Pereira et al. *EPJ Quantum Technology* (2023) 10:20
https://doi.org/10.1140/epjqt/s40507-023-00176-z

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Impact of transmitter imbalances on the security of continuous variables quantum key distribution

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

*Correspondence:
danielfpereira@ua.pt
[1] Instituto de Telecomunicações, University of Aveiro, Campus de Santiago, 3810-193, Aveiro, Portugal
[2] Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus de Santiago, 3810-193, Aveiro, Portugal

Abstract

Continuous-variable quantum key distribution (CV-QKD) provides a theoretical unconditionally secure solution to distribute symmetric keys among users in a communication network. However, the practical devices used to implement these systems are intrinsically imperfect, and, as a result, open the door to eavesdropper attacks. In this work, we study the impact of transmitter stage imperfections on the performance and security of a Discrete Modulated (DM) CV-QKD system using M-symbol Quadrature Amplitude Modulation (M-QAM) and Amplitude and Phase Shift Keying (M-APSK) coupled with Probabilistic Constellation Shaping (PCS). Assuming two different modulation stage topologies, we first deform the constellations and then evaluate the secure key rate achievable with the deformed constellation. The presented results show that, due to the erroneously estimated channel parameters, non-monitored imbalances greatly reduce the system's performance, with situations where Bob and Alice estimate that no secure bits can be obtained while the real value of the key rate is still positive. Our results show the importance of monitoring these constellation imbalances and show that the optimal constellation may vary depending on the degree of device imperfection.

Keywords: Continuous variables; Quantum key distribution; Device imperfections; Excess noise; Discrete modulated; Probabilistic constellation shaping

1 Introduction

Continuous Variables Quantum Key Distribution (CV-QKD) tackles the problem of the generation and distribution of symmetric cryptographic keys without assuming any computational limitations on a supposed adversary [1], doing so while employing standard telecom equipment [2]. However, the security of CV-QKD is highly dependent on the channel noise level [3]. Channel noise is not exclusively noise that originates in the channel, but also includes noise originating from the transmitter which then travels through the quantum channel [4]. Therefore, a precise characterization of the transmitter is necessary for the implementation of efficient and secure CV-QKD systems [4, 5].

Coherent-state CV-QKD typically encodes the information in the phase and amplitude of weak coherent states, thus allowing for implementation with current modulation methods [3]. The first implementations of CV-QKD protocols were carried out by using a transmitted local oscillator (LO) setup [6]. However, that was found to open security loopholes [7–11]. As a result, local LO (LLO) techniques, are today the most common implementations of CV-QKD [12]. Lately, LLO CV-QKD implementations using single-sideband modulation with true heterodyne detection and using root-raised-cosine (RRC) signal modulation have been proposed, avoiding low-frequency and out-of-band noise [12–14]. Misalignments between the polarizations of the two laser fields interfering in the coherent detection scheme will severely reduce the efficiency of the detection scheme employed [15]. To tackle this, both active [15] and passive [13] solutions have been proposed. Coherent state CV-QKD can be grouped into Gaussian modulated (GM) or discrete modulated (DM) [3] methods. GM-CV-QKD based systems allow for maximizing the transmitted information, as a result exhibiting an optimal theoretical secure key rate and resistance to excess noise [3]. However, GM-CV-QKD protocols put an extreme burden on the transmitter's random number source [16] and tend to be more susceptible to imperfect state preparation [17]. As a result, the majority of the experimental work done in CV-QKD uses DM [18]. In [3], a proof of security for 2-state and 4-state CV-QKD against collective attacks, while assuming a linear channel model, was presented, where the security is evaluated via the channel parameters (transmission and excess noise), with this method being further adapted into an 8-state protocol in [19]. A generalization towards non-linear channel assumptions were presented for 4-state CV-QKD in [20, 21], and were further expanded for arbitrary modulation formats in [22]. Based on this last expanded proof, systems using M-symbol quadrature amplitude modulation (M-QAM) [23] and M-symbol Amplitude and Phase Shift Keying (M-APSK) [14, 24], both coupled with probabilistic constellation shaping (PCS), have been proposed and implemented. For both M-QAM and M-APSK constellations, the larger the cardinality, M, the closer the performance of the system will come to that of the GM scenario [23, 24]. But in all these scenarios, the optical system itself is assumed to be perfectly balanced [3, 4, 14, 19, 23, 24]. The effect of receiver imbalances on the security and performance of DM-CV-QKD has been explored previously, being shown that, due to an incorrect estimation of the receiver shot noise, they can pose a security threat or otherwise reduce the performance of the system [25]. Meanwhile, in [26–28], the authors studied the impact of different receiver imbalances on multiple parameters of the output voltage of the receiver. Conversely, studies on the impact of imperfect state preparation in GM-CV-QKD have been done, examining the impact these have on the estimated channel parameters and, subsequently, on its estimated performance [17, 29–33]. A study on the impact of transmitter stage imperfections on DM-CV-QKD was made in [34], also considering the impact of the imperfections on the estimated channel parameters. Nevertheless, these previous studies do not take into account the inherent security of the deformed constellations.

