensional reconciliation and $16\frac{B_{QC}}{3}$ bit/s for sign reconciliation
Identifier of the side information: $32\frac{B_{QC}}{3N}$ bit/s both for multidimensional reconciliation and for sign reconciliation
Syndromes for the sum-product algorithm: $\frac{B_{QC}}{3} \cdot (1 - R)$ bit/s
Identifier of the syndromes for the sum-product algorithm: $32\frac{B_{QC}}{3L}$ bit/s
Acknowledgement of the receipt of the information of corrected and uncorrected frames: $32\frac{B_{QC}}{L}$ bit/s
Acknowledgement of the receipt of the subset of the extracted key for comparison: $32\frac{B_{QC}}{3N}$ bit/s
Result of the comparison: $\frac{B_{QC}}{3N}$ bit/s
Identifier of the result of the comparison: $32\frac{B_{QC}}{3N}$ bit/s
Acknowledgement of receipt of the frame error rate: $32\frac{B_{QC}}{3N}$ bit/s
Estimated extraction key rate: $64\frac{B_{QC}}{3N}$ bit/s
Identifier of the estimated extraction key rate: $32\frac{B_{QC}}{3N}$ bit/s
Privacy amplification
Acknowledgement of the receipt of the seed for privacy amplification: $32\frac{B_{QC}}{3N}$ bit/s
Acknowledgement of the receipt of the subset of the extracted key for comparison: $32\frac{B_{QC}}{3N}$ bit/s
Result of the comparison: $\frac{B_{QC}}{3N}$ bit/s
Identifier of the result of the comparison: $32\frac{B_{QC}}{3N}$ bit/s

Abbreviations: 3N, number of states exchanged between Alice and Bob for receiver's noise estimation, channel's noise estimation and key extraction; B_{QC}, baud rate of the quantum channel; d, dimension of multidimensional reconciliation; L, length of the MET-LDPC code; R, code rate of the MET-LDPC code.

For the estimation of the channel's noise, Alice sends to Bob the positions of the states to be used for parameter estimation and their respective value. The position of the states used for parameter estimation is given by a binary sequence with length N, thus consuming $N\frac{B_{QC}}{3N} = \frac{B_{QC}}{3}$ bit/s on the classical channel. Since, at Alice's side, the quantum symbols are noiseless, they can be represented by a binary string using, for example, Gray mapping. Therefore, Alice sends Bob the value of the $\frac{N}{2}$ symbols used for parameter estimation, consuming $\log_2 M \cdot \frac{N}{2} \cdot \frac{B_{QC}}{3N} = \log_2 M \cdot \frac{B_{QC}}{6}$ bit/s on the classical channel, where M is the number of positions in the constellation. Additionally, Alice sends to Bob the identifiers of the positions of the states to be used for parameter estimation, consuming $32\frac{B_{QC}}{3N}$ bit/s, and the identifier of their respective value, also consuming $32\frac{B_{QC}}{3N}$ bit/s. The acknowledgment of receipt provided by Bob consumes $32\frac{B_{QC}}{3N}$ bit/s for the positions of the states to be used for parameter estimation and $32\frac{B_{QC}}{3N}$ bit/s for their respective value.

The amount of data exchanged between Alice and Bob during information reconciliation depends on the chosen method. If multidimensional reconciliation is chosen, as side information Bob needs to send Alice a rotation matrix $M_R(\mathbf{y}, \mathbf{u}^{\mathrm{MR}})$, composed of d^2 real values, represented using 16 bits, per each d bits of data. The rate of bits considered for the information reconciliation step is $2\frac{N}{2}\frac{B_{QC}}{3N}$ bit/s, since $\frac{N}{2}$ of the symbols exchanged in the quantum channel proceed to the information reconciliation step, and each symbol is associated to 2 bits, due to the use of heterodyne detection. Therefore, for multidimensional reconciliation, the exchange of the side information from Bob to Alice consumes $16 \cdot \frac{d^2}{d} \cdot \frac{B_{QC}}{3} = 16 \cdot d \cdot \frac{B_{QC}}{3}$ bit/s, where d is the dimension of multidimensional reconciliation. If SR is used, Bob needs to send to Alice the vector $\mathbf{t}$ as side information, composed of one real value, represented using 16 bits, per bit of data, thus consuming $16\frac{B_{QC}}{3}$ bit/s. Since the side information uses the majority of the bit rate required for the classical channel, we consider each real value of $M_R(\mathbf{y}, \mathbf{u}^{\mathrm{MR}})$ and of $\mathbf{t}$ to be composed of only 16 bits. Tests using 64 and 16 bits showed no decrease in performance due to the decrease in the number of bits. In both cases, Bob also sends the identifier of the type of the information exchanged and Alice acknowledges the information received, both consuming $32\frac{B_{QC}}{3N}$ bit/s.

