

Slice Reconciliation in Continuous-Variable Quantum Key Distribution Using Discrete Modulation

Margarida Almeida^{1,2}^a, Armando N. Pinto^{1,2}^b and Nuno A. Silva¹^c

¹*Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*

²*Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*
{mralmeida, anp, nasilva}@ua.pt

Keywords: Quantum Key Distribution, Continuous-Variable, Discrete Modulation, Higher-Order Constellations, Information Reconciliation, Slice Reconciliation, Multidimensional Reconciliation.

Abstract: Information reconciliation is a critical component of Continuous-Variable Quantum Key Distribution (CV-QKD) systems. This particular step of the CV-QKD system significantly affects the extraction key rate. Previous studies that incorporate higher-order discrete modulation (DM) while accounting for the information reconciliation step in the computation of the extraction key rate of CV-QKD systems have focused on multidimensional reconciliation. However, higher-order DM formats, such as 64-Quadrature Amplitude Modulation (QAM), enable higher signal-to-noise ratios (SNRs) where slice reconciliation is known to outperform multidimensional reconciliation. In this work, we compare the performance of multidimensional reconciliation and slice reconciliation in DM-CV-QKD systems. Our findings demonstrate that slice reconciliation delivers superior performance at metropolitan distances. At 20 km, using slice reconciliation with 3 slices of code rates 0, 0.01, and 0.6 increases the key rate by more than 400 times when compared to multidimensional reconciliation with a code rate of 0.05. This significant performance boost more than compensates for the higher computational time associated with slice reconciliation. With the proper optimization of the number of slices, and of the code rate per slice, slice reconciliation is a valid option for real-world implementations of DM-CV-QKD systems using higher-order constellations.


1 INTRODUCTION


Quantum Key Distribution (QKD) is a revolutionary technique to ensure the secure communication between two distant parties without relying on any computational assumption (Pirandola et al., 2020). In that sense, QKD guarantees unconditional security by exploiting the inherent properties of quantum states (Pirandola et al., 2020). In the field of quantum cryptography, Continuous-Variable (CV) QKD has gained significant attention due to its compatibility with existing telecommunication infrastructure and its potential for high key rates over metropolitan distances (Zhang et al., 2019).


In CV-QKD, information is typically encoded in the quadratures of coherent states using Gaussian Modulation (GM) (Laudenbach et al., 2018). While GM has been theoretically proven to be optimal in

terms of key rates, its practical implementation poses several challenges. This is due to the need for optoelectronic modulators with infinite extinction ratios (Liu et al., 2021; Denys et al., 2021) and the complexity of generating truly Gaussian-distributed random variables (Liu et al., 2021).

Discrete Modulation (DM) has been proposed as a practical alternative to GM for real-world implementations (Leverrier and Grangier, 2011). In DM, information is encoded using specific constellations, such as M-symbol Phase Shift Keying (M-PSK), which offer experimental simplicity (Ghorai et al., 2019; Kleis et al., 2017; Lin and Lütkenhaus, 2020). Notably, higher-order constellations, especially M-symbol Quadrature Amplitude Modulation (M-QAM), can approach the performance of GM (Denys et al., 2021). Experimental demonstrations of 64-, 256-, and 1024-QAM for CV-QKD have been reported in (Roumestan et al., 2021a; Roumestan et al., 2021b). However, like most CV-QKD implementations, these experiments omitted the critical step of in-

^a <https://orcid.org/0000-0003-1812-5971>

^b <https://orcid.org/0000-0003-2101-5896>

^c <https://orcid.org/0000-0002-6309-6818>

formation reconciliation. As a result, the reported key rates do not accurately reflect the actual performance of the system in a real-world scenario (Almeida et al., 2023a; Almeida et al., 2023b).

In the information reconciliation step, Alice and Bob correct discrepancies between their respective measurement outcomes due to noise and other imperfections in the quantum channel. The efficiency of this process directly impacts the overall performance of the QKD system. Information reconciliation was proposed for small-order DM-CV-QKD systems (Leverrier et al., 2008) considering sign reconciliation, originally applied to GM-CV-QKD systems (Li et al., 2019). In GM-CV-QKD, reconciliation methods such as multidimensional reconciliation and slice reconciliation are commonly employed (Li et al., 2019; Wang et al., 2022; Leverrier et al., 2008; Wen et al., 2021). Multidimensional reconciliation relies on a transformation step, being particularly effective for low signal-to-noise ratios (SNRs) due to its lossless rotation (Wang et al., 2022). On the other hand, slice reconciliation operates through a quantization step (Feng et al., 2021), enabling the distillation of more than one bit per symbol per measured quadrature, and showing higher efficiency at higher SNRs (Wang et al., 2022; Van Assche et al., 2004).

