Reconciliation Efficiency Impact on Discrete Modulated CV-QKD Systems Key Rates

Margarida Almeida, Daniel Pereira, Margarida Facão, Armando N. Pinto, and Nuno A. Silva

***Abstract*—Continuous variable quantum key distribution (CV-QKD) allows the distribution of symmetric keys in a secure manner. CV-QKD systems can extract keys at its maximum rate when using Gaussian modulation (GM). Nonetheless, GM demands high-capacity random number sources and tends to be very hard to approach in practice. To circumvent these disadvantages, higher-order probabilistic-shaped discrete modulation (DM) can be used. State-of-the-art works compute the key rates of DM-CV-QKD systems considering a fixed value for the reconciliation efficiency and do not take into account the frame error rate (FER) of the system, thus over or under estimating the key rates. In this work, we study the security bounds of CV-QKD systems considering probabilistic shaped DM formats with 256-symbols in the finite-size regime. This accounting for the true value of the reconciliation efficiency, and the FER of the information reconciliation step. Both conventional and hexagonal 256-quadrature amplitude modulation (QAM) constellations yield higher key rates than 256-amplitude and phase shift keying (APSK) constellations, with 256-QAM constellations being indistinguishable in performance with GM for high transmission distances. Minimum signal-to-noise ratio (SNR) values were fixed from a FER analysis through a CV-QKD simulation allowing for key extraction considering different FER levels. Lower FER values are associated with higher SNRs in the system and thus lower achievable transmission distances. Nonetheless, the FER maximizing the extraction key rate is not null. Our results show that the extraction key rate is maximized by SNR adjustment which should have in account both the reconciliation efficiency and the FER.**

***Index Terms*—Continuous variables, discrete modulation, quantum key distribution.**

I. Introduction

QUANTUM key distribution (QKD) can be used to distribute symmetric keys over optical links avoiding any computational assumption [1]. In the continuous variables (CVs) realm this can be provided by using weak coherent fields and off-the-shelf coherent detection [2], [3], [4], [5]. The use of discrete modulation (DM) alongside CV-QKD protocols is an attractive solution due to the possibility of using standard modulation formats, such as M-symbol (M-) quadrature amplitude modulation (QAM) and M- amplitude and phase shift keying (APSK) constellations. Such DM formats can approximate the theoretically optimal performance of Gaussian modulation (GM) [6], [7]. Nonetheless, to the best of our knowledge, the impact of the information reconciliation step, fundamental to retrieving symmetric keys from any QKD implementation, on the performance of higher-order DM-CV-QKD remains an open issue in the literature. CV-QKD systems were initially proposed using GM to model the quantum signal [4], [8]. GM is theoretically optimal in terms of secret key rate [9]. Nonetheless, the security proofs assume ideal GM, which is very difficult to achieve in practice due to the finite extinction ratio of the electro-optic modulators [10]. Moreover, ideal GM requires high amounts of randomness, which demands the use of extreme high-speed true random number generators [10]. On the other hand, DM-CV-QKD avoids these disadvantages, while keeping a simpler practical implementation [11], [12]. Early DM-CV-QKD systems, both theoretical and experimental, considered small-order DM formats such as 4-phase shift keying (PSK) and 8-PSK constellations [13]. Notwithstanding, these constellations are far from the optimal performance of GM [6]. The use of higher-order DM formats in CV-QKD was initially provided by authors in [6] focusing on M-QAM constellations. This work was latter extended in [7] considering M-APSK constellations, having into account finite-size effects. The performance of higher-order DM formats increases with the number of symbols in the constellation approaching GM's performance [7], [6]. Experimental demonstrations of 64-, 256-, and 1024-QAM for CV-QKD were performed in [14], [15], [16], with 1024-QAM being capable to extract 38.3 Mb/s over 9.5 km, considering finite-size effects [15]. On the other hand, 128-APSK has been experimentally demonstrated, albeit without the consideration of the finite-size effects [17]. Due to different considerations, the comparison between the different modulation formats is not straightforward. Thus, a performance comparison between DM formats in CV-QKD is also an open issue. Moreover, the experimental demonstrations of higher-order DM formats for secret keys extraction were obtained offline without the implementation of all post-processing

M. Almeida, D. Pereira, A. N. Pinto and N. A. Silva are with Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal. M. Almeida, D. Pereira, and A. N. Pinto are with Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal. M. Facão is with Department of Physics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal and with I3N, Department of Physics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal. N. A. Silva is with the University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal. 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), UIDB/50008/2020-UIDP/50008/2020 (action QuRUNNER and QUESTS), QuantaGenomics (QuantERA/0001/2021), and by I3N projects UIDB/50025/2020, UIDP/50025/2020 and LA/P/0037/2020.

Manuscript received April 00, 2021; revised August 00, 2021.

steps [14], [15], [16], [17]. As such, the obtained key rates do not account for the frame error rate (FER) in the system. Furthermore, state-of-the-art works in DM-CV-QKD such as [6], [7], [14], [15], [16], [17] assume a fixed value for the reconciliation efficiency parameter, leading to an under or over estimation of the key rates achieved by the system. This undervaluing the effect of the information reconciliation method and of the signal-to-noise ratio (SNR) of the system on the reconciliation efficiency parameter.

We assess the performance of probabilistic shaped 256-symbols DM CV-QKD systems. Considering the true value of the reconciliation efficiency, the performance of 256-QAM constellations closely approximates the optimum performance of GM. On the other hand, 256-APSK constellations are further apart from GM's performance. We found that maximizing the reconciliation efficiency leads to higher FER values, thus deteriorating the extraction key rate. Moreover, minimizing the FER does not maximize the final extraction key rate. To maximize the final extraction key rate of the DM-CV-QKD system, the SNR must be adjusted to allow a high reconciliation efficiency and a low FER. For 10 km, SNR values around 0.23 were found to lead to maximum key extraction rates.

This paper is organized as follows. In Section II we introduce the model considered to compute the secret key rate, accounting for the true value of the reconciliation efficiency. Section III briefly describes the DM formats and distributions considered for probabilistic shaping, alongside the DM-CV-QKD implemented simulation. In Section IV we present results considering the true value of the reconciliation efficiency. Finally, we study the extraction key rate of DM-CV-QKD systems considering the FER of the system. In Section V a brief conclusion is presented and directions for future work are discussed.