In this paper, we describe the impact of transmitter device imperfections at the transmitter side on the security and performance of a DM-CV-QKD system. The constellations 1024-QAM, 256-QAM, 64-QAM and 256-APSK(reg32) and 256-APSK(reg64) are considered, using PCS following a Maxwell–Boltzmann distribution. We show that, in a naive scenario where Alice and Bob trust their imperfect devices, the performance of the system degrades very quickly, with deviations of 5% from the ideal value being enough to completely incapacitate the system.

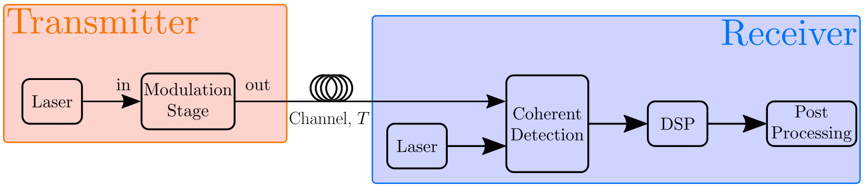

Figure 1 High level block diagram of a coherent state CV-QKD system. Channel, T: Transmission channel with transmission coefficient T, DSP: digital signal processing

This work is divided into four sections. In Sect. 2, we describe the two generic modulation stages under analysis and identify the sources of imperfections under study. In Sect. 3, we present a framework showing how to compute the channel parameters and associated secret key rate while under the effect of device imperfections and present results showing the impact of the previously identified imbalances on the performance and security of the system. We finalize this work with a summary of the major conclusions in Sect. 4.

2 Modulation stage imperfections

In this section, we describe the theoretical model used to describe the role of modulation stage imperfections on the performance of a DM-CV-QKD system. We present the impact of those imbalances on the shape of a 256-QAM constellation in order to illustrate the problem. The 256-QAM constellation is chosen because it has a high-cardinality and, due to it being square, deformations to it are simple to identify.

A high-level, simplified diagram of a prepare and measure CV-QKD system is presented in Fig. 1. The transmitter stage is comprised of a laser source, which generates a coherent signal that is then modulated in a generic modulation stage. The modulated signal is then transmitted through a channel with a transmission coefficient of T. At the receiver assembly, the modulated signal is evaluated with the help of a reference tone extracted from a local laser source, with which it is mixed in a coherent detection assembly, which may consist of an intradyne or heterodyne receiver. The output of the balanced receiver is subjected to a Digital Signal Processing (DSP) stage, at the end of which the transmitted constellation is recovered. Measurements performed at the receiver are used to estimate the channel parameters, which is a fundamental step to obtain the secure key rate. The modulation stage mentioned in Fig. 1 can take different forms. For the purposes of this work two different modulation methods are assumed: (1) an Amplitude Modulator (AM) connected in tandem with a Phase Modulator (PM); (2) a single In-phase and Quadrature (IQ) Modulator. Both modulation methods can be fully described as systems of Beam Splitters (BSs) and PMs. For the diagrams presented in this work, the BSs are presented as teal squares labeled by their transmission coefficient, η_i, while the PMs are presented as yellow rectangles with rounded corners labeled by the complex exponential that describes their action on the signal, $e^{i(\phi_i(t)+\phi_{\text{bias}_i})}$, where $\phi_i(t)$ is the time-varying phase that is intended to be imparted on the signal and ϕ_{bias_i} is a constant factor that sets the phase added to the signal, assuming that $\phi_i(t) = 0$.