In (Almeida et al., 2023a; Almeida et al., 2023b), the impact of the reconciliation efficiency and of the frame error rate (FER) of the information reconciliation step on the extraction key rate was studied. These works showed the importance of accounting for the information reconciliation step when optimizing the parameters of the system. Notwithstanding, only multidimensional reconciliation was considered. Since the use of higher-order DM formats allow for higher SNRs, it is of the most importance to study the impact of slice reconciliation on the extraction key rate of DM-CV-QKD systems. Remark that in (Yang et al., 2023) a comparison between multidimensional reconciliation and slice reconciliation is provided considering only Gaussian modulation, and not DM. This through the comparison of state-of-the-art works using only one of the reconciliation methods in different conditions. Moreover, (Yang et al., 2023) compares both reconciliation methods regarding only the information reconciliation step, and not the extraction key rate. Here we compare how the performance of multidimensional and slice reconciliation affect the extraction key rate of DM-CV-QKD systems, understanding which method is the most beneficial for DM-CV-QKD systems in each SNR scenario. With this study we intend to bridge the gap between theoretical performance and real-world applicability, paving the way for more robust and efficient quantum communi-

cation systems. From the results, slice reconciliation is a valid candidate for the reconciliation of keys in CV-QKD systems using higher-order DM, allowing for higher extraction rates than multidimensional reconciliation at metropolitan distances.

In the following sections, we provide a detailed theoretical background on DM-CV-QKD and information reconciliation, describing the computation of the extraction key rate for CV-QKD using higher-order DM in Section 2. In Section 3 we briefly explain multidimensional reconciliation and slice reconciliation. Section 4 is focused on the results of the study and their discussion. Finally, Section 5 presents the final conclusions.

2 KEY RATE FOR CV-QKD USING HIGHER-ORDER CONSTELLATIONS

A CV-QKD system can be divided into two primary components: the physical layer and the post-processing layer. The physical layer is responsible for the exchange of quantum states over the quantum channel between the two parties, typically referred to as Alice (the sender) and Bob (the receiver). Here, the quantum channel is considered to be optical fiber. The post-processing layer encompasses the critical steps of parameter estimation, information reconciliation, and privacy amplification. This layer ensures that the keys generated are identical, secure, and free from eavesdropping.

In DM-CV-QKD, the quantum coherent states are given by specific points in a constellation diagram. The constellation points are geometric and probabilistic shaped to optimize the performance of the system. In this work, we use 64-QAM following the Boltzmann-Maxwell distribution for probabilistic shaping to approximate the optimum performance of GM (Denys et al., 2021; Roumestan et al., 2021b; Almeida et al., 2023a). The in-phase and quadrature points of the 64-QAM constellation are defined by $|\alpha_{k,l}| = (k + il)\sqrt{(V_A)/(2\sum_{k,l}P_{k,l}\sqrt{k^2+l^2})}$ with k, l equidistant values between -1 and 1, V_A the modulation variance, and $P_{k,l} = \exp(-v(k^2+l^2))/\sum_{k,l}P_{k,l}$ the probability of the states under the Boltzmann-Maxwell distribution. The parameter v is optimized to maximize the secret key rate.

The secret key rate, K , of a DM-CV-QKD system is given by:

$$K = \frac{n}{N} [\beta I_{BA} - \chi_{BE} - \Delta(n)], \quad (1)$$

where I_{BA} is the mutual information between Bob and

Alice computed considering DM (Essiambre et al., 2010), χ_{BE} is the Holevo bound between Bob and Eve considering heterodyne detection, reverse reconciliation and collective Gaussian attacks, computed following (Becir et al., 2012), β is the reconciliation efficiency, and $\Delta(n)$, computed from (Leverrier et al., 2010), accounts for the finite-size effects, considering the close approximation between 64-QAM and GM (Roumestan et al., 2021a). The ratio $\frac{n}{N}$ accounts for the fact that $N - n$ states are reserved for parameter estimation. The computation of χ_{BE} involves the Z parameter, which is defined as (Denys et al., 2021)

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

Here T_{ch} is the channel's transmission, ξ is the excess noise, $\text{Tr}(\cdot)$ 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, $W = \sum_{k,l} P_{k,l} \left(\langle\alpha_{k,l}|\hat{a}^\dagger\hat{a}\tau|\alpha_{k,l}\rangle - |\langle\alpha_{k,l}|\hat{a}\tau|\alpha_{k,l}\rangle|^2 \right)$, $\hat{a}\tau = \tau^{1/2}\hat{a}\tau^{-1/2}$, and \hat{a} and \hat{a}^\dagger are the annihilation and creation operators on Alice's system, respectively. Due to the finite-size effects, the values of T_{ch} and ξ are adjusted to their respective lower and upper bounds with a probability of at least $1 - \varepsilon_{PE}$, respectively (Leverrier et al., 2010).