II. Secret Key Rate Model

The secret key rate of a CV-QKD system, K, can be computed from the difference between the mutual information between Bob and Alice, I_{BA}, and the Holevo bound between Bob and Eve, χ_{BE}. Since m states from the total number of transmitted states, N, are used to estimate the channel transmission, T, and excess noise, ξ, in the CV-QKD system, only $n = N - m$ states are used to extract the final binary key. As such, in the finite-size effect regime, the secret key rate of a CV-QKD system is given by [18]

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

where the impact of the finite-size blocks to obtain the secret key rate is considered by the $\Delta(n)$ parameter and by the use of the worst case estimators for the channel transmission, T and excess noise, ξ [18]. The $\Delta\left(n\right)$ parameter is related with the security of privacy amplification in the finite-size regime, being given by

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

where $\bar{\epsilon}$ is a *smoothing* parameter, and ϵ_{PA} is the failure probability of the privacy amplification procedure [18]. The limited number of exchanged states degrades Alice's and Bob's knowledge on the channel transmission, T, and excess noise, ξ [19]. As such, the analysis of the finite-size effects must also have into account the effect due to the parameter estimation step. This is provided by considering the lower bound of the channel transmission and the upper bound on the excess noise with a probability of at least $1 - \epsilon_{\mathrm{PE}}$ [18]. Moreover, the CV-QKD system can, at most, extract the amount of bits allowed by the information reconciliation process. Therefore, the mutual information between Bob and Alice, I_{BA}, must be multiplied by the reconciliation efficiency parameter, β. The reconciliation efficiency can be defined as $\beta = \frac{2R}{I_{\mathrm{BA}}}$, where R is the rate of bits that can be extracted from the information reconciliation step.

For GM, the mutual information between Bob and Alice can be computed as in [20], [21], while for DM we use [22]. On the other hand, for collective Gaussian attacks, the Holevo bound between Bob and Eve, χ_{BE}, can be computed as described by [23], through a proper definition of the Z^* parameter, required to compute χ_{BE}. For DM, the Z^* parameter can be computed following [6], through the knowledge of the density matrix τ that describes the average state sent by Alice, $\tau = \sum_k p_k |\alpha_k\rangle\langle\alpha_k|$, where p_k is the probability of Alice sending the state $|\alpha_k\rangle$. Thus, the Z^* parameter can be computed numerically using

$$Z^*(T,\xi) = 2\sqrt{T}\mathrm{Tr}\left(\tau^{1/2}\hat{a}\tau^{1/2}\hat{a}^\dagger\right) - \sqrt{2T\xi W}, \tag{3}$$

where $\mathrm{Tr}\left(X\right)$ is the trace of X, $W = \sum_k p_k\left(\langle\alpha_k|\hat{a}_\tau^\dagger\hat{a}_\tau|\alpha_k\rangle - |\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle|^2\right)$, and $\hat{a}_\tau = \tau^{1/2}\hat{a}\tau^{-1/2}$. For GM, the Z^* parameter is well known, being $Z^* = \sqrt{T\left(V_{\mathrm{A}}^2 + 2V_{\mathrm{A}}\right)}$ [23], [6], where V_{A} is the modulation variance.

III. DM-CV-QKD System

In this work we will study the regular and irregular 256-APSK, conventional 256-QAM and hexagonal regular and irregular 256-QAM (see Fig. 1). The regular 256-APSK contains 32 states per ring. The probabilistic shaping will consider the binomial and the Boltzmann-Maxwell distributions functions. For the M-APSK constellations, the ring's probability, P_p, is given by $P_p = \frac{2}{2^{(2Q-1)}}\binom{2Q-1}{Q-p}$ for the binomial distribution, where $\binom{n}{k}$ is the number of ways to choose k elements from a set of n elements, and by $P_p = \exp\left(-\nu\left(\frac{p}{Q}\right)^2\right)/\sum_p P_p$ for the Boltzmann-Maxwell distribution, with $p = 1, 2, ..., Q$, where Q is the number of rings in the constellation, and ν a parameter that needs to be optimized. The probability associated to each state of the constellation is $P_{p,k} = P_p/M_p$, with $k = 1, ..., M_p$ and M_p being the number of points in ring p. For the conventional M-QAM format, the binomial distribution is defined by choosing the probability of each state to be $P_{k,l} = \frac{1}{2^{(2Q-1)}}\binom{Q-1}{k}\binom{Q-1}{l}$, with $k, l = -1, -1+\frac{2}{Q}, -1+\frac{4}{Q}, ..., 1-\frac{4}{Q}, 1-\frac{2}{Q}, 1$ and $Q = \sqrt{M}$ being the number of levels in each quadrature. For the hexagonal M-QAM formats, the binomial distribution is defined by constructing a hexagonal grid, using two square grids with different