The remaining steps are similar in both multidimensional and SR. Bob needs to send to Alice the syndromes of his binary data given by $2(1 - R)$ times the symbols for key extraction $\left(\frac{B_{QC}}{6}\right)$, where the two accounts for heterodyne detection and R is the code rate of the MET-LDPC code, thus consuming $\left(\left(1 - R\right)\frac{B_{QC}}{3}\right)$. Moreover, per syndrome sent, Bob also sends an identifier message. Since Bob sends syndromes at a rate of $\frac{2B_{QC}}{6L} = \frac{B_{QC}}{3L}$, where L is the length of the MET-LDPC code, the identifier message for the syndromes consumes $32\frac{B_{QC}}{3L}$ from Bob to Alice. Alice responds with an acknowledgment of receipt, also consuming $32\frac{B_{QC}}{3L}$ bit/s. We assume that Alice sends to Bob the information of the corrected and uncorrected frames, using one bit of information per framer, consuming $\frac{B_{QC}}{3L}$ bit/s, and the respective identifier, consuming $32\frac{B_{QC}}{3L}$ bit/s, while Bob responds with the respective acknowledgment, consuming $32\frac{B_{QC}}{3L}$ bit/s.

After the reconciliation step has been implemented, Alice sends Bob a subset of the extracted key for comparison requiring $R_{\mathrm{comp},IR} \cdot \frac{B_{QC}}{3} \cdot (1 - \mathrm{FER})$ bit/s, where $R_{\mathrm{comp},IR}$ is the rate of bits for comparison after information reconciliation

and $\frac{B_{QC}}{3} \cdot (1 - \text{FER})$ is the bit rate corresponding to the reconciled key discarding the frames for which the reconciliation was unsuccessful. Alice also sends to Bob the respective identifier, consuming $32\frac{B_{QC}}{3N}$ bit/s, while Bob responds with the acknowledgment, consuming $32\frac{B_{QC}}{3N}$ bit/s. The data shared for comparison is discarded from the reconciled key that proceeds to privacy amplification. Moreover, Alice sends Bob the computed FER value, which is a real value represented using 64 bits, consuming $64\frac{B_{QC}}{3N}$ bit/s, alongside with the identifier, consuming $32\frac{B_{QC}}{3N}$ bit/s. Bob sends to Alice, the respective acknowledgment, consuming $32\frac{B_{QC}}{3N}$ bit/s. Considering the data for comparison, Bob sends Alice the result of the comparison using one bit per reconciled key, $\frac{B_{QC}}{3N}$ bit/s, and the extraction key rate value, which is a real value represented using 64 bits, thus consuming $64\frac{B_{QC}}{3N}$ bit/s. For both types of information, Bob sends an identifier consuming $32\frac{B_{QC}}{3N}$ bit/s for each. Alice acknowledges the receipt consuming $32\frac{B_{QC}}{3N}$ bit/s for both the acknowledgment of the result of the comparison and for the acknowledgment of the extraction key rate.

For privacy amplification, Alice must send a seed consuming $\frac{B_{QC}}{3} \cdot \left(1 + K \cdot \frac{N}{n(1-\text{FER})}\right) \cdot \left(1 - R_{\text{comp},IR}\right) \cdot (1 - \text{FER})$ bit/s, with $\frac{N}{n} = 2$. Note that the bit rate of the reconciled key prior to privacy amplification is $\frac{B_{QC}}{3} \cdot \left(1 - R_{\text{comp},IR}\right) \cdot (1 - \text{FER})$ bit/s, and that Equation (1) for K already accounts for the amount of bits discarded for parameter estimation and during information reconciliation corresponding to the unsuccessfully reconciled frames. Moreover, Alice sends Bob a subset of the extracted key consuming $\frac{B_{QC}}{3} \cdot R_{\text{comp},PA} \cdot \left(1 - R_{\text{comp},IR}\right) \cdot K \cdot \frac{N}{n}$, where $R_{\text{comp},PA}$ bit/s is the rate of bits for comparison after privacy amplification, while Bob informs Alice of the correctness of the subset, $\frac{B_{QC}}{3N}$ bit/s. Once again, during this process, for each of the three types of information, both the identifiers and the acknowledgments of receipt are exchanged, each consuming $32\frac{B_{QC}}{3N}$ bit/s.

In ref. [4], MET-LDPC codes with different code rates were considered alongside multidimensional reconciliation of dimension 8, showing the importance of accounting for the reconciliation step when maximizing the extraction key rate. With this, we maximize the extraction key rate considering both the reconciliation efficiency and the FER on the optimisation of the modulation variance. Here, we consider only a MET-LDPC code with code rate, R, of 0.1 [25], and length, L, of 20,000, as our primary focus is the comparison between different reconciliation methods regarding the information consumption on the classical channel, and not between the same reconciliation method for different code rates. A relatively small MET-LDPC matrix is considered due to a slow decoder. Comparing the bit rate demanded by the side information of each reconciliation method, multidimensional reconciliation demands d times more data to be exchanged than SR. Despite multidimensional reconciliation of dimension 8 achieving the best performance [20, 24], here dimension 2 and 4 will also be considered, due to the different requirements in terms of bit rate in the classical channel for the same parameters. Moreover, the number of states in the constellation, M, is 64, and the rate of bits for comparison after information reconciliation, $R_{\text{comp},IR}$, and after privacy amplification, $R_{\text{comp},PA}$, is 0.05.