The reconciliation efficiency β ensures that only the correct amount of information is extracted, preventing potential security breaches. The FER is another critical metric, indicating the proportion of frames that remain uncorrected after the reconciliation step. The FER parameter is used to compute the final extraction key rate of the system, given by

$$K_{\text{extraction}} = \frac{n}{N}(1 - \text{FER})[\beta I_{BA} - \chi_{BE} - \Delta(n)]. \quad (3)$$

3 RECONCILIATION OF SYMMETRIC KEYS FOR CV-QKD SYSTEMS

In the post-processing layer, the information reconciliation step ensures that the discrepancies between Alice's and Bob's raw data, X and Y , due to the noise in the quantum channel are mitigated, leading to identical keys at Alice's and Bob's side. Two of the most prominent reconciliation methods in CV-QKD are multidimensional reconciliation and slice reconciliation, each with distinct advantages depending on the system's conditions.

Multidimensional reconciliation is particularly effective in the low SNR environment, by leveraging a lossless rotation of the data points in higher-dimensional spaces to align Alice's and Bob's raw

data. The dimension d of multidimensional reconciliation can take the value of 1, 2, 4 and 8 (Leverrier et al., 2008). Due to its improved performance, here we consider d equal to 8 (Leverrier et al., 2008; Feng et al., 2021). Multidimensional reconciliation starts by organizing Alice's and Bob's raw data, X and Y , into 8-dimensional vectors $\mathbf{x} = (x_1, x_2, \dots, x_8)$ and $\mathbf{y} = (y_1, y_2, \dots, y_8)$, respectively. Bob then generates a binary random sequence, \mathbf{m} , using a true random number generator and the respective 8-dimensional sequences $\mathbf{u} = \frac{1}{\sqrt{8}} [(-1)^{m_1}, (-1)^{m_2}, \dots, (-1)^{m_8}]$. To proceed, Bob computes the rotation matrix $M(\mathbf{y}, \mathbf{u}) = \sum_{i=1}^8 \alpha_i(\mathbf{y}, \mathbf{u}) \mathbf{Q}_i$ which maps \mathbf{y} into \mathbf{u} through $M(\mathbf{y}, \mathbf{u})\mathbf{y} = \mathbf{u}$. Here $\alpha_i(\mathbf{y}, \mathbf{u})$ are the coordinates of \mathbf{u} on the orthogonal basis $[\mathbf{Q}_1\mathbf{y}, \mathbf{Q}_2\mathbf{y}, \dots, \mathbf{Q}_8\mathbf{y}]$, obtained by doing $\alpha_i(\mathbf{y}, \mathbf{u}) = [\mathbf{T}^{-1}\mathbf{u}]_i$, with \mathbf{T} and \mathbf{Q}_i detailed in (Leverrier et al., 2008). The rotation matrix $M(\mathbf{y}, \mathbf{u})$ is sent to Alice as side information. By knowing $M(\mathbf{y}, \mathbf{u})$, Alice can compute the noisy version of \mathbf{u} , $\mathbf{v} = M(\mathbf{y}, \mathbf{u})\mathbf{x}$. Using the sum-product algorithm, Alice can obtain the best estimate of the binary random sequence \mathbf{m} , thus obtaining the raw binary key. For such, the log-likelihood ratio for the *priori* message probabilities, r_i , is given by (Feng et al., 2021)

$$r_i = -\frac{9}{2} \log \left[\frac{8 + (v_i - 1)^2}{8 + (v_i + 1)^2} \right]. \quad (4)$$

For multidimensional reconciliation, and considering heterodyne detection, the reconciliation efficiency is given by

$$\beta_{\text{MR}} = \frac{2R}{I_{BA}}, \quad (5)$$

where R is the code rate of the low-density parity check (LDPC) matrix used.

On the other hand, slice reconciliation is particularly efficient for higher SNR environments by quantizing the key data into slices. Moreover, it allows the extraction of more than one bit per symbol per quadrature, which increases efficiency when the channel conditions are favorable (Wang et al., 2022). Slice reconciliation starts by quantifying Y into m sets of binary data, (Y_1, Y_2, \dots, Y_m) , using a quantization function $Q(y) : \mathbb{R} \rightarrow \{0, 1\}^m$, as provided in (Wen et al., 2021). The quantization function is obtained by dividing the set of real numbers into 2^m intervals $T(Y)$, defined by $2^m - 1$ variables $\tau_1, \tau_2, \dots, \tau_{2^m-1}$. The interval a with $1 \leq a \leq 2^m$ is defined by the set $\{x : \tau_{a-1} \leq x \leq \tau_a\}$ where $\tau_0 = -\infty$ and $\tau_{2^m} = +\infty$ (Van Assche et al., 2004). The 2^m intervals, i.e. $\tau_1, \tau_2, \dots, \tau_{2^m-1}$, are equidistant (Wen et al., 2021) and defined by maximizing the mutual information between X and $T(Y)$ (Wang et al., 2022). The best bit assignment method assigns the least significant bit to the first slice $Q_1(y)$. Then, each bit is subsequently assigned up to the