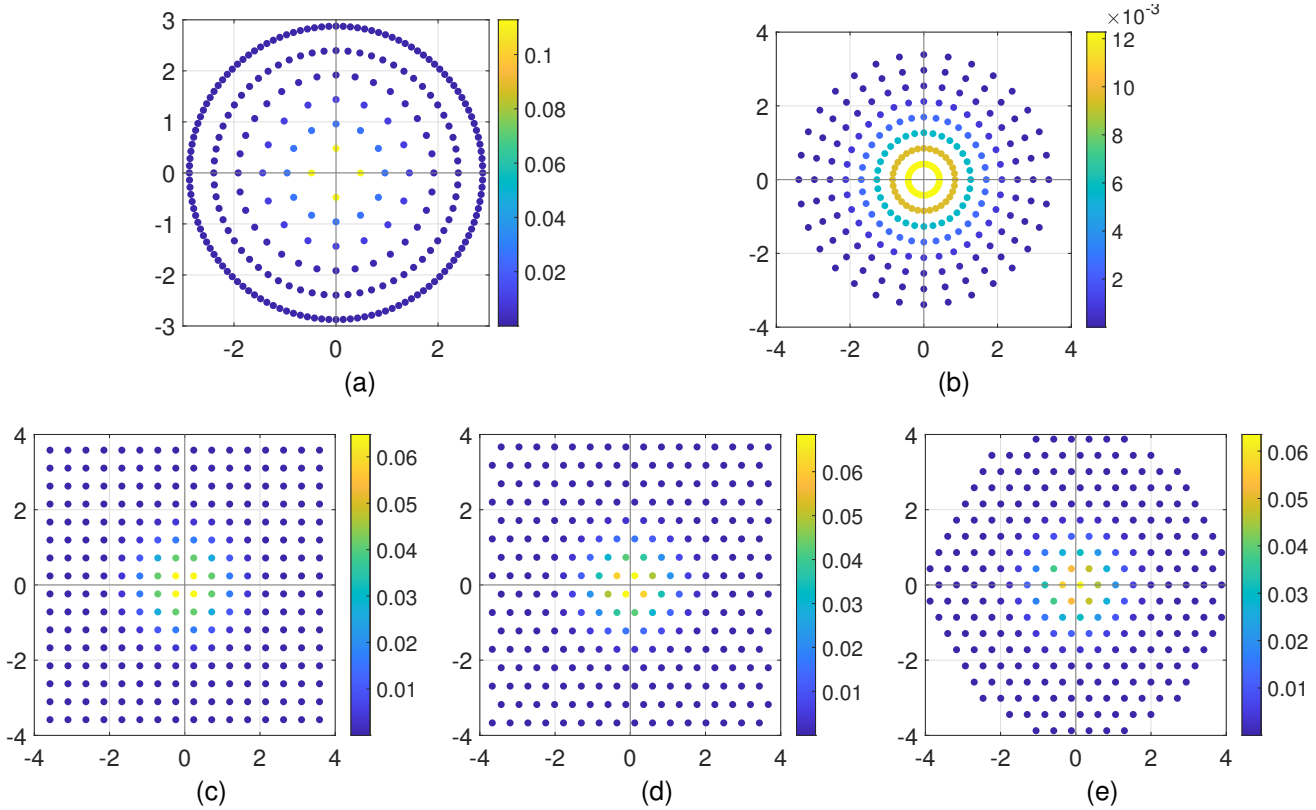

Fig. 1. Schematic representation of the DM formats considered in this work: (a) irregular 256-APSK, (b) regular 256-APSK, (c) conventional 256-QAM, (d) hexagonal regular 256-QAM, and (e) hexagonal irregular 256-QAM, where the color represents the probability of each symbol in the constellation. The probabilistic shaping was obtained considering the (a,b) binomial distribution and (c,d,e) the Boltzmann-Maxwell distribution, and a mean number of photons of 1 photon per symbol.

centers. The probability of the points nonexistent in the hexagonal constellation are then discarded, and the probabilities of the remaining points are scaled such that the total probability is unitary. For all M-QAM constellations, the Boltzmann-Maxwell distribution is applied by considering $P_{k,l} = \exp\left(-\nu\left(k^2+l^2\right)\right) / \sum_{k,l} P_{k,l}$.

At the physical layer of the DM-CV-QKD system, Alice prepares her sequence of states from the chosen DM format (Fig. 1). Alice then sends her states to Bob by the quantum channel, who measures the states. After the state's preparation, transmission and measurement, Alice and Bob apply post-processing techniques to distill a common secret key. The post-processing techniques are composed of parameter estimation, information reconciliation and privacy amplification.

In the parameter estimation step, the lower bound of the channel transmission and the upper bound of the excess noise, with a probability of at least $1-\epsilon_{\mathrm{PE}}$, are estimated from Alice's and Bob's shared states [18]. Here, ϵ_{PE} was chosen to be 10^{-10}. From this, the secret key rate can be easily estimated using (1), by substituting T and ξ by their lower and upper bound estimates. If the estimate of the secret key rate is positive, the method follows to information reconciliation. If not, the method is aborted.

Information reconciliation was applied by considering multi-dimensional reconciliation of dimension 8 as described in [24], [25], alongside the sum-product algorithm [24], [26]. Here we consider the multi-edge type (MET) low-density parity check (LDPC) codes of code rates 0.01, 0.02, 0.05, and 0.1 specified in Table I [27], [28]. MET-LDPC codes can be seen as a generalization of irregular LDPC codes [28], with performance close to the Shannon's limit in the low SNR regime [13], [28]. All MET-LDPC matrices used in this work were generated considering the Progressive-Edge Growth method [29]. At the end of the information reconciliation step we can compute the FER value of the system. The FER is given by the ratio between the number of uncorrected groups and the total number of groups after the information reconciliation step.

After information reconciliation, Alice and Bob own a weakly secret binary sequence W. Since Eve may contain some information on W, Alice and Bob perform privacy amplification. This is provided through the application of the Toeplitz extractor, using a uniformly random and non-secret seed s [30], [31]. The Toeplitz matrix, M, is applied to the weakly secret information vector W, returning a vector Z with almost uniform secret randomness, by doing $W \cdot M = Z$ [32]. Moreover, we apply fast-Fourier transforms to the Toeplitz extractor following the method described in [13]. The size of the extracted key Z is given by $\lfloor |W|\left(\beta I_{\mathrm{BA}} - \chi_{\mathrm{BE}} - \Delta(n)\right)\rfloor$, where $\lfloor\cdot\rfloor$ denotes the floor function and $|W|$ is W's length. With this, at the end of privacy amplification one is able to

TABLE I
MULTIVARIATE POLYNOMIAL PAIRS OF MET-LDPC CODES FOR THE CODE RATES OF 0.1 AND 0.05 PRESENTED IN [28] AND THE CODE RATES 0.02 AND 0.01 PRESENTED IN [27].