4 | RESULTS AND DISCUSSION

In Figure 1 we present the amount of information exchanged from Alice to Bob and from Bob to Alice for each post processing step. This corresponds, for real time operation, to the minimum bandwidth requirement in both directions of the classical channel imposed by the post-processing steps. The results were obtained considering SR and multidimensional reconciliation of dimension 2, 4, and 8 and a baud rate on the quantum channel of 155 Mbaud. Moreover, in Figure 1, we assumed an extraction key rate of 1 bits/symbol and an FER of 0 to upper bound the information in the classical channel. The amount of information transmitted in the classical channel from Alice to Bob has a higher contribution of the parameter estimation step, followed by the privacy amplification step (Figure 1). This is due to the transmission of the states for parameter estimation and of the seed for privacy amplification. We assume Alice to send Bob the information for parameter

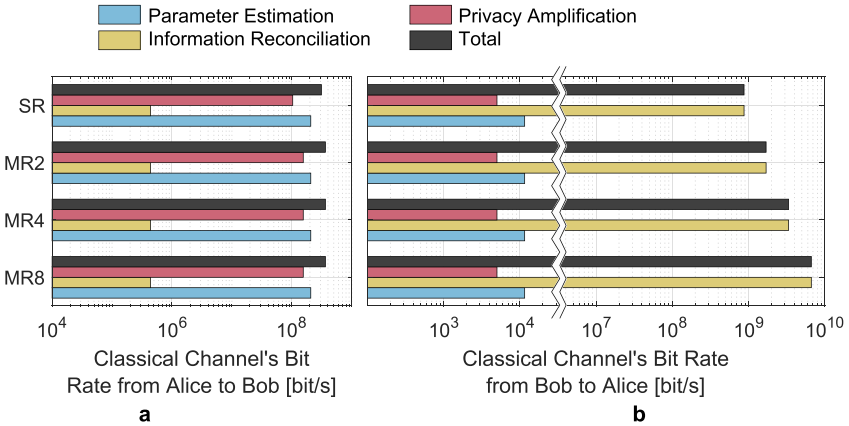

FIGURE 1 Amount of information exchanged (a) from Alice to Bob and (b) from Bob to Alice for each post processing step (parameter estimation, information reconciliation and privacy amplification) for a baud rate on the quantum channel of 155 Mbaud. This for an extraction key rate of 1 bit/symbol, a FER of 0, and a MET-LDPC code with code rate 0.1 and length 20,000 for the 64-QAM constellation.

estimation since, at Alice's side, the states can be represented by $\log_2 M$ bits, thus reducing the overall bit rate consumption. The demand of the information reconciliation step has an insignificant effect on the data transmitted from Alice to Bob.

From Bob to Alice, the contribution of parameter estimation and of privacy amplification is minor; both cases being independent of the information reconciliation method considered. In reverse reconciliation, Alice is responsible for the reconciliation of the raw data, using the side information sent by Bob, $\mathbf{t}$ for SR or $M_R(\mathbf{y}, \mathbf{u}^{\mathrm{MR}})$ for multidimensional reconciliation. The side information composes the majority of the data exchange demand, 94.7% of the bit rate for SR, and 97.3%, 98.6%, and 99.3% of the bit rate for multidimensional reconciliation of dimension 2, 4, and 8, respectively (Figure 1b). Due to the exchange of the side information, the direction of the link from Bob to Alice requires a bandwidth at least twice the bandwidth of the link from Alice to Bob.

In Figure 2 we present the bandwidth requirements on the classical channel as a function of the baud rate on the quantum channel, considering the most demanding link direction, that is, from Bob to Alice. The minimum bandwidth requirement on the classical channel is directly proportional to the bandwidth of the quantum channel. Due to the dimensions of the rotation matrix, $M_R(\mathbf{y}, \mathbf{u}^{\mathrm{MR}})$, multidimensional reconciliation demands classical links with higher bandwidths (Figures 1 and 2). The demand decreases with the decrease of the dimension d of multidimensional reconciliation. Nonetheless, decreasing the size of the rotation matrices results in more rotation matrices being exchanged. Therefore, the bandwidth required by multidimensional reconciliation for the side information sent from Bob to Alice, given by $16 \cdot d \cdot \frac{2B_{QC}}{6}$, is proportional to the dimension d of multidimensional reconciliation. For multidimensional reconciliation of dimension 2, 4, and 8, this term equals $16 \cdot 2 \cdot \frac{2B_{QC}}{6} \approx 10.67 B_{QC}$, $16 \cdot 4 \cdot \frac{2B_{QC}}{6} \approx 21.33 B_{QC}$, and $16 \cdot 8 \cdot \frac{2B_{QC}}{6} \approx 42.67 B_{QC}$, respectively. Theredfore, by decreasing the dimension of multidimensional reconciliation from 8 to 4 to 2, the information demand decreases to, approximately, one half and one quarter, respectively. Note that the scaling as $d/2$ when going from dimension 8 to 4 to 2 in multidimensional reconciliation is only approximate, due to the contribution of all the remaining terms. With this, considering all the information exchanged in the channel from Bob to Alice, the bandwidth required in the classical channel for multidimensional reconciliation with 2, 4, and 8 dimensions is 10.97, 21.63 and 42.97 times greater than the baud rate of the quantum channel, respectively (Figure 2). The use of SR allows the smallest bandwidth in the classical channel, 5.63 times the baud rate of the quantum channel, for real time operation (Figure 2). Note that, the constellation used, the values of the extraction key rate, the FER, and the number of exchanged states have an insignificant effect on the bandwidth requirements in the classical channel and on the allowed baud rate in the quantum channel.