A low-level block diagram of an AM&PM pair is presented in Fig. 2, assuming the AM to be in a push-pull configuration. The input signal is first split in the η_1 BS, with the reflected component having the phase $\phi_1(t) + \phi_{\text{bias}_1}$ imparted on it and the transmitted one the phase $\phi_2(t) + \phi_{\text{bias}_2}$. After these individual phase modulations, the two resulting

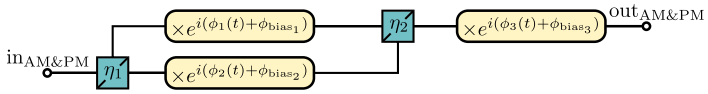
$\text{in}_{\text{AM\&PM}}$
η_1
$\times e^{i(\phi_1(t)+\phi_{\text{bias}_1})}$
$\times e^{i(\phi_2(t)+\phi_{\text{bias}_2})}$
η_2
$\times e^{i(\phi_3(t)+\phi_{\text{bias}_3})}$
$\text{out}_{\text{AM\&PM}}$

Figure 2 Low level block diagram of an Amplitude- and Phase-modulator based modulation stage

signals are combined again in the second BS with transmission coefficient η_2. The interference that occurs at this combination is what accomplishes the amplitude modulation. The amplitude modulated signal is then subjected to one last phase rotation of $\phi_3(t) + \phi_{\text{bias}_3}$. The in-out relations of a generic AM&PM pair can be described as

$$\begin{aligned}\text{out}_{\text{AM\&PM}} = \Big[&\sqrt{\eta_1(1-\eta_2)}e^{i(\phi_1(t)+\phi_{\text{bias}_1})} \\ &+ \sqrt{(1-\eta_1)\eta_2}e^{i(\phi_2(t)+\phi_{\text{bias}_2})}\Big]e^{i(\phi_3(t)+\phi_{\text{bias}_3})}\text{in}_{\text{AM\&PM}}. \end{aligned} \tag{1}$$

Note that, from a theoretical point of view, the relative position of the AM and PM is arbitrary, as the resulting in-out relations will be the same. In an ideal balanced scenario, we would have $\eta_1 = \eta_2 = 0.5$, $\phi_1(t) = -\phi_2(t)$, $-\phi_{\text{bias}_1} = \phi_{\text{bias}_2} = \pi/2$ and $\phi_{\text{bias}_3} = 0$. In this scenario, (1) would simplify to

$$\text{out}_{\text{AM\&PM}} = \sin\big(\phi_1(t)\big)e^{i\phi_3(t)}\text{in}_{\text{AM\&PM}}. \tag{2}$$

A further factor is that, in order for the desired constellation to be faithfully recreated, $\phi_1(t)$ should contain the arcsin of the desired amplitude levels, in order to prevent the appearance of non-linearities in the AM, and $\phi_3(t)$ should be fully driven, i.e. it should make a full rotation from $-\pi$ to π.

The deformation of a regular 256-QAM constellation, taking into account different imbalance types, in the AM&PM scenario is presented in Fig. 3. In Fig. 3(a) the ideal regular 256-QAM constellation is a schematically represented for comparison. Figure 3(b) shows the constellation generated when the internal BSs are imbalanced, for this particular constellation $\eta_1 = 0.6$ and $\eta_2 = 0.5$ were assumed. In this situation, the signals in each arm of the AM will have different amplitudes, thus impacting the interference that occurs at the η_2 BS, inhibiting the destructive interference. Note that if $\eta_1 \neq 0.5$ and $\eta_2 \neq 0.5$ but $\eta_1 + \eta_2 = 1$, the output constellation will appear with a lower amplitude but otherwise unaffected, having no effect on the system's performance. Figure 3(c) shows the constellation generated when the bias points of the individual PMs of the AM are incorrectly set. For the particular constellation considered in Fig. 3(c), $\phi_{\text{bias}_1} = -\frac{2\pi}{5}$ and $\phi_{\text{bias}_2} = \frac{\pi}{2}$ were assumed. Again, the interference that occurs at the η_2 BS is impacted, as the signals at each arm are no longer in phase opposition. Figure 3(d) shows the constellation generated when the signals driving the two individual PMs of the AM have different amplitudes. For the particular constellation in Fig. 3(d), $\phi_1(t) = -1.2\phi_2(t)$ was assumed. In this situation we observe deformation from the non-linear nature of complex exponentials. Finally, Figs. 3(e) and (f) show the constellation generated when the PM is either over- or under-driven, i.e. $\phi_3(t)$ is not contained in or is not capable of filling the $[-\pi,\pi]$ domain, respectively. In Fig. 3(e) we assume that the PM is over-driven by a factor of 20%, resulting in the overlapping of constellation points in the 2nd and 3rd quadrants. Conversely, in Fig. 3(f) we assume that