Code rate	Degree distribution
0.1	$\nu(\mathbf{x}) = 0.0775x_1^2x_2^{20} + 0.0475x_1^3x_2^{22} + 0.875x_3^1$ $\mu(\mathbf{x}) = 0.0025x_1^{11} + 0.0225x_1^{12} + 0.30x_2^2x_3^1 + 0.845x_2^3x_3^1$
0.05	$\nu(\mathbf{x}) = 0.04x_1^2x_2^{34} + 0.03x_1^3x_2^{34} + 0.93x_3^1$ $\mu(\mathbf{x}) = 0.01x_1^8 + 0.01x_1^9 + 0.41x_2^2x_3^1 + 0.52x_2^3x_3^1$
0.02	$\nu(\mathbf{x}) = 0.02x_1^2x_2^{51} + 0.02x_1^3x_2^{60} + 0.96x_3^1$ $\mu(\mathbf{x}) = 0.016x_1^4 + 0.004x_1^9 + 0.30x_2^3x_3^1 + 0.66x_2^2x_3^1$
0.01	$\nu(\mathbf{x}) = 0.01x_1^2x_2^{103} + 0.01x_1^3x_2^{125} + 0.98x_3^1$ $\mu(\mathbf{x}) = 0.008x_1^4 + 0.002x_1^9 + 0.32x_2^3x_3^1 + 0.66x_2^2x_3^1$

TABLE II
CHARACTERISTICS OF THE MET-LDPC CODES CORRESPONDING TO THE MULTIVARIATE POLYNOMIAL PAIRS PRESENTED IN TABLE I.

Code rate	Threshold	Minimum SNR	Maximum reconciliation efficiency
0.1	2.541 [28]	0.1549	96.26%
0.05	3.674 [28]	0.0741	96.97%
0.02	5.94 [27]	0.0283	98.32%
0.01	8.41 [27]	0.0141	99.01%

compute the extraction key rate, $K^{\text{extraction}}$, given by

$$K^{\text{extraction}} = \frac{n}{N}(1 - \text{FER})\left(\beta I_{\text{BA}} - \chi_{\text{BE}} - \Delta(n)\right). \quad (4)$$

The extraction key rate gives the rate at which the DM-CV-QKD system extracts key bits per symbol transmitted in the quantum channel, and should not be confused with the secret key rate. The secret key rate does not account for the information reconciliation step, while the extraction key rate does. Usually, the secret key rate is considered to study the performance of DM-CV-QKD systems, which is equivalent to assuming that the FER in the system is null. Nonetheless, the extraction key rate given by (4) is a better figure of merit of the performance of CV-QKD systems.

IV. RESULTS

The reconciliation efficiency, β, is the ratio of twice the code rate of the MET-LDPC code used for information reconciliation to the mutual information, i.e., $\beta = \frac{2R}{I_{\text{BA}}}$. As such, smaller SNRs in the system require smaller code rates for key extraction. Remark that each MET-LDPC code has a minimum SNR for which key extraction is possible. The minimum value of the SNR, $\text{SNR}_{\min}$, can be computed from the threshold, obtained by [27], [28] through density evolution, by doing $\text{SNR}_{\min} = 1/(\text{threshold}^2)$. The maximum reconciliation efficiencies are computed from the minimum value of the SNR assuming GM, since [27], [28] obtained the threshold parameter considering a Gaussian modulated CV-QKD system. Table II presents these characteristics for the MET-LDPC codes considered in this work.

For non-unity reconciliation efficiency, β, there is a trade-off between the mean number of photons per symbol and the key rate value. Such trade-off was analyzed for Gaussian modulation in [21], [33]. Despite such analysis, in the case of discrete modulation being out of our focus, we optimize the mean number of photons per symbol such that the secret key rate is maximized. This for each transmission distance, and considering the reconciliation efficiency value associated with the MET-LDPC code rate that was used.

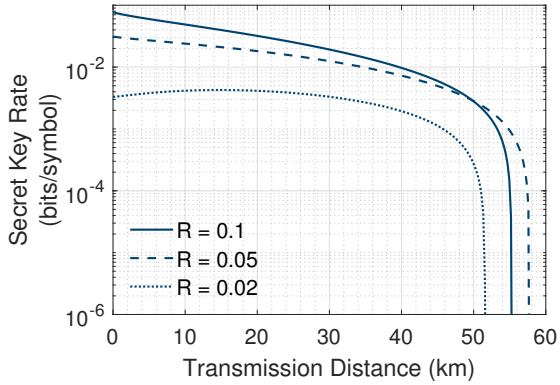

Fig. 2. Secret key rate given by (1) with the mean number of photons per symbol optimized as a function of the transmission distance for conventional 256-QAM. This considering the true value of the reconciliation efficiency for the code rates R of 0.1, 0.05, and 0.02. The code rate 0.01 has null secret key rate for all transmission distance range. The results were obtained considering the finite-size effect scenario, for a transmission coefficient of 0.2 dB km^{-1}, a detector's efficiency of 0.6, an excess noise value of 0.01 SNU, a thermal noise of 0.25 SNU, and a total of 10^8 transmitted states.

In this section, we present results for the secret key rate given by (1) and for the extraction key rate given by (4), considering numerical simulations of the DM-CV-QKD system using MET-LDPC codes for information reconciliation with different code rates. Moreover, we compare the results of the secret key rate given by (1) from the simulations with the theoretical ones. All these results consider the real value of the reconciliation efficiency parameter. We have considered the maximum values of reconciliation efficiency and the minimum values of SNR presented in Table II. The theoretical results are computed from the theoretical expressions, considering the lower bound of the channel transmission and the upper bound of the excess noise. For the results of the numerical simulations, the lower bound of the channel transmission and the upper bound of the excess noise are estimated from the comparison of Alice's and Bob's states.