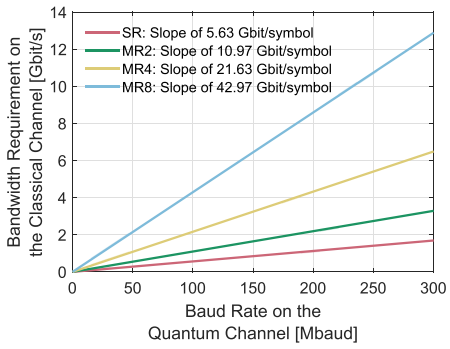

FIGURE 2 Bandwidth requirement on the classical channel as a function of the baud rate in the quantum channel, when considering sign reconciliation (SR) and multidimensional reconciliation of dimension 2, 4 and 8 (MR2, MR4, and MR8, respectively). This for an extraction key rate of 1 bit/symbol, a FER of 0, and a MET-LDPC code with code rate 0.1 and length 20,000 for the 64-QAM constellation.

In Figure 3 we present the FER as a function of the SNR and of the transmission distance obtained considering simulations of the physical layer of the CV-QKD system. For multidimensional reconciliation, the FER is not independent of the transmission distance (Figure 3). Note that, while for SR, Alice's noisy version of $\mathbf{u}^{\mathrm{SR}}$, $\mathbf{v}^{\mathrm{SR}}$, is proportional to the modulus of Bob's raw data, $|\mathbf{y}|$. For multidimensional reconciliation, Alice's noisy version of $\mathbf{u}^{\mathrm{MR}}$, $\mathbf{v}^{\mathrm{MR}}$, is proportional to Alice's raw data, $\mathbf{x}$. When increasing the transmission distance, to maintain the received SNR, an increase of the amplitude of Alice's states is required, then, for multidimensional reconciliation, Alice's noisy version of $\mathbf{u}^{\mathrm{MR}}$ is affected, thus impacting the FER on the system. Multidimensional reconciliation of dimension 8 can extract keys for smaller SNR values, except for low transmission distances, for which multidimensional reconciliation with dimension 4 shows higher performance. Fit curves were obtained to model the FER as a function of the SNR for each transmission distance considered for the simulations (Figure 3). From the fits computed with the data from the simulations, one can estimate the FER for different SNR and transmission distance pairs, and compute the respective extraction key rate.

For a fully CV-QKD system deployment in a real scenario, it is fundamental to compute the baud rate that can be used in the quantum channel, depending on the system's bandwidth limitations. In one hand, if the baud rate in the quantum channel is set too low, a needless decrease in performance will be observed in a real-time implementation. On the other hand, setting the baud rate too high, may require more time to process the data than the acquisition time, resulting in unused data and misleading extraction key rates. Moreover, for a cost-effective and wide deployment of CV-QKD systems in the field, it is important to better understand the reconciliation method that best fits the available equipment, especially for implementations using optical networks already deployed in the field, whose links and devices may have bandwidth limitations.

In Figure 4 the extraction key rate is presented as a function of the transmission distance for 1 Gbit/s of bandwidth in the classical channel (Figure 4a) and as a function of the bandwidth on the classical channel for 4 km (Figure 4b). In Figure 4c we present the respective FER. The allowed baud