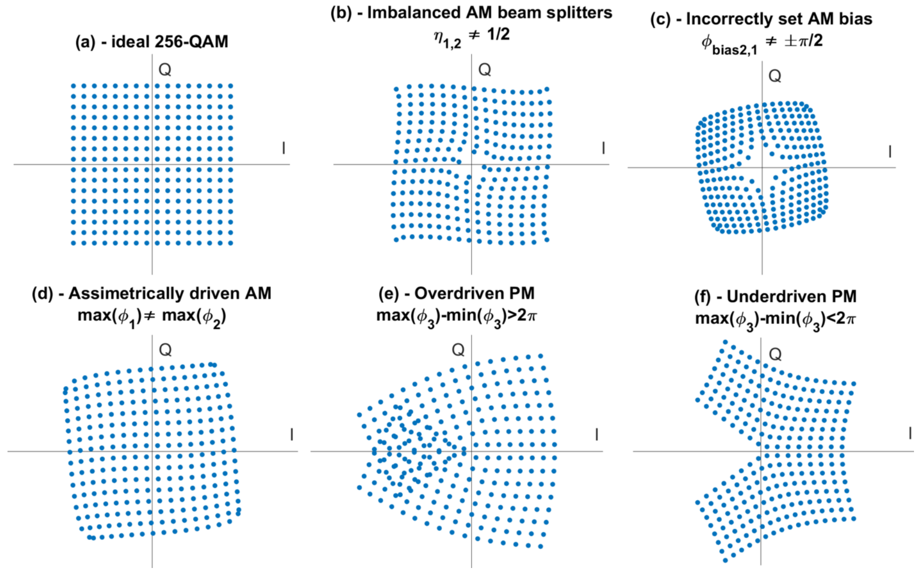

Figure 3 Exemplary deformed 256-QAM constellations for multiple imbalanced AM&PM scenarios

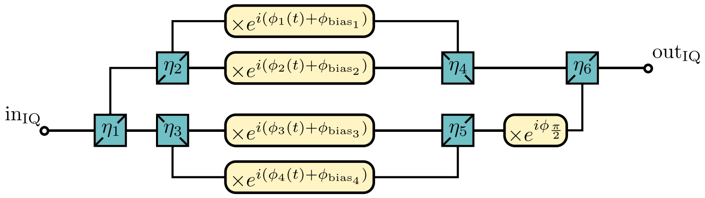
in_{IQ}
η_1
η_2
η_3
η_4
η_5
η_6
$\times e^{i(\phi_1(t)+\phi_{\text{bias}_1})}$
$\times e^{i(\phi_2(t)+\phi_{\text{bias}_2})}$
$\times e^{i(\phi_3(t)+\phi_{\text{bias}_3})}$
$\times e^{i(\phi_4(t)+\phi_{\text{bias}_4})}$
$\times e^{i\phi_{\frac{\pi}{2}}}$
out_{IQ}

Figure 4 Low level block diagram of an IQ-modulator based modulation stage

the PM is under-driven by a factor of 20%, which results in a slice of the 2nd and 3rd quadrants to not be reachable, causing the constellation to have an open region. An incorrectly set ϕ_{bias_3} will result in a simple rotation of the whole constellation. Since this can be easily compensated in DSP [12], this effect is not considered further in this work.

A low-level block diagram of an IQ Modulator is present in Fig. 4. An IQ Modulator can be seen as a pair of nested AMs, with one modulating the in-phase and the other the quadrature component of the signal. To accomplish this, the input signal is first split in the η_1 BS, with each output of being subjected to the same amplitude modulation process described previously in the AM&PM scenario. The output of the lower AM in Fig. 4 is then subjected to a phase rotation of $\phi_{\frac{\pi}{2}}$ before it is combined with the output of the upper AM. The in-out relations of a generic IQ Modulator can be described as

$$\begin{aligned}\text{out}_{\text{IQ}} = \Big\{&\sqrt{\eta_1(1-\eta_6)}\Big[\sqrt{(1-\eta_2)(1-\eta_4)}e^{i(\phi_1(t)+\phi_{\text{bias}_1})} + \sqrt{\eta_2\eta_4}e^{i(\phi_2(t)+\phi_{\text{bias}_2})}\Big] \\ &+ \sqrt{(1-\eta_1)\eta_6}\Big[\sqrt{\eta_3\eta_5}e^{i(\phi_3(t)+\phi_{\text{bias}_3})} + \sqrt{(1-\eta_3)(1-\eta_5)}e^{i(\phi_4(t)+\phi_{\text{bias}_4})}\Big]\Big\}\text{in}_{\text{IQ}} \qquad (3)\end{aligned}$$