most significant bit, which is assigned to the last slice $Q_m(x)$ (Van Assche et al., 2004). This ensures that the first slice contains only noisy values that helps Bob narrow down his guess as quickly as possible. This ensures that the slices can be corrected with as little leaked information as possible. The sum-product algorithm is applied to each slice at a time. The log-likelihood ratio for the *priori* message probabilities, r_i , is given by (Guo et al., 2020):

$$r_i = \log \left(\frac{\sum_{a:y_i=0} \operatorname{erf} \left(\frac{\tau_a - x}{\sqrt{2\sigma^2}} \right) - \operatorname{erf} \left(\frac{\tau_{a-1} - x}{\sqrt{2\sigma^2}} \right)}{\sum_{a':y_i=1} \operatorname{erf} \left(\frac{\tau_{a'} - x}{\sqrt{2\sigma^2}} \right) - \operatorname{erf} \left(\frac{\tau_{a'-1} - x}{\sqrt{2\sigma^2}} \right)} \right), \quad (6)$$

where $x \in \mathcal{X}$ are the points of Alice's discrete constellation, $\operatorname{erf}(\cdot)$ is the error function, and $\sigma^2 = \frac{T\eta}{2}\xi + 1 + \xi_{\text{thermal}}$. For slice reconciliation, and considering heterodyne detection, the reconciliation efficiency is given by (Wang et al., 2022)

$$\beta_{\text{SR}} = \frac{2(H(T(Y)) - \sum_{i=1}^m (1 - R_i))}{I_{BA}}, \quad (7)$$

where R_i is the code rate of the LDPC matrix used for slice i , and (Wang et al., 2022)

$$H(T(Y)) = - \sum_a P_a \log_2 P_a, \quad (8)$$

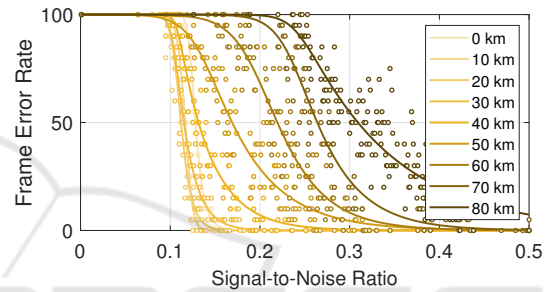
where $P_a = \int_{\tau_{a-1}}^{\tau_a} \frac{1}{\sqrt{2\pi}V_B} \exp\left(-\frac{y^2}{2V_B}\right)$, and $V_B = \frac{T\eta}{2} \cdot 2\langle n \rangle + \frac{T\eta}{2}\xi + 1 + \xi_{\text{thermal}}$ is the variance of Bob's states.

4 RESULTS AND DISCUSSION

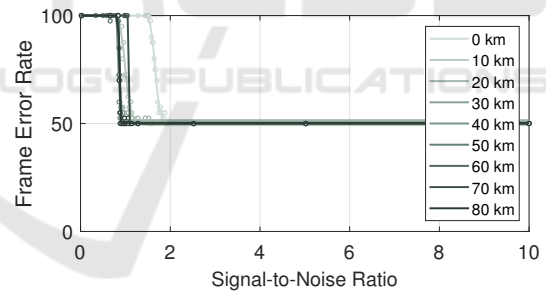
Through a simulation of a CV-QKD system using 64-QAM, with multidimensional and slice reconciliation for the information reconciliation step, we obtained the FER associated to each reconciliation method for different SNR values of the CV-QKD system (Fig. 1). Since differences were found in the relationship between the FER and the SNR depending on the transmission distance, the simulations were conducted for discrete transmission distances between 0 and 80 km, in intervals of 10 km. This differences are due to the impact of the transmission distance on the noise of the system and on the optimization of the slice intervals for slice reconciliation. Due to the high computation time of the information reconciliation step, only 10^5 states were considered for the simulation. In Fig. 1, we present the FER results of the simulations as a function of the SNR for the different transmission distances, alongside the respective fit curves. Despite the simulations being conducted for various possibilities of code rates for multidimensional reconciliation and

for various combinations of code rates for slice reconciliation, in Fig. 1 we only present results considering multidimensional reconciliation with code rate $R = 0.05$ (Fig. 1a)), slice reconciliation with 2 slices of code rates $R_1 = 0.05$ and $R_2 = 0.4$ (Fig. 1b)), and slice reconciliation with 3 slices of code rates $R_1 = 0$, $R_2 = 0.01$ and $R_3 = 0.6$ (Fig. 1c)).