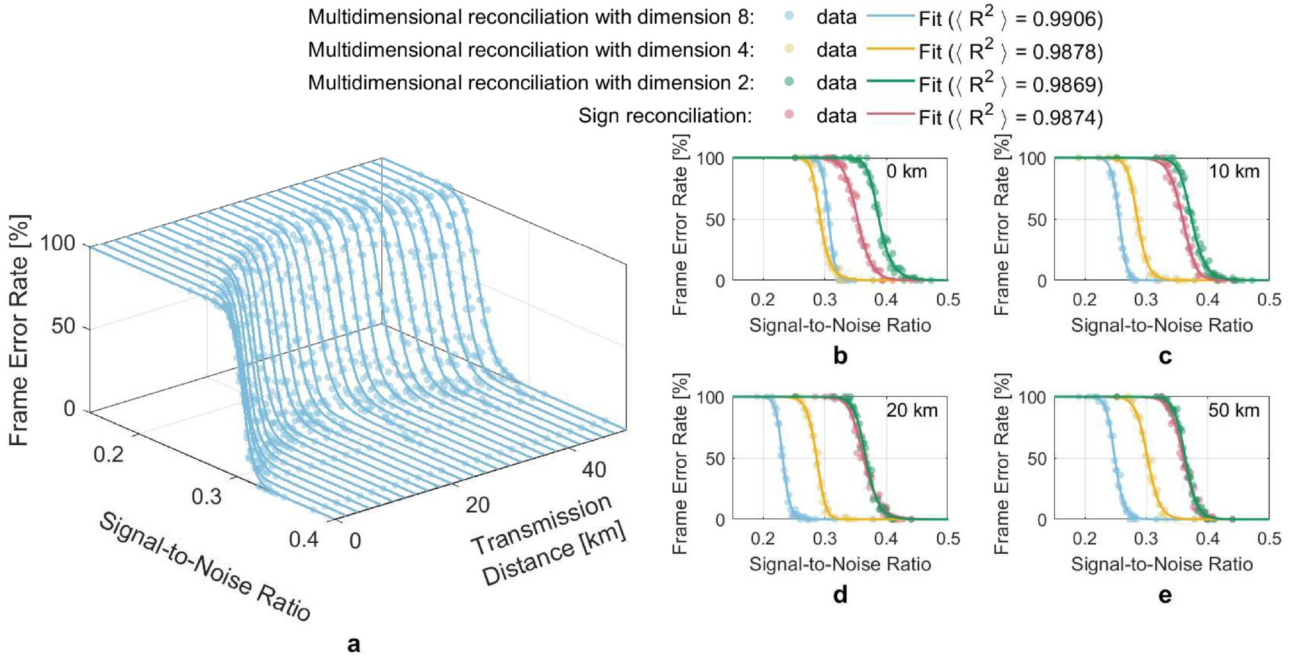

FIGURE 3 FER as a function of the SNR and of the transmission distance for a MET-LDPC code of code rate 0.1 and length 20,000 obtained considering simulations of the physical layer of the CV-QKD system, that is, of the quantum states exchanged between Alice and Bob in the quantum channel and of the information reconciliation step, considering 64-QAM. Fit curves are also represented for the different data sets. (a) Also represents the FER as a function of the transmission distance. In (b–e) the FER is presented for 0, 10, 20 and 50 km, respectively.

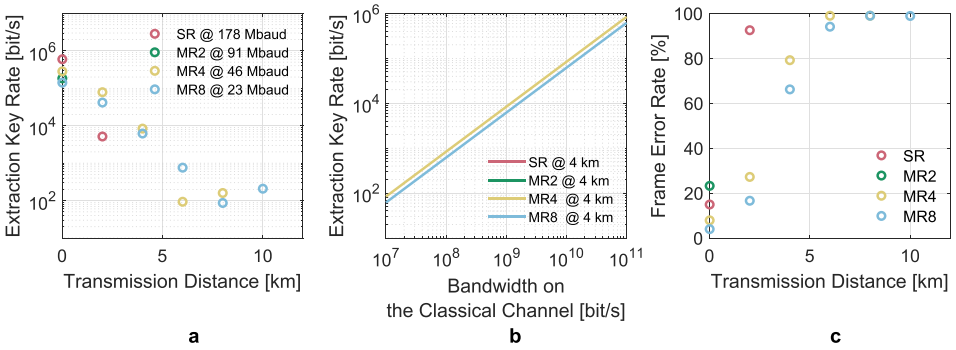

FIGURE 4 (a) Extraction key rate as a function of the transmission distance considering a baud rate in the quantum channel such that the bit rate in the classical channel is 1 Gbit/s; (b) Extraction key rate as a function of the bandwidth on the classical channel for 4 km; (c) FER as a function of the transmission distance. This for a MET-LDPC code of code rate 0.1 and length 20,000, considering sign reconciliation (SR) and multidimensional reconciliation of dimension 2, 4, and 8 (MR2, MR4 and MR8, respectively), 2^{26} states exchanged between Alice and Bob for parameter estimation and key extraction, 64-QAM, a transmission coefficient of 0.2 dB/km, a detection efficiency η of 0.76, an excess noise ξ of 0.046 SNU, a thermal noise ξ_{thermal} of 0.35 SNU, chosen considering realistic values from literature, and with the modulation variance optimised considering the reconciliation efficiency and the FER following the method presented in [4]. Due to high simulation time, a reduced number of transmission distances were considered.

rate in the quantum channel for the same bandwidth restriction in the classical channel varies depending on the information reconciliation method chosen (Figure 2). Therefore, a higher FER value may not result in a smaller extraction key rate. Such a scenario can be observed for SR in a back-to-back situation, and for multidimensional reconciliation of dimension 4 for 2 and 4 km, where the low performance in terms of FER is compensated by the higher allowed baud rate in the quantum channel (Figure 4a). For 4 km, if the CV-QKD system is limited by the bandwidth of the classical channel, multidimensional reconciliation of dimension 4 is the method which allows for the highest extraction key rate (Figure 4b). At 4 km, multidimensional reconciliation of dimension 4 can extract keys at a rate of 8.4, 83.7 and 209 kbit/s for bit rates in the classical channel of 1, 10 and 25 Gbit/s, respectively, for 2^{26} states exchanged between Alice and Bob for parameter estimation and key extraction, for an expected FER of 79%. For the same distance, multidimensional reconciliation of dimension 8 can extract keys at 74% the rate, due to a smaller expected FER of 66% and smaller allowed baud rate on the quantum channel. Multidimensional reconciliation of dimension 2 can only extract keys in a back-to-back situation.

Multidimensional reconciliation of dimension 8 shows better key extraction performance for higher transmission distances, since it can correctly reconcile keys for longer transmission distances (Figure 4a), despite requiring the exchange of data during post-processing at the smallest baud rate. Increasing the transmission distance to 6 km, we can extract keys at a rate of 758 bit/s for 1 Gbit/s of bit rate in the classical channel, using multidimensional reconciliation of dimension 8, for an expected FER of 94%. Increasing the transmission distance even further results in expected FER values close to 100% (Figure 4c).

Note that, to compute the extraction key rate, the modulation variance was optimised both accounting for the reconciliation efficiency and for the FER in the system. Therefore, for 4 km, the extraction key rate is maximised, using multidimensional reconciliation of dimension 4, for a modulation variance of 1.2 for the 64-QAM constellation, corresponding to an SNR of 0.28. In this situation, the reconciliation efficiency is 0.57 and the FER is of 79%. The smaller value of the reconciliation efficiency corresponds to a lower FER, resulting in a higher extraction key rate. Depending on the parameters of the system, lower reconciliation efficiency values may be required to maximise the extraction key rate. With increasing transmission distance, the SNR decreases, and, the reconciliation efficiency increases for which the modulation variance is optimum. Note that the effect of the reconciliation efficiency on the optimisation of the modulation variance was studied in more detail in ref. [4].