In an ideal, balanced scenario, we would have $\eta_1 = \eta_2 = \eta_3 = \eta_4 = \eta_5 = \eta_6 = 0.5$, $\phi_1(t) = -\phi_2(t)$, $\phi_3(t) = -\phi_4(t)$, $-\phi_{\text{bias}_1} = \phi_{\text{bias}_2} = -\phi_{\text{bias}_3} = \phi_{\text{bias}_4} = \pi/2$ and $\phi_{\frac{\pi}{2}} = \frac{\pi}{2}$. In this scenario,

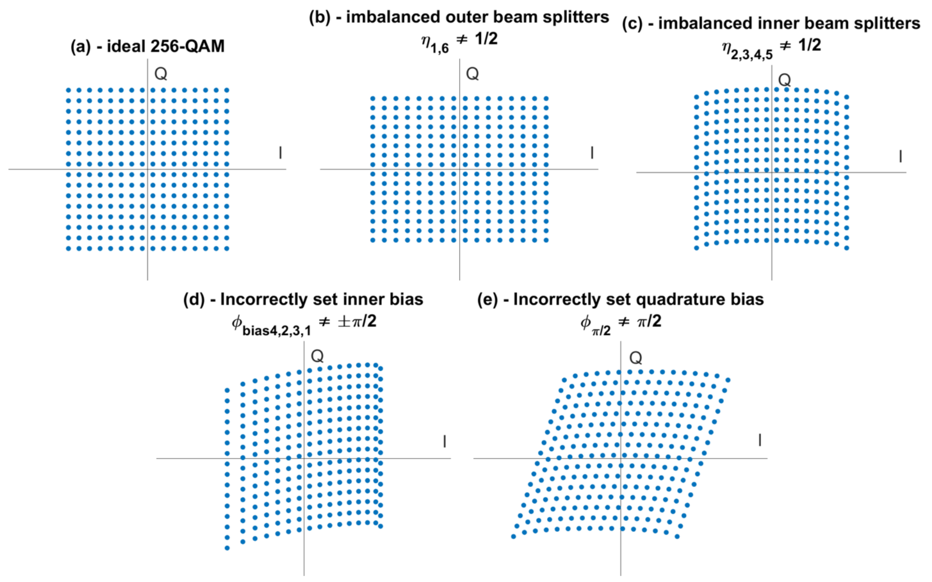

Figure 5 Exemplary deformed 256-QAM constellations for multiple imbalanced IQ scenarios

(3) would simplify to

$$\text{out}_{\text{IQ}} = \left[\sin\left(\phi_1(t)\right) + i\sin\left(\phi_3(t)\right)\right]\text{in}_{\text{IQ}}. \tag{4}$$

Again, a further factor is that $\phi_1(t)$ and $\phi_3(t)$ should contain the arcsin of the desired amplitude levels.

The deformation of the constellation caused by different imbalances in the IQ scenario is presented in Fig. 5. Again we include an ideal regular 256-QAM constellation for comparison, presented in Fig. 5(a). Figure 5(b) shows the constellation generated when the external BSs (external in relation to the nested AMs, i.e. η_1 and η_6) of the IQ are imbalanced. For this particular constellation $\eta_1 = 0.6$ and $\eta_6 = 0.5$ were assumed. In this situation, the signals in each nested AM will have different amplitudes, resulting in the output constellation having *stretched out* appearance. Note that, analogously to what occurs in the AM+PM scenario, if $\eta_1 = \eta_6$, the output constellation will appear with a lower amplitude but otherwise unaffected, having no effect on the system's performance. Figure 5(c) shows the constellation generated when internal BSs are imbalanced. For this particular constellation $\eta_2 = 0.6$ and $\eta_3 = \eta_4 = \eta_5 = 0.5$ were assumed. This causes a slight *bowing* of the output constellation in the direction of the quadrature being modulated by the imbalanced AM. Figure 5(d) shows the constellation generated when the bias points of the internal PMs deviate from $\pm\frac{\pi}{2}$, for the particular constellation shown $\phi_{\text{bias}_1} = -\frac{2\pi}{5}$ and $\phi_{\text{bias}_2} = -\phi_{\text{bias}_3} = \phi_{\text{bias}_4} = \frac{\pi}{2}$ were assumed. In this situation, an asymmetric *bowing* of the constellation is now seen, again affecting the quadrature being modulated by the now imbalanced AM. Finally, Fig. 5(e) shows the constellation generated when the quadrature bias point is incorrectly set, i.e. $\phi_{\frac{\pi}{2}} \neq \frac{\pi}{2}$. For this particular constellation $\phi_{\frac{\pi}{2}} = \frac{2\pi}{5}$. When this occurs, the two signals being modulated in each nested AM are no longer separated by $\frac{\pi}{2}$, resulting in the constellation now being slanted diagonally.