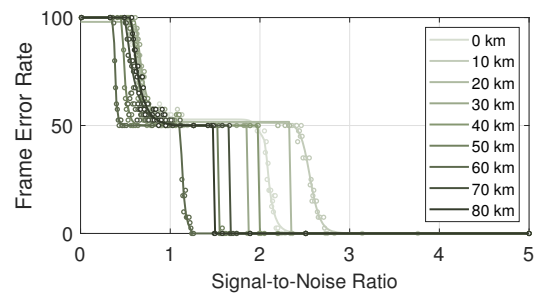
In line with state-of-the-art, multidimensional reconciliation is well fit for smaller SNRs, while slice reconciliation allows the reconciliation for higher SNRs (Fig. 1). Remark that slice reconciliation has associated heights, since each code rate (with a different LDPC matrix) is applied to each slice. From a practical perspective, it is important to analyze the role of the reconciliation efficiency and of the FER on the computation of the extraction key rate. This



a) Multidimensional reconciliation ($R = 0.05$)



b) Slice reconciliation (2 slices: $R_1 = 0.05$, $R_2 = 0.4$)



c) Slice reconciliation (3 slices: $R_1 = 0$, $R_2 = 0.01$, $R_3 = 0.6$)

Figure 1: FER as a function of the SNR for different transmission distances, considering (a) multidimensional reconciliation with code rate 0.05, (b) slice reconciliation with 2 slices of code rates 0.05 and 0.4, and (c) slice reconciliation with 3 slices of code rates 0, 0.01 and 0.6.

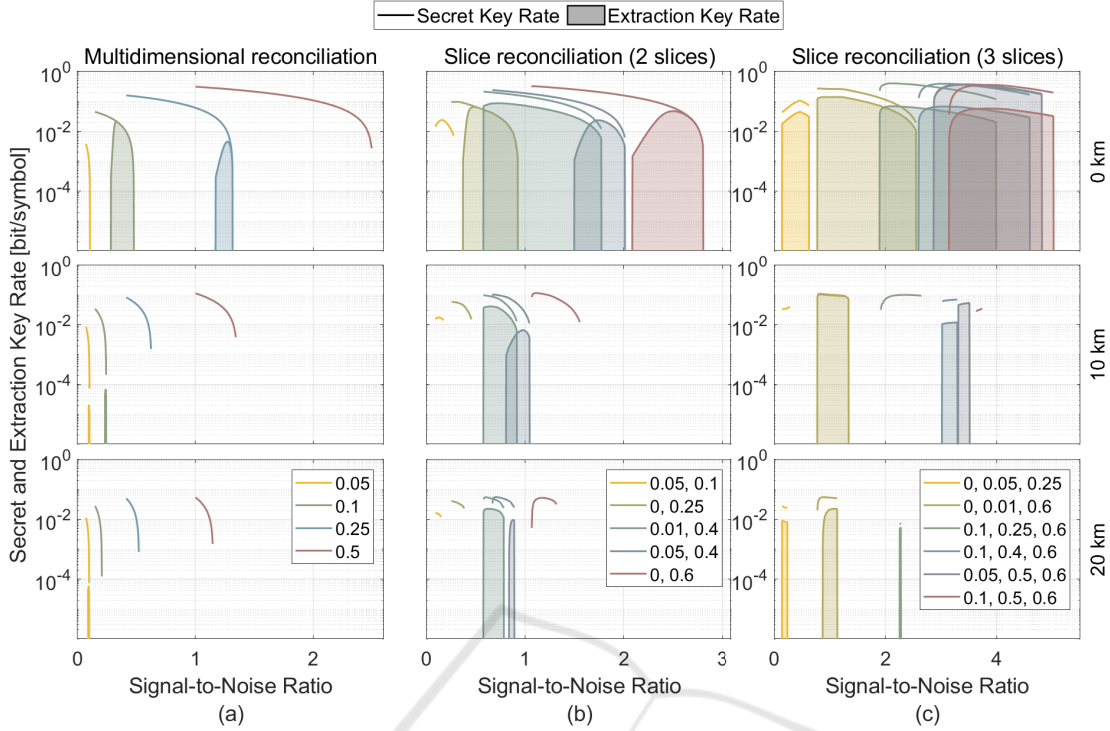


Figure 2: Secret key rate, given by Eq. 1, and extraction key rate, given by Eq. 3, as a function of the SNR for 0, 10 and 20 km, considering (a) multidimensional reconciliation for different code rates, (b) slice reconciliation with 2 slices for different code rate combinations, and (c) slice reconciliation with 3 slices for different code rate combinations. This considering 10^{14} 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, and a thermal noise ξ_{thermal} of 0.35 SNU.

for both multidimensional and slice reconciliation. In that sense, we compare the use of slice reconciliation with the use of multidimensional reconciliation, to better understand if the higher correction capabilities of slice reconciliation in the high SNR regime can be beneficial for the key extraction in CV-QKD systems using higher-order DM which usually allows for higher SNR than the low cardinality constellations initially considered in the literature.