Fig. 2 shows the secret key rate along transmission distance for different code rates for conventional 256-QAM using optimized mean number of photons per symbol. The code rate may be chosen in order to maximize the secret key rate. From the theoretical results of the secret key rate of Fig. 2 we can see that, for the various constellations under study, the MET-LDPC code with $R = 0.05$ performs better for longer transmission distances. In opposition, the MET-LDPC code with $R = 0.1$ allows higher secret key rates for shorter transmission distances. Remark that the secret key rate for $R = 0.1$ decreases faster than for $R = 0.05$. As such, for higher transmission distances, choosing a smaller code rate for the MET-LDPC code is beneficial. Nonetheless, further decreasing the code rate may not result in the extension of the maximum achievable transmission distance, as observed

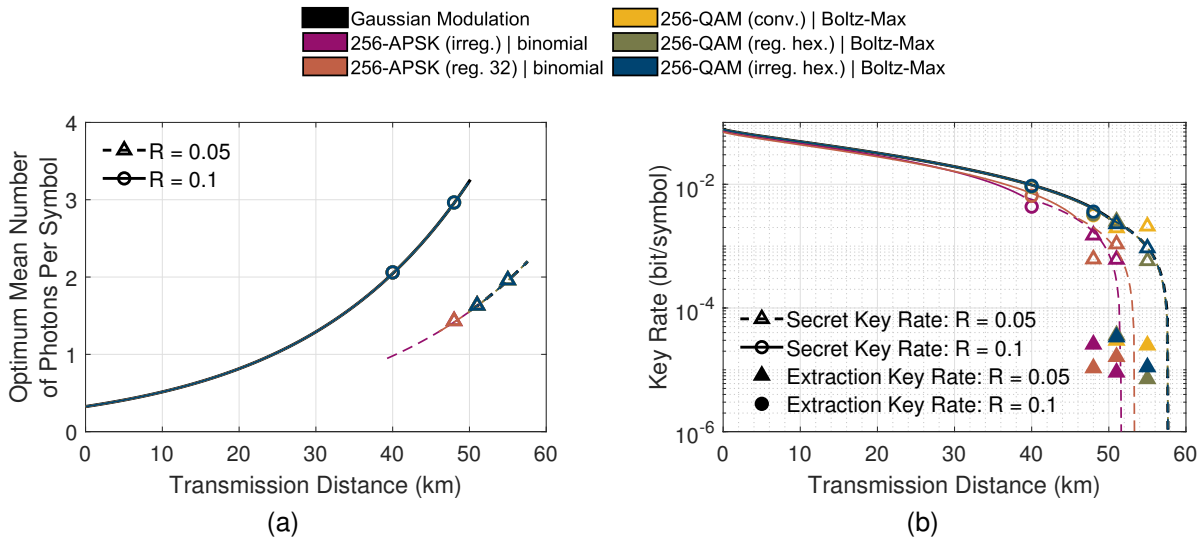

Fig. 3. (a) Optimum mean number of photons per symbol, and (b) secret key rate given by (1) and extraction key rate given by (4) having into account the FER in the system, as a function of the transmission distance. This considering the true value of the reconciliation efficiency for the code rates R of 0.1 and 0.05 that maximize the secret key rate. The code rates 0.02 and 0.01 are unable to maximize the secret key rate. Moreover, for $R = 0.1$ at 40 km, the simulation extracted no key (null extraction key rate) despite the positive secret key rate. The symbols correspond to results obtained from simulations while the lines correspond to theoretical results. The results were obtained considering the finite-size effect scenario, for a transmission coefficient of 0.2 dB km^{-1}, a detector's efficiency of 0.6, an excess noise value of 0.01 SNU, a thermal noise of 0.25 SNU, and a total of 10^8 transmitted states.

for $R = 0.02$. In fact, the decrease of the secret key rate due to the decrease of the code rate may be such that the secret key rate is null for all range of transmission distances, such as occurs for $R = 0.01$. As such, the MET-LDPC codes of code rates 0.02 and 0.01 do not maximize the secret key rate for any transmission distance. A proper choice of the code rate of the information reconciliation method is fundamental.

For both theoretical and numerical results, we have optimized the mean number of photons per symbol in order to maximize the secret key rate. The optimum mean number of photons per symbol is represented in Fig. 3a for the code rates R of 0.1, 0.05, 0.02, and 0.01 as a function of the transmission distance. The mean number of photons per symbol that maximizes the secret key rate given by (1) is statistically the same for all constellations considered. Fig. 3a presents a different evolution with the transmission distance than the one observed for the same figure of merit when fixing the reconciliation efficiency (see for instance Fig. 10 of [7]). Maximizing the secret key rate given by (1), when the true value of the reconciliation efficiency is considered, leads to an increase on the optimum mean number of photons per symbol with the transmission distance and with the code rate. For transmission distances above 25 km, the optimum mean number of photons per symbol is higher than 1 photon per symbol, allowing an easier practical implementation of the DM-CV-QKD system.

The optimization of the mean number of photons per symbol (Fig. 3a) is such that the SNR is approximately constant and kept close to the minimum value of SNR corresponding to the maximum value of the reconciliation efficiency (Table II). For the MET-LDPC code of code rate 0.1, this occurs for SNR values close to 0.15 allowing a reconciliation efficiency of 96.26% (Table II) for all range of transmission distance.

In Fig. 3b we present both theoretical results and numerical results from simulations of the secret key rate given by (1) as a function of the transmission distance considering the true value of the reconciliation efficiency and the finite-size effects for a total of $N = 10^8$ exchanged states. The numerical results were obtained in the parameter estimation step of simulations of the DM-CV-QKD system performed for transmission distances of 40, 48, 51 and 55 km. The secret key rate was maximized considering the mean number of photons per symbol and the code rate R of the MET-LDPC codes. Remark that such optimization in the simulation of the DM-CV-QKD, as in an experimental implementation, must assume channel's transmission and excess noise values. Nonetheless, the channel's transmission can be monitored in a practical implementation while the effect of the excess noise on the optimum value of the mean number of photons per symbol is small. For the various simulations we also present the extraction key rate given by (4) considering the FER in the system after information reconciliation.