In all the imbalanced scenarios shown previously, the deformation of the constellation will impact the true performance of the system, as the set of states now being generated deviates from that of the ideally generated constellations. If Alice and Bob assume the constellation was correctly generated, it will cause the channel parameters estimated in the receiver to degrade.

3 Performance impact of imperfect modulation stage devices

In this section, we describe how to compute the channel parameters and subsequent secure key rate and show the impact of transmitter device imperfections on the performance of a DM-CV-QKD system.

For this work we will be studying the impact of modulation imbalances on the performance of systems using 5 different constellation formats: 1024-QAM, 256-QAM, 64-QAM and regular 256-APSK with 32 states per ring and 64 states per ring. The probability of the amplitude levels of the constellations studied in this work follow a Maxwell–Boltzmann distribution. For a constellation with Q different amplitude levels, $A_i, i \in \{1, \ldots, Q\}$, the probability of each amplitude i is given by [35]

$$P_i = \frac{e^{-\nu A_i^2}}{\sum_{n=1}^{Q} P_n}, \tag{5}$$

where the ν parameter needs to be optimized for each scenario. The probability, q_k, of a given state, $|\alpha_k\rangle$, with amplitude $|\alpha_k| = A_i$, in a given constellation, can be readily computed by dividing the amplitude probability by the total number of states with the same amplitude. All constellations are generated with the same initial maximum amplitude of 1, with new amplitude levels being added progressively closer to the origin. After deformation, the final amplitude of the constellations was set so that

$$\langle n\rangle = \sum_{k=1}^{M} q_k |\alpha_k|^2, \tag{6}$$

where $\langle n\rangle$ is the average number of photons per symbol. For the results in this work, $\langle n\rangle$ was optimized for each constellation format, with Alice assuming that her constellation is faithfully recreated in the optical domain, i.e. that the modulation system is balanced and that the constellation points are correctly positioned. The value of $\langle n\rangle$ was kept constant regardless of the degree of the constellation deformation.

The transmitter, a, and receiver, b, constellations are related by the normal linear model [12]:

$$b = ta + z, \tag{7}$$

where $t = \sqrt{2\langle n\rangle \eta_d T}$ and z is the noise contribution, which follows a normal distribution with null mean and variance $\sigma^2 = 2 + \eta_d T\epsilon + 2\epsilon_{\text{thermal}}$. In the t and σ^2 parameters, T is the channel transmission, η_d is the quantum efficiency of Bob's detection system, ϵ is the excess channel noise and $\epsilon_{\text{thermal}}$ is the receiver thermal noise, these last two being both expressed in shot noise units (SNU). Moreover, t and σ^2 can be estimated through [12]:

$$\tilde{t} = \frac{1}{N}\mathrm{Re}\left\{\sum_{i=1}^{N} \frac{a_i b_i^*}{|\alpha_i|^2}\right\}, \qquad \tilde{\sigma}^2 = \frac{\sum_{i=1}^{N} |b_i - \tilde{t}a_i|^2}{N}. \tag{8}$$

Table 1 Code rates and respective minimum SNR requirements of different MET-LDPC codes [36, 37]

R	Minimum SNR
0.25	0.4162
0.10	0.1549
0.05	0.0741
0.02	0.0286
0.01	0.0141

The transmission and excess noise are then estimated through:

$$\tilde{T} = \frac{\tilde{t}^2}{2\langle n\rangle \eta_d}, \qquad \tilde{\epsilon} = \frac{\tilde{\sigma}^2 - 2 - 2\epsilon_{\text{thermal}}}{\eta_d \tilde{T}}. \tag{9}$$

The security of DM-CV-QKD against collective attacks was established in [3] and has since been updated in [22]. The work in [22] was used as a basis for the QAM implementation in [23], and for the development in [24], from which we take the methodology followed in this work. The achievable secure key rate is given by [3]