In Fig. 2 we present the secret key rate, given by Eq. 1, and the extraction key rate, given by Eq. 3, as a function of the SNR for 0, 10 and 20 km, considering multidimensional reconciliation for different code rates (Fig. 2a)), and slice reconciliation with 2 and 3 slices for different code rate combinations (Fig. 2b) and Fig. 2c)). The extraction key rate was computed by estimating the FER depending on the SNR using the fit curves to the results of the simulations of the CV-QKD system (Fig. 1).

For multidimensional reconciliation, higher code rates of the LDPC code result in higher secret key rates, given by Eq. 1, at higher SNRs, due to the higher reconciliation efficiency, computed using Eq. 5. Notwithstanding, using a LDPC with code rate 0.5 (the highest code rate considered) does not

allow for any key extraction even in a back-to-back configuration (Fig. 2a)). This is due to the impact of the FER on the extraction key rate, given by Eq. 3, which, for code rate 0.5 is unitary for SNRs below than 2.5. Decreasing the code rate of the LDPC matrix to a code rate of 0.25 allows key extraction in a back-to-back configuration, but at smaller rates than using a LDPC with code rate 0.1. At 0 km, the code rate 0.1 allows the extraction of 0.02 bit/symbol at an SNR of 0.33, while the code rate 0.25 can only extract 0.005 bit/symbol at an SNR of 1.27 (Fig. 2a)). For higher transmission distances, smaller code rates of 0.05 and 0.1 must be considered, with the LDPC matrix of code rate 0.05 allowing key extraction at a rate of 5.6×10^{-5} bit/symbol at 20 km for an SNR of 0.09.

Generally, the use of slice reconciliation using 2 slices also allows for higher secret key rates, given by Eq. 1, at higher SNRs by increasing the sum of the code rates of the LDPC codes considered for each slice (Fig. 2b)). The same conclusion cannot be drawn for slice reconciliation using 3 slices in what concerns to the secret key rate, with code rate combinations of 0.1, 0.25, 0.6 and 0.1, 0.4, 0.6 achieving higher secret key rates than code rate combinations of 0.1, 0.5, 0.6

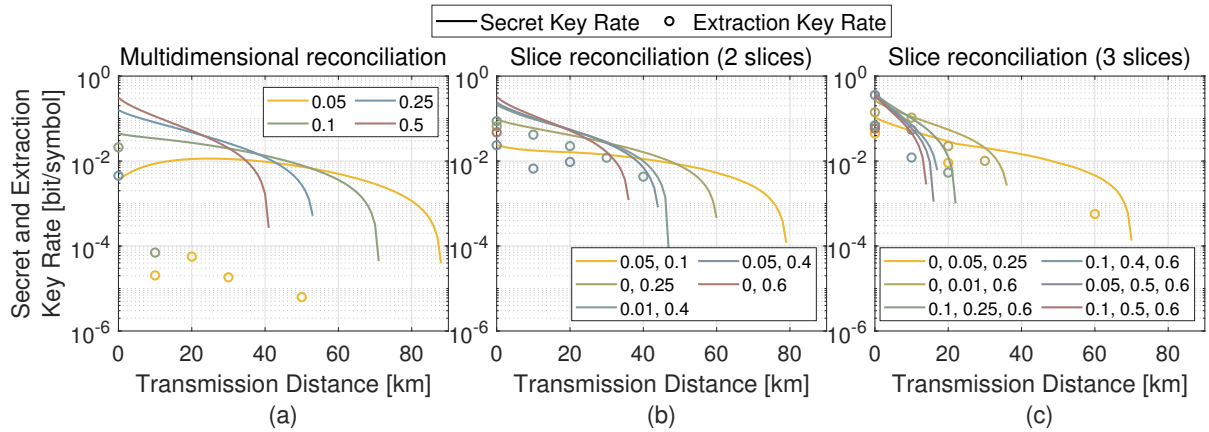


Figure 3: Secret key rate, given by Eq. 1, and extraction key rate, given by Eq. 3, as a function of the transmission distance with the SNR optimized, considering (a) multidimensional reconciliation for different code rates, (b) slice reconciliation with 2 slices for different code rate combinations, and (c) slice reconciliation with 3 slices for different code rate combinations. This considering 10^{14} 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, and a thermal noise ξ_{thermal} of 0.35 SNU.