From the results in Fig. 3b we can see that, regular 256-APSK performs better than irregular 256-APSK in terms of the secret key rate given by (1), but both are still far from the performance of GM (Fig. 3b). All three 256-QAM modulation formats are almost overlapped in terms of secret key rate with GM, thus approximately achieving optimal performance (Fig. 3b). Despite the difference between the different 256-QAM constellations being minimal, concerning the theoretical results, the hexagonal irregular one is the modulation format achieving the highest performance, being followed by the hexagonal regular and then by the conventional one. Remark that this may not be the case for the numerical results, since the secret and extraction key rates are estimated from the

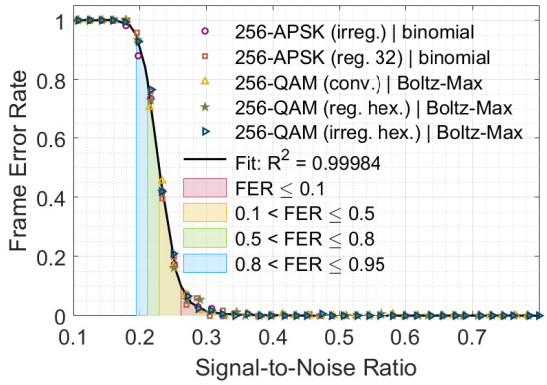

Fig. 4. FER as a function of the SNR for simulations of the DM-CV-QKD system using a MET-LDPC code with code rate 0.1 for information reconciliation. The fitted curve was fitted to all results obtained through the simulation. The shaded regions represent the SNR region for which the FER is smaller or equal than 0.1, 0.5, 0.8, and 0.95. The results were obtained for a transmission distance of 40 km, an attenuation of 0.2 dB km^{-1}, a detector's efficiency of 0.6, an excess noise value of 0.01 SNU, a thermal noise of 0.25 SNU, and a total of $N = 10^6$ states.

simulation, which may result in deviations from simulation to simulation. As an example, in the particular simulations here presented, for 55 km, conventional 256-QAM extracted more data than hexagonal irregular 256-QAM. Similarly, irregular 256-APSK achieved higher extraction key rate than the regular counterpart for 48 km, for the same code rate R.

Optimizing the mean number of photons to adjust the SNR to the code rate, allowing β close to 1, was beneficial to maximize the secret key rate but, due to the FER associated to the system's SNR, it was not optimal for the extraction key rate. Fig. 4 presents the FER as a function of the SNR considering a MET-LDPC code of code rate 0.1. A 40 km distance was considered and the SNR was allowed to vary due to the variation of the mean number of photons per symbol. The FER is unitary for SNR values tending to zero and null for higher values of SNR. For the MET-LDPC code with $R = 0.1$, the FER is unitary, thus not allowing key extraction, for SNR values smaller than 0.17. The minimal SNR for which error correction is possible is expected to decrease with the decrease of the code rate.

With this, the SNR of the system that maximizes the secret key rate when using the MET-LDPC code of code rate 0.1 is below the value allowing error correction (Fig. 4), resulting in an unitary FER value, thus not allowing key extraction. As such, for the simulations conducted for 40 km, a null extraction key rate given by (4) was obtained, despite the relatively high secret key rate value given by (1) (Fig. 3b). When considering the MET-LDPC code with $R = 0.05$, key extraction was possible since the FER was not unitary for the minimum SNR corresponding to the maximum value of the reconciliation efficiency. Even so, in this case the FER was close to unitary, thus resulting in a high reduction of the amount of extracted bits in the system given by (4), in relation to the secret key rate given by (1) (Fig. 3b). No simulations were conducted for transmission distances below 40 km, since the system was expected to extract no key for the code rates here considered, as long as minimum SNRs are used.

The study of the FER as a function of the SNR for the various MET-LDPC codes allowed the definition of minimum values of SNR for different FER levels, as done in Fig. 4 for the code rate 0.1. In Fig. 5a we present results for the secret key rate given by (1) and of the extraction key rate given by (4) for different transmission distances considering different FER levels, by fixing different minimum values of SNR. Fig. 5a also contains theoretical results for the secret key rate in the system. This considering regular and irregular 256-APSK with a binomial distribution, and conventional and hexagonal regular and irregular 256-QAM with Boltzmann-Maxwell distribution, concerning the true value of the reconciliation efficiency, and accounting for the finite-size effects.

To decrease the expected FER level in the system, the SNR must increase. This results in a decrease of the maximum achievable transmission distance considering the secret key rate given by 1 (Fig. 5a). From the simulations conducted for several transmission distances and the various 256-states constellations, we observe the decrease of the FER with the increase of the minimum SNR values fixed in the simulation of the system. The obtained FER values deviate from the expected values (Fig. 5a). Remark that far less exchanged states were used to model the FER as a function of the SNR than for the simulations of the DM-CV-QKD system. To model the FER as a function of the SNR only $N = 10^6$ states were considered due to time constraints, while for the simulations of the system a total of $N = 10^8$ of exchanged states was considered to achieve positive secret key rates while accounting for finite-size effects. Nonetheless, for the same transmission distance the differences in the FER between constellations are minimal.

By increasing the SNR in the system, the FER decreases, and the extraction key rate given by (4) approximates the value of the estimated secret key rate given by (1) (Fig. 5). Remark that, since a smaller range of transmission distance is considered through the increase of the SNR, the secret key rate is maximized only using the MET-LDPC code of code rate 0.1. It is also of interest to notice that, increasing the minimum SNRs of the system, irregular 256-APSK achieves higher performances than regular 256-APSK. Moreover, the increase of the SNR in the system also results in a decrease of the reconciliation efficiency. From the FER level of 0.95 to the level of 0.1, resulting in a mean FER of 0.842 and 0.036, respectively, for 10 km, the reconciliation efficiency decreases from 0.75 to 0.59. For the minimum value of SNR, the reconciliation efficiency was expected to be close to 0.96. Nonetheless, such decrease of the reconciliation efficiency is compensated with the decrease of the FER in the system, which results in higher extraction key rates.