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{10}$$

where β is the reconciliation efficiency, given by [36]

$$\beta = 2\frac{R}{I_{\text{BA}}}, \tag{11}$$

where R is the rate of the reconciliation code being employed. Meanwhile, I_{BA} is the mutual information between Bob and Alice, given by [3]:

$$I_{\text{BA}} = \log_2\left(1 + \frac{2\tilde{T}\eta_d\langle n\rangle}{2 + \tilde{T}\eta_d\tilde{\epsilon} + 2\epsilon_{\text{thermal}}}\right) = \log_2(1 + \text{SNR}), \tag{12}$$

where SNR stands for Signal to Noise Ratio. As β is dependent on I_{BA}, it will be indirectly dependent on the SNR, in fact, a given code rate R is limited by the minimum SNR it requires to function, with the higher the rate, the higher the minimum SNR required. For this work we assume a Multi Edge Type Low Density Parity Check (MET-LDPC) reconciliation method, with the code rates and corresponding SNR limits being presented in Table 1 [36, 37]. The value of β was computed for each scenario, with the optimal code rate being chosen for each.

In (10), χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained from the symplectic eigenvalues of the system's covariance matrix [3]

$$\gamma_{\text{AB}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}Z\sigma_Z \\ \sqrt{T}Z\sigma_Z & (TV + 1 - T + T\epsilon)\mathbb{I}_2 \end{bmatrix}, \tag{13}$$

where $V = 2\langle n\rangle + 1$ corresponds to the variance of the signal at the output of the transmitter plus the unavoidable shot noise, $\mathbb{I}_2$ is the 2-D identity matrix, $\sigma_Z = \text{diag}(1, -1)$ and where Z is a measure of the correlation between the states at the transmitter and receiver, being given by

$$Z = 2\mathrm{tr}\big(\hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{\frac{1}{2}}\hat{a}^{\dagger}\big) - \sqrt{2\epsilon W}, \tag{14}$$

where $\hat{\rho} = \sum_{k=1}^{M} p_k|\alpha_k\rangle\langle\alpha_k|$ is the density operator of the M-symbol discrete constellation and [22]

$$W = \sum_{k=1}^{M} p_k\big(\langle\alpha_k|\hat{a}_{\rho}^{\dagger}\hat{a}_{\rho}|\alpha_k\rangle - \big|\langle\alpha_k|\hat{a}_{\rho}|\alpha_k\rangle\big|^2\big) \tag{15}$$

and finally $\hat{a}_{\rho} = \hat{\rho}^{\frac{1}{2}}\hat{a}\hat{\rho}^{-\frac{1}{2}}$. The exact methodology to compute χ_{BE} can be found in [22].

In order to evaluate the impact of the constellation deformations, we look at two different security scenarios:

- The *real* scenario, in which the value of Z in (13) is calculated for each individual deformed constellation and the deformations themselves are assumed to be taken into account during parameter estimation, i.e. the deformation does not affect the estimated channel parameters. This value will correspond to the actual key rate of the deformed constellations.
- The *naive* scenario, which consists of the key rate that Alice and Bob estimate by assuming that the transmitter system is balanced, using the value of Z computed for the ideal constellation and attributing all deviations from the ideal constellation to reduced transmission and excess channel noise.

The system parameters assumed in this work were $T = 0.1585$ (corresponding to the transmission coefficient of a standard 40 km SMF), $\eta = 0.9$, $\epsilon_{\mathrm{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU. In the naive scenario, the noise introduced by the deformation of the constellations is added to ϵ.

The performance of the imbalanced AM&PM modulation stage (see Fig. 2), measured in terms of the secret key rate, given by (10), for a combination of 3 different constellations with 256 cardinality, is presented in Fig. 6. Figure 6(a) shows the key rate in function of the different values of the AM BSs. We see that, for the three constellations assumed, the real value of the key rate decreases slowly as $\eta_{1,2}$ deviates from 0.5, while the naively estimated value decreases much more sharply, as the excess noise induced by the deformation takes it toll. Meanwhile, in Fig. 6(b) we show the key rate in function of the bias point of the internal PM of the AM. This time around, both the real and naive values of key rate decrease very quickly as the value deviates from equilibrium. In both the previous scenarios we see that the 256-APSK (reg64) constellation, the one that places its lowest amplitude states the farthest away from the origin, is the one whose performance, both in the real and naive scenarios, decreases the slowest. This is due to imbalances in the AM degrading its ability to perform destructive interference, causing the lower amplitude states to be shifted, which will be read as excess noise. Figure 6(c) shows the key rate in the situation of an asymmetrically driven AM, where the amplitude of $\phi_1(t)$ is multiplied by a constant factor while $\phi_2(t)$ remains unchanged. This time around, the real value of the key rate decreases faster when $\phi_1(t)/\phi_2(t) < 1$ than in the opposite scenario, while the naively estimated value decreases much more sharply and roughly at the same rate for the three constellations studied. Finally, Fig. 6(d) shows the key rate in the situation of an under/overdriven PM. The real value of the key rate decreases very slowly as the value deviates from equilibrium, while in