(Fig. 2c)).

The impact of the FER of the information reconciliation step is not as critical for slice reconciliation as it is for multidimensional reconciliation. In a back-to-back situation, slice reconciliation with 3 slices of code rates 0.05, 0.5, and 0.6 can extract 0.358 bit/symbol, while slice reconciliation with 2 slice of code rates 0.01 and 0.4 can only extract 0.087 bit/symbol. This corresponds to 17.9 and 4.35 times more than multidimensional reconciliation with code rate 0.1. At 10 km and 20 km the key rate extracted when using slice reconciliation with 3 slices of code rates 0, 0.01, and 0.6 is 150 times and 402 times greater than using multidimensional reconciliation with code rate 0.1 and 0.05, respectively (Fig. 2)). Remark however that, with higher transmission distances, the range of the SNRs for which key extraction is possible decreases. This turns the practical implementation of the CV-QKD system more difficult by requiring a precise setting of the modulation variance in the system to ensure the proper SNR depending on the remaining practical conditions of the system.

In Fig. 3, the secret key rate is presented as a function of the transmission distances considering multidimensional reconciliation for different code rates (Fig. 3a)), and slice reconciliation with 2 and 3 slices for different code rate combinations (Fig. 3b) and Fig. 3c)). The secret key rate was maximized considering an optimization of the SNR. Remark that smaller code rates for multidimensional reconciliation, and smaller sums of code rates for the code rate combinations for slice reconciliation tend to allow a positive secret key rate for higher transmission distances (Fig. 3). In this regard, multidimensional rec-

onciliation maximizes the transmission distance for which the secret key rate is positive, being followed by slice reconciliation with two slices.

When accounting for the FER in the computation of the extraction key rate, given by Eq. 3, the use of slice reconciliation increases the extraction key rate by several orders of magnitude, for metropolitan distances up to 60 km. Notwithstanding, one must properly choose the code rates to use in slice reconciliation, not only to ensure the maximization of the extraction key rate, but also key extraction, since not all code rate combinations may allow for key extraction. Moreover, despite the use of 3 slices generally yielding greater performance in terms of extraction key rate than the use of 2 slices, one must also considering the computation time associated to the additional number of slices because a reduced performance in terms of extraction key rate may be compensated by the reduced computation time.

5 CONCLUSION

The impact of the reconciliation efficiency and of the FER of the information reconciliation step must be accounted on the computation of the extraction key rate of CV-QKD systems. By comparing the performance of multidimensional reconciliation and slice reconciliation in terms of the extraction key rate in DM-CV-QKD systems, we show that slice reconciliation allows for better performances than multidimensional reconciliation for transmission distances up to 60 km. At 0 km and 10 km, slice reconciliation with 3 slices can extract 17.9 and 150 times more bits

per symbol than multidimensional reconciliation with code rate 0.1. This using the code rate combinations of 0.05, 0.5 and 0.6 at 0 km and 0, 0.01, and 0.6 at 10 km, for slice reconciliation. At 20 km the key rate extracted when using slice reconciliation with 3 slices of code rates 0, 0.01, and 0.6 increases to 402 times the extraction rate when using multidimensional reconciliation with code rate 0.05. Such increase in performance largely compensates the higher computation time associated to slice reconciliation. Remark that the information reconciliation step must be optimized to maximize the extraction key rate in DM-CV-QKD systems. This accounting both for the method (multidimensional or slice reconciliation), but also for the code rates used and for the number of slices considered, in the case of slice reconciliation.

In this study only a reduced number of options were considered for the code rate combinations for slice reconciliation with 2 and 3 slices. This mainly due to high computation time, which results in limited statistic in the analysis of the FER depending on the SNR and on the transmission distance. An improved study should consider the implementation of the information reconciliation step in the graphics processing unit (GPU) or in a field programmable gate array (FPGA) for increased processing speed. Currently, the information reconciliation step is implemented in the central processing unit (CPU), resulting in long processing times, decreasing the number of the simulations conducted. With a faster implementation of the information reconciliation step, the detailed study of the FER as a function of the SNR should consider at least 10^{10} states per simulation of the CV-QKD system for a better statistical analysis, and greater LDPC matrices, for increased performance. Doing so, would improve the estimation of the FER considered for the computation of the extraction key rate, improving the conclusions on which information reconciliation method is the best fit for a particular CV-QKD system, depending on the system's conditions. Moreover, it would allow the proper assessment of the critical points or thresholds for the SNR that determine when the of multidimensional or slice reconciliation is more advantageous. This is especially important when choosing the code rates that maximize the key extraction rate of the system. Furthermore, an improved analysis should considered all possibilities of code rate combinations for slice reconciliation, and should study the application of slice reconciliation with more than 3 slices to better understand if the increase of the number of slices is always beneficial, or if it exists an optimum number of slices.