Despite the decrease of the FER value, for higher minimum SNR values allowed in the system, resulting in an approximation of the extraction key rate given by (4) to the secret key rate given by (1), the secret key rate of the system also decreases. As such, a point is reached for which the increase of the SNR is no longer attractive (See the results of the simulation undertaken for 10 km of Fig. 5). By increasing the SNR of the system from 0.20 to 0.21 for the MET-LDPC code

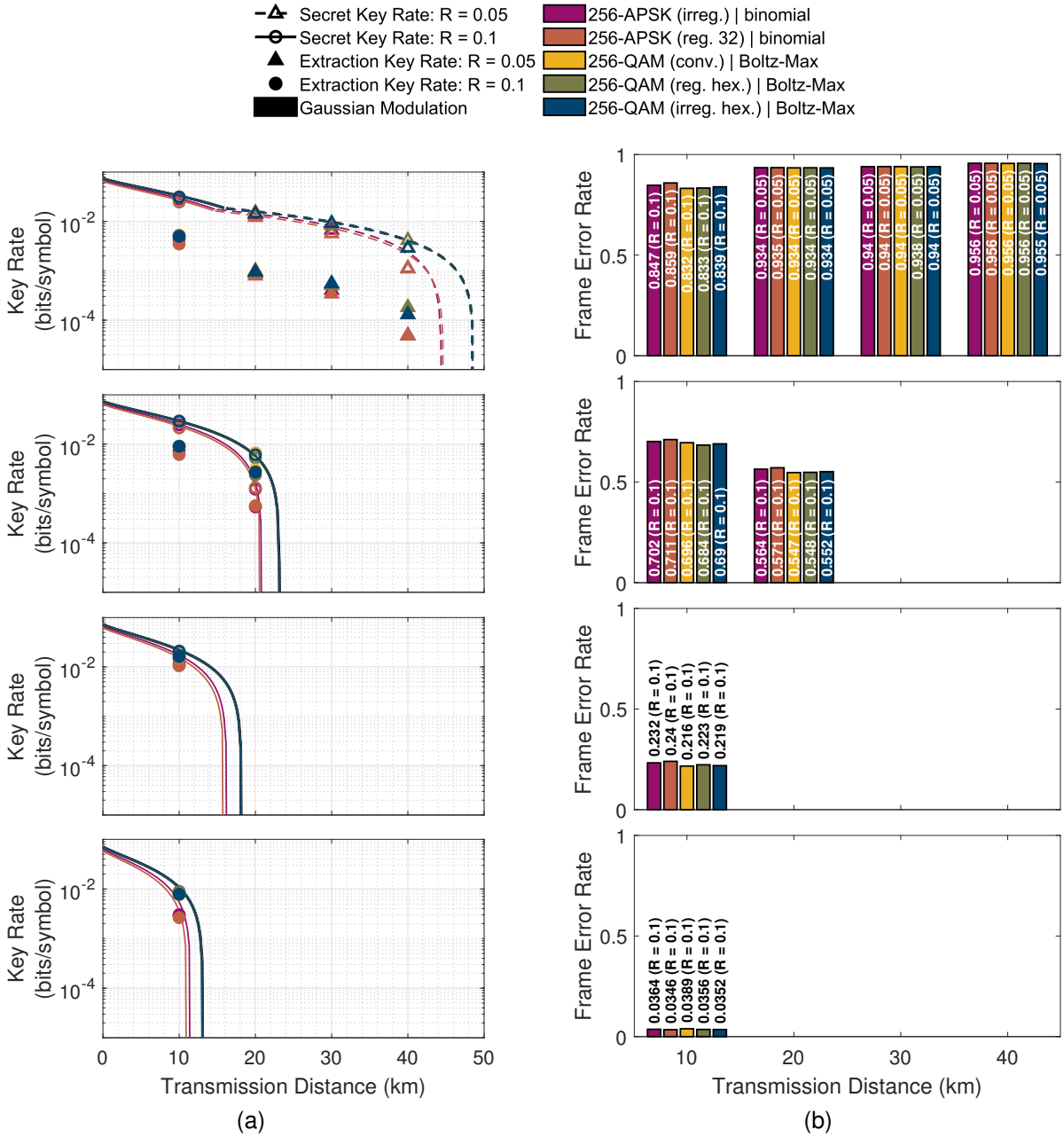

Fig. 5. (a) Secret and extraction key rates and (b) FER obtained from the complete simulation of the DM-CV-QKD system, for regular and irregular 256-APSK with binomial distribution for probabilistic shaping, and conventional and hexagonal regular and irregular 256-QAM with Boltzmann-Maxwell distribution for probabilistic shaping for different transmission distances concerning the true value of the reconciliation efficiency, and accounting for the finite-size effects. (a) also presents theoretical secret key rate results. This for the SNRs associated to the different FER levels of, from top to bottom: 0.95, 0.8, 0.5, and 0.1.

of code rate 0.1, associated to the FER levels of 0.95 and 0.8, respectively (Fig. 5), one observes an increase of the extraction key rate given by (4) despite the decrease on the secret key rate given by (1). For the hexagonal irregular 256-QAM, this increase is of 0.004 bits per symbol. By increasing once again the minimum SNR from 0.21 to 0.23, associated to the FER levels of 0.8 and 0.5, respectively (Fig. 5), an increase is again observed. For the hexagonal irregular 256-QAM, the extraction key rate increases from 0.009 to 0.016 bits per symbol due to the increase of the system's SNR. However, further increasing the SNR value to 0.26 to reach the FER level of 0.1 (Fig. 5), smaller extraction key rates are obtained. In this case, for the hexagonal irregular 256-QAM, the extraction key rate decreases to 0.008 bits per symbol. Perfect error correction, i.e., a null FER, is not advantageous to maximize the extraction key rate given by (4) due to the effect of the true value of the reconciliation efficiency on the secret key rate. To maximize the extraction key rate of a CV-QKD system, one must not restrict the analysis to the maximization of the secret key rate according to the mean number of photons per symbol for a specific transmission distance. One must also consider the expected FER value and the effect of the reconciliation efficiency on the secret key rate to properly acknowledge the extraction key rate given by (4). As future work, higher

code rates should be considered, since this may allow for even higher key rates for small transmission distances. Such is specially interesting for metropolitan communication lines. Moreover, other information reconciliation methods could be studied and compared with multidimensional reconciliation when considering DM CV-QKD, in particular methods combining different codes rates or with varying code rates.