Considering the finite-size effects, the performance of the DM-CV-QKD system improves by increasing the number of states exchanged between Alice and Bob. Nonetheless, this requires the DM-CV-QKD system to be stable for a longer duration. This increase in the required stability duration of the system is more critical, baud rate in the quantum channel is the smallest, that is, for multidimensional reconciliation of dimension 8. By increasing the bandwidth of the classical channel, the stability duration requirement decreases, allowing Alice and Bob to exchange between themselves a higher amount of samples per extracted key (Figure 5). Note that the stability duration of the system is also limited. For example, the system by ref. [32] has a maximum stability duration of 10 s [32]. This limits the amount of states that we may consider for the finite-size effects allowing a positive extraction key rate (Figure 5). Therefore, a compromise is required when choosing the bandwidth of the classical channel, to ensure that the system is stable during sufficient time for the exchange of enough states for a positive extraction key rate. Nonetheless, the baud rate on the quantum channel and the bandwidth of the classical channel must also be feasible, and commercially available. Moreover, the baud rate on the quantum channel must be sufficiently low to be detected within the receiver's bandwidth.

In Figure 6 we present the extraction key rate as a function of the transmission distance for 1 Gbit/s bandwidth in the classical channel. The extraction key rate was computed defining the number of states exchanged between Alice and Bob according to limitations of the CV-QKD system's stability duration of 10, 60, and 3600 s. Since multidimensional reconciliation with dimension 4 can use more states than multidimensional reconciliation with dimension 8, for 4 km it can extract keys at 1.89, 1.46, and 1.33 times the rate for acquisition times of 10, 60, and 3600 s, respectively.

The reconciliation method to be used in a CV-QKD system cannot be chosen solely based on the reconciliation code that better approximates the chosen reconciliation efficiency. A trade-off exists between the reconciliation efficiency and the FER in the system. Therefore, the reconciliation method must be optimised considering both its reconciliation efficiency and expected FER depending on the parameters on the physical layer of the CV-QKD system. Depending on the system's limitations, for example, in terms of bandwidth on the classical channel, but also in terms of baud rate for the transmitter and receiver units, one must also account for the different requirements in terms of minimum bandwidth for the classical channel that different reconciliation methods have. A trade-off also exists between the reconciliation performance and the amount of information demanded to be exchanged in the classical channel. Furthermore, a trade-off may also be expected regarding the reconciliation performance and the processing speeds associated to each reconciliation method. Therefore, one must also account for the bandwidth limitations imposed by the reconciliation method in the post-processing, especially during the reconciliation step. The trade-offs are expected to be observed for all DM formats, and also for GM. A proper optimisation of the reconciliation method to be used in a CV-QKD system must account for the

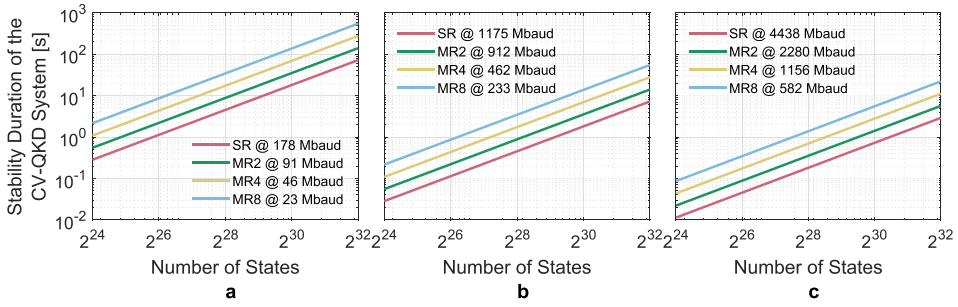

FIGURE 5 Required duration of stability of the CV-QKD system as a function of the number of states exchanged between Alice and Bob, such that the bit rate in the classical channel is (a) 1, (b) 10 and (c) 25 Gbit/s, for a MET-LDPC code of code rate 0.1 and length 20,000, considering sign reconciliation (SR) and multidimensional reconciliation of dimension 2, 4, and 8 (MR2, MR4 and MR8, respectively).

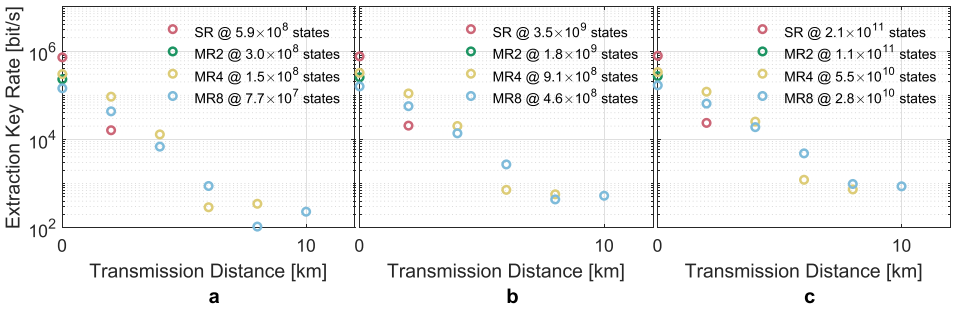

FIGURE 6 Extraction key rate as a function of the transmission distance considering a baud rate in the quantum channel such that the bit rate in the classical channel is 1 Gbit/s for a MET-LDPC code of code rate 0.1 and length 20,000, considering sign reconciliation (SR) and multidimensional reconciliation of dimension 2, 4, and 8 (MR2, MR4 and MR8, respectively), for a number of states exchanged between Alice and Bob for parameter estimation and key extraction such that the stability duration of the CV-QKD system is at least (a) 10 s, (b) 60 s, (c) 3600 s. This for the 64-QAM constellation considering the optimization of the SNR, and thus of the modulation variance having into account the expected FER in the system (Figure 3), a transmission coefficient of 0.2 dB/km, a detection efficiency η of 0.76, an excess noise ξ of 0.046 SNU, and a thermal noise ξ_{thermal} of 0.35 SNU, chosen considering realistic values from literature. Due to high simulation time, a reduced number of transmission distances were considered.