ACKNOWLEDGMENTS

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 Grant UI/BD/153377/2022, and co-funded by the European Defence Industrial Development Programme (EDIDP) under the project DISCRETION (S12.858093), and by the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

REFERENCES

- Almeida, M., Pereira, D., Facão, M., Pinto, A. N., and Silva, N. A. (2023a). Reconciliation Efficiency Impact on Discrete Modulated CV-QKD Systems Key Rates. *Journal of Lightwave Technology*, 41(19):6134–6141.
- Almeida, M., Pinto, A. N., and Silva, N. A. (2023b). Modulation variance optimization in discrete modulated CV-QKD systems | SPIE Sensors + Imaging. In *EMERGING IMAGING AND SENSING TECHNOLOGIES FOR SECURITY AND DEFENCE*, Amsterdam, Netherlands. SPIE.
- Becir, A., El-Orany, F. A. A., and Wahiddin, M. R. B. (2012). Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10(01):1250004.
- Denys, A., Brown, P., and Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540.
- Essiambre, R.-J., Kramer, G., Winzer, P. J., Foschini, G. J., and Goebel, B. (2010). Capacity limits of optical fiber networks. *Journal of Lightwave Technology*, 28(4):662–701.
- Feng, Y., Wang, Y.-J., Qiu, R., Zhang, K., Ge, H., Shan, Z., and Jiang, X.-Q. (2021). Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution. *Physical Review A*, 103(3):032603.
- Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A. (2019). Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X*, 9(2):021059.
- Guo, D., He, C., Guo, T., Xue, Z., Feng, Q., and Mu, J. (2020). Comprehensive high-speed reconciliation for continuous-variable quantum key distribution. *Quantum Information Processing*, 19(9):320.
- Kleis, S., Rueckmann, M., and Schaeffer, C. G. (2017). Continuous variable quantum key distribution with a

- real local oscillator using simultaneous pilot signals. *Optics Letters*, 42(8):1588.
- Laudenbach, F., Pacher, C., Fung, C.-H. F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., and Hübel, H. (2018). Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Advanced Quantum Technologies*, 1(1):1800011.
- Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., and Grangier, P. (2008). Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325.
- Leverrier, A. and Grangier, P. (2011). Continuous-variable quantum key distribution protocols with a non-Gaussian modulation. *Physical Review A*, 83(4):042312.
- Leverrier, A., Grosshans, F., and Grangier, P. (2010). Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343.
- Li, Q., Wen, X., Mao, H., and Wen, X. (2019). An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. *Quantum Information Processing*, 18(1):25.
- Lin, J. and Lütkenhaus, N. (2020). Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. *Physical Review Applied*, 14(6):064030.
- Liu, W.-B., Li, C.-L., Xie, Y.-M., Weng, C.-X., Gu, J., Cao, X.-Y., Lu, Y.-S., Li, B.-H., Yin, H.-L., and Chen, Z.-B. (2021). Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum Key Distribution with High Excess Noise Tolerance. *PRX Quantum*, 2(4):040334.
- Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., and Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012.
- Roumestan, F., Ghazisaeidi, A., Renaudier, J., Brindel, P., Diamanti, E., and Grangier, P. (2021a). Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution. In *Optical Fiber Communication Conference (OFC) 2021*, page F4E.1, Washington, DC. Optica Publishing Group.
- Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Diamanti, E., and Grangier, P. (2021b). High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM. In *2021 European Conference on Optical Communication (ECOC)*, pages 1–4, Bordeaux, France. IEEE.
- Van Assche, G., Cardinal, J., and Cerf, N. (2004). Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE Transactions on Information Theory*, 50(2):394–400.
- Wang, X., Wang, H., Zhou, C., Chen, Z., Yu, S., and Guo, H. (2022). Continuous-variable quantum key distribution with low-complexity information reconciliation. *Optics Express*, 30(17):30455.
- Wen, X., Li, Q., Mao, H., Wen, X., and Chen, N. (2021). An Improved Slice Reconciliation Protocol for Continuous-Variable Quantum Key Distribution. *Entropy*, 23(10):1317.
- Yang, S., Yan, Z., Yang, H., Lu, Q., Lu, Z., Cheng, L., Miao, X., and Li, Y. (2023). Information reconciliation of continuous-variables quantum key distribution: Principles, implementations and applications. *EPJ Quantum Technology*, 10(1):40.
- Zhang, Y., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., Huang, Y., Xu, C., Zhang, X., Wang, Z., Li, M., Zhang, X., Zheng, Z., Chu, B., Gao, X., Meng, N., Cai, W., Wang, Z., Wang, G., Yu, S., and Guo, H. (2019). Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology*, 4(3):035006.