V. Conclusion

We studied the secret key rate of various 256-symbols DM formats with different probabilistic shaping, considering the true value of the reconciliation efficiency. The highest achievable transmission distances were obtained for M-QAM constellations considering the Boltzmann-Maxwell distribution and for M-APSK considering the binomial distribution. M-QAM constellations, namely conventional and regular and irregular hexagonal M-QAM, achieve higher performance than M-APSK constellations, namely regular and irregular M-APSK. The 256-QAM constellations are almost indistinguishable from the performance of GM. When considering the true value of the reconciliation efficiency, different MET-LDPC code rates maximize the secret key rate for different transmission distance ranges. The code rate maximizing the secret key rate and the reconciliation efficiency decreases with the transmission distance. Nonetheless, this is associated to small values of SNR, resulting in higher FER values, not allowing for key extraction. Thus, higher SNR values must be considered, even if resulting in the decrease of the reconciliation efficiency. The higher the SNR, the smaller the FERs, and the closer the extraction key rate, at the end of the privacy amplification step, is to the secret key rate estimated in the parameter estimation step. Nonetheless, the minimization or even nullification of the FER does not maximize the extraction key rate. The maximization of the extraction key rate is achieved using high reconciliation efficiency, but also low FER, which requires a compromise on the SNR value. More possibilities of code rates for the MET-LDPC codes can be considered depending on the target distance, which may be less vulnerable to high FER values. As future work, we intend to study not only higher code rates in multidimensional reconciliation, but also different information reconciliation methods, alongside DM CV-QKD systems. The use of adaptable reconciliation methods might also be of interest to achieve higher transmission distances. Remark that different reconciliation methods require different parameters to be optimized for the maximization of the extraction key rate. Besides that, eavesdropper attacks in addiction to the collective ones presented in this work should also be considered.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, p. 1012, Dec. 2020.

[3] M. Almeida, D. Pereira, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of imperfect homodyne detection on measurements of vacuum states shot noise," *Opt. Quant. Electron.*, vol. 52, no. 11, p. 503, Nov. 2020.

[4] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, Jan. 2002.

[5] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of receiver imbalances on the security of continuous variables quantum key distribution," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 22, Dec. 2021.

[6] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, Sep. 2021.

[7] M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, and N. A. Silva, "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution," *Opt. Express*, vol. 29, no. 23, p. 38669, Nov. 2021.

[8] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, p. 010303, Dec. 1999.

[9] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 84, no. 6, p. 062317, Dec. 2011.

[10] E. Kaur, S. Guha, and M. M. Wilde, "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 103, no. 1, p. 012412, Jan. 2021.

[11] J. Lin and N. Lütkenhaus, "Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution," *Phys. Rev. Applied*, vol. 14, no. 6, p. 064030, Dec. 2020.

[12] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *npj Quantum Inf*, vol. 4, no. 1, pp. 1–9, Apr. 2018.

[13] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," *Opt. Express*, vol. 28, no. 22, p. 32882, Oct. 2020.

[14] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, "High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM," in *2021 European Conference on Optical Communication (ECOC)*. IEEE, Sep. 2021, pp. 1–4.

[15] F. Roumestan, A. Ghazisaeidi, J. Renaudier, P. Brindel, E. Diamanti, and P. Grangier, "Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution," in *Optical Fiber Communication Conference (OFC) 2021*. Optica Publishing Group, 2021, p. F4E.1.

[16] F. Roumestan, A. Ghazisaeidi, H. Mardoyan, J. Renaudier, E. Diamanti, and P. Grangier, "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 (OFC) 2022*. Optica Publishing Group, 2022, p. Tu3I.4.

[17] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres," *Opt. Lett.*, vol. 47, no. 15, pp. 3948–3951, Aug. 2022.

[18] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, no. 6, p. 062343, Jun. 2010.

[19] A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, "Composably secure data processing for Gaussian-modulated continuous variable quantum key distribution," *Phys. Rev. Research*, vol. 4, no. 1, p. 013099, Feb. 2022.

[20] S. Ghorai, E. Diamanti, and A. Leverrier, "Composable security of two-way continuous-variable quantum key distribution without active symmetrization," *Phys. Rev. A*, vol. 99, no. 1, p. 012311, Jan. 2019.

[21] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, p. 042305, Oct. 2007.

[22] R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks," *J. Lightwave Technol.*, vol. 28, no. 4, pp. 662–701, Feb. 2010.

[23] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, "Continuous-variable quantum key distribution protocols with eight-state discrete modulation," *Int. J. Quantum Inform.*, vol. 10, no. 01, p. 1250004, Feb. 2012.

[24] Y. Feng, Y.-J. Wang, R. Qiu, K. Zhang, H. Ge, Z. Shan, and X.-Q. Jiang, "Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 103, no. 3, p. 032603, Mar. 2021.

[25] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, p. 042325, Apr. 2008.
[26] G. Limei, R. Qi, J. Di, and H. Duan, "QKD iterative information reconciliation based on LDPC codes," *Int. J. Theor. Phys.*, vol. 59, no. 6, pp. 1717–1729, Jun. 2020.
[27] H. Mani, "Error reconciliation protocols for continuous-variable quantum key distribution," Ph.D. dissertation, Tech. Univ. of Denmark, Dec. 2020.
[28] X. Wang, Y.-C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," *Quantum Inf. Comput.*, vol. 17, no. 13&14, pp. 1123–1134, 2017.
[29] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Improved construction of irregular progressive edge-growth Tanner graphs," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1155–1157, Dec. 2010.
[30] D. Aggarwal, Y. Dodis, Z. Jafargholi, E. Miles, and L. Reyzin, "Amplifying privacy in privacy amplification," in *Advances in Cryptology – CRYPTO 2014*, vol. 8617. Springer Berlin Heidelberg, 2014, pp. 183–198.
[31] Q. Li, B.-Z. Yan, H.-K. Mao, X.-F. Xue, Q. Han, and H. Guo, "High-speed and adaptive FPGA-based privacy amplification in quantum key distribution," *IEEE Access*, vol. 7, pp. 21 482–21 490, 2019.
[32] X. Zhang, Y.-Q. Nie, H. Liang, and J. Zhang, "FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers," in *2016 IEEE-NPSS Real Time Conference (RT)*, Jun. 2016, pp. 1–5.
[33] V. C. Usenko and R. Filip, "Squeezed-state quantum key distribution upon imperfect reconciliation," vol. 13, no. 11, p. 113007. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/13/11/113007