modulation format to be used and the parameters in the system, such as the modulation variance, the transmission distance. and the SNR, but also account for the FER and reconciliation efficiency for the different parameters of the quantum channel, and for the requirements that physical implementations may impose.

5 | CONCLUSIONS

We apply sign and multidimensional reconciliation to higher-order DM-CV-QKD systems using the 64 probabilistic-shaped QAM constellation. Simulations of the CV-QKD system allowed a precise estimation of the FER for accounting on the extraction key rate. Under the considered conditions, the use of a MET-LDPC code with code rate 0.1 allows to extract keys for low transmission distances. Multidimensional reconciliation of dimension 8 shows better reconciliation capabilities in the low SNR regime. Nonetheless, it imposes high minimum bandwidth requirements on the classical channel. For multidimensional reconciliation of dimension 8, the bandwidth of the classical channel must be 43 times greater than the baud rate of the quantum channel. Decreasing the dimension of multidimensional reconciliation to 4 and 2 allows to decrease the required bandwidth of the classical channel by, approximately, 2 and 4 times, respectively. The global implementation of a CV-QKD network may impose bandwidth limitations on the classical channel or on the baud rate of the quantum channel. Depending on the restrictions, different reconciliation methods may allow for higher extraction key rates. For the same bandwidth on the classical channel, the higher allowed baud rate of the quantum channel for multidimensional reconciliation of dimension 4 allows to extract keys at higher rates than multidimensional reconciliation of dimension 8 for small transmission distances. The higher baud rate also allows for a higher number of exchanged states considering the finite-size effects, increasing even more the extraction key rate. By maximising the baud rate in the quantum channel and the allowed number of states exchanged between Alice and Bob, multidimensional reconciliation with dimension 4 can extract keys at 13 kbit/s for 4 km, 1.89 times more than multidimensional reconciliation with dimension 8. This for a CV-QKD system with 10 s of stability duration. The study of other reconciliation methods and the optimization of the reconciliation algorithms and of the code rates is fundamental to improve the key rates and the achievable transmission distances.

AUTHOR CONTRIBUTIONS

Margarida Almeida: Conceptualization; investigation; methodology; formal analysis; visualisation; writing – original draft preparation; writing – review and editing; validation. **Daniel Pereira**: Conceptualization; methodology; writing – review and editing; validation. **Armando N. Pinto**: Supervision; conceptualization; writing – review and editing; project administration; funding acquisition. **Nuno A. Silva**: Supervision; conceptualization; methodology; writing – review and editing; project administration; funding acquisition.

ACKNOWLEDGEMENTS

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under the PhD Grants SFRH/BD/139867/2018 and UI/BD/153377/2022, projects QuantumPrime (PTDC/EEI-TEL/8017/2020), QuantaGenomics (QuantERA/0001/2021), and co-funded by the European Defence Industrial Development Programme (EDIDP) under the project DISCRETION (S12.858093).

NOMENCLATURE

CV-QKD	continuous-variable quantum key distribution
DM	discrete modulation
FER	frame error rate
GM	Gaussian modulation
LDPC	low-density parity check
M-APSK	M-symbol amplitude and phase shift keying

MET	multi-edge type
M-QAM	M-symbol quadrature and amplitude modulation
SNR	signal-to-noise ratio

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflict of interests.

DATA AVAILABILITY STATEMENT

The data that supports the findings of this study is available from the corresponding author upon reasonable request.

ORCID

Margarida Almeida https://orcid.org/0000-0003-1812-5971

REFERENCES

1. Pirandola, S., et al.: Advances in quantum cryptography. Adv. Opt. Photon. 12(4), 1012 (2020). https://doi.org/10.1364/AOP.361502
2. Li, Q., et al.: An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. Quant. Inf. Process. 18(1), 25 (2019). https://doi.org/10.1007/s11128-018-2126-0
3. Almeida, M., et al.: Reconciliation efficiency impact on discrete modulated CV-QKD systems key rates. J. Lightwave Technol. 41(19), 6134–6141 (2023). https://doi.org/10.1109/JLT.2023.3280076
4. Almeida, M., Pinto, A.N., Silva, N.A.: Modulation variance optimization in discrete modulated CV-QKD systems. Emerg. Imag. Sens. Tech. Secur. Defence VIII 12740, 1274009 (2023). https://doi.org/10.1117/12.2683577
5. Lodewyck, J., et al.: Quantum key distribution over 25 Km with an all-fiber continuous-variable system. Phys. Rev. 76(4), 042305 (2007). https://doi.org/10.1103/PhysRevA.76.042305
6. Lin, J., Lütkenhaus, N.: Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. Phys. Rev. Appl. 14(6), 064030 (2020). https://doi.org/10.1103/PhysRevApplied.14.064030
7. Jouguet, P., Kunz-Jacques, S., Leverrier, A.: Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys. Rev. 84(6), 062317 (2011). https://doi.org/10.1103/PhysRevA.84.062317
8. Kaur, E., Guha, S., Wilde, M.M.: Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. Phys. Rev. 103(1), 012412 (2021). https://doi.org/10.1103/PhysRevA.103.012412
9. Hirano, T., et al.: Implementation of continuous-variable quantum key distribution with discrete modulation. Quantum Sci. Technol. 2(2), 024010 (2017). https://doi.org/10.1088/2058-9565/aa7230
10. Lin, J., Upadhyaya, T., Lütkenhaus, N.: Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys. Rev. X 9(4), 041064 (2019). https://doi.org/10.1103/PhysRevX.9.041064
11. Denys, A., Brown, P., Leverrier, A.: Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum 5, 540 (2021). https://doi.org/10.22331/q-2021-09-13-540
12. Almeida, M., et al.: Secret key rate of multi-ring M-APSK continuous variable quantum key distribution. Opt Express 29(23), 38669 (2021). https://doi.org/10.1364/OE.439992
13. Roumestan, F., et al.: 254.6 Mb/s secret key rate transmission over 13.5 Km SMF using PCS-256QAM super-channel continuous variable quantum key distribution. In: Optical Fiber Communication Conference. Optica Publishing Group (2022).Tu3I4
14. Pereira, D., et al.: Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres. Opt Lett. 47(15), 3948–3951 (2022). https://doi.org/10.1364/OL.456333
15. Roumestan, F., et al.: High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM. In: 2021 European Conference on Optical Communication (ECOC), pp. 1–4. IEEE (2021)
16. Roumestan, F., et al.: Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution. In: Optical Fiber Communication Conference. Optica Publishing Group (2021).F4E1
17. Leverrier, A.: Theoretical Study of Continuous-Variable Quantum Key Distribution. PhD thesis. Télécom ParisTech (2009)
18. Silberhorn, C., et al.: Continuous variable quantum cryptography—beating the 3 dB loss limit. Phys. Rev. Lett. 89(16), 167901 (2002). https://doi.org/10.1103/PhysRevLett.89.167901
19. Wang, X., et al.: Continuous-variable quantum key distribution with low-complexity information reconciliation. Opt Express 30(17), 30455 (2022). https://doi.org/10.1364/OE.461665
20. Leverrier, A., et al.: Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys. Rev. 77(4), 042325 (2008). https://doi.org/10.1103/PhysRevA.77.042325
21. Zhou, Y., et al.: Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation. Chin. Phys. B 27(5), 050301 (2018). https://doi.org/10.1088/1674-1056/27/5/050301
22. Van Assche, G., Cardinal, J., Cerf, N.: Reconciliation of a quantum-distributed Gaussian key. IEEE Trans. Inf. Theor. 50(2), 394–400 (2004). https://doi.org/10.1109/TIT.2003.822618
23. Wen, X., et al.: An improved slice reconciliation protocol for continuous-variable quantum key distribution. Entropy 23(10), 1317 (2021). https://doi.org/10.3390/e23101317
24. Feng, Y., et al.: Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution. Phys. Rev. 103(3), 032603 (2021). https://doi.org/10.1103/PhysRevA.103.032603
25. Wang, X., et al.: Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. Quant. Inf. Comput. 17(13and14), 1123–1134 (2017). https://doi.org/10.26421/QIC17.13-14
26. Zhou, C., et al.: Continuous-variable quantum key distribution with rateless reconciliation protocol. Phys. Rev. Appl. 12(5), 054013 (2019). https://doi.org/10.1103/PhysRevApplied.12.054013
27. Roumestan, F., et al.: Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution. arXiv:2207.11702 (2022). (arXiv:2207.11702)
28. Essiambre, R.J., et al.: Capacity limits of optical fiber networks. J. Lightwave Technol. 28(4), 662–701 (2010). https://doi.org/10.1109/JLT.2009.2039464
29. Becir, A., El-Orany, F.A.A., Wahiddin, M.R.B.: Continuous-variable quantum key distribution protocols with eight-state discrete modulation. Int. J. Quant. Inf. 10(01), 1250004 (2012). https://doi.org/10.1142/S0219749912500049
30. Leverrier, A., Grosshans, F., Grangier, P.: Finite-size analysis of a continuous-variable quantum key distribution. Phys. Rev. 81(6), 062343 (2010). https://doi.org/10.1103/PhysRevA.81.062343
31. Pereira, D., et al.: Impact of receiver imbalances on the security of continuous variables quantum key distribution. EPJ Quan. Technol. 8(1), 22 (2021). https://doi.org/10.1140/epjqt/s40507-021-00112-z
32. Brunner, H.H., et al.: Precise noise calibration for CV-QKD. In: 2020 22nd International Conference on Transparent Optical Networks (ICTON), pp. 1–4. IEEE (2020)
33. Qi, B., et al.: Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X 5(4), 041009 (2015). https://doi.org/10.1103/PhysRevX.5.041009

How to cite this article: Almeida, M., et al.: Classical channel bandwidth requirements in continuous variable quantum key distribution systems. IET Quant. Comm. 5(4), 601–611 (2024). https://doi.org/10.1049/qtc2.12103