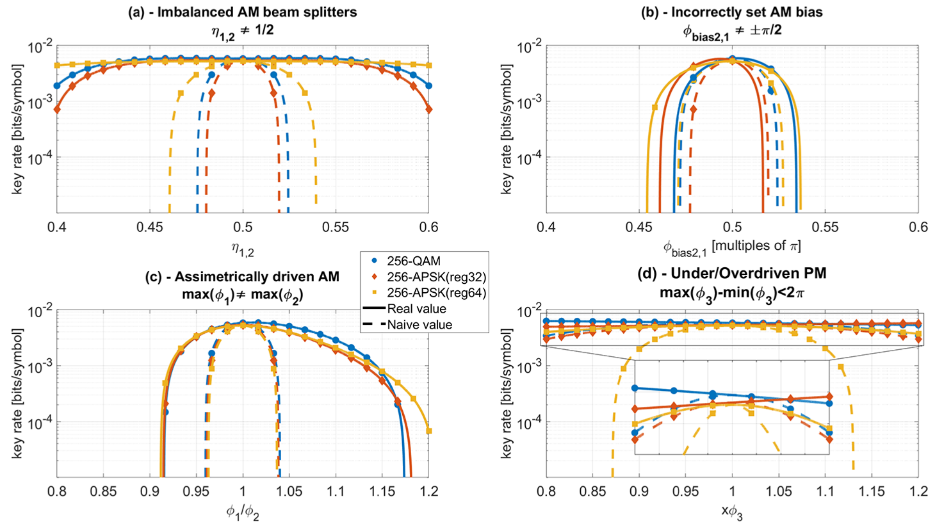

Figure 6 Real (full line) and naively (dashed line) estimated secret key rates for an imbalanced AM&PM modulation stage. Shapes and colours indicate the different constellation formats, blue circles indicate the 256-QAM constellation, orange diamonds indicate the 256-APSK with 32 states per ring and yellow squares indicate the 256-APSK with 64 states per ring. The parameters assumed were $T = 01585$, $\nu = 0.9$, $\epsilon_{\text{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU. In the naive scenario the excess noise ϵ is added to the contribution of the deformation of the constellations

the naive scenario only the 256-APSK (reg64) constellation sees a considerable reduction in performance. This is due to the 256-APSK (reg64) constellation placing the most points close the x-axis, and as a result will have more points deviated from their optimal position. For all the results in Fig. 6, we see that the performance estimated by Alice and Bob in the naive scenario is lower than its corresponding real value.

The performance of the imbalanced IQ modulation stage (see Fig. 4), measured in terms of the secret key rate, given by (10), and for a combination of 3 different QAM constellations, is presented in Fig. 7. Figure 7(a) shows the key rate in function of the different values of the outer BSs of the IQ modulator. We see that, for the three constellations assumed, the real value of the key rate decreases slowly as the value deviates from equilibrium, while the naively estimated value decreases much more sharply, with the 1024- and 256-QAM constellations exhibiting almost the same performance and the 64-QAM one exhibiting a noticeably lower one. Figure 7(b) shows the key rate in function of the different values of the inner BSs of the IQ modulator. Again, the naive value of the key rate decrease much faster than the real one, with the detail that the 64-QAM constellation being slightly more resistant to the drop in performance than the other, higher-cardinality constellations. Figure 7(c) shows the key rate in function of the bias point of the internal PMs of the IQ modulator. Once more, the naive value of the key rate decreases much faster than the real one, with the 1024-QAM constellation being slightly more affected and exhibiting a higher performance drop than the other two considered. Lastly, Fig. 7(d) shows the key rate in function of the bias point of the IQ modulator's quadrature bias. Similar results to the case of Fig. 7(a) are seen, with the real value of the key rate decreasing slower than the naive one, with the 1024- and 256-QAM constellations exhibiting almost the same performance and the 64-QAM exhibiting a noticeably lower one. Similarly to the AM&PM scenario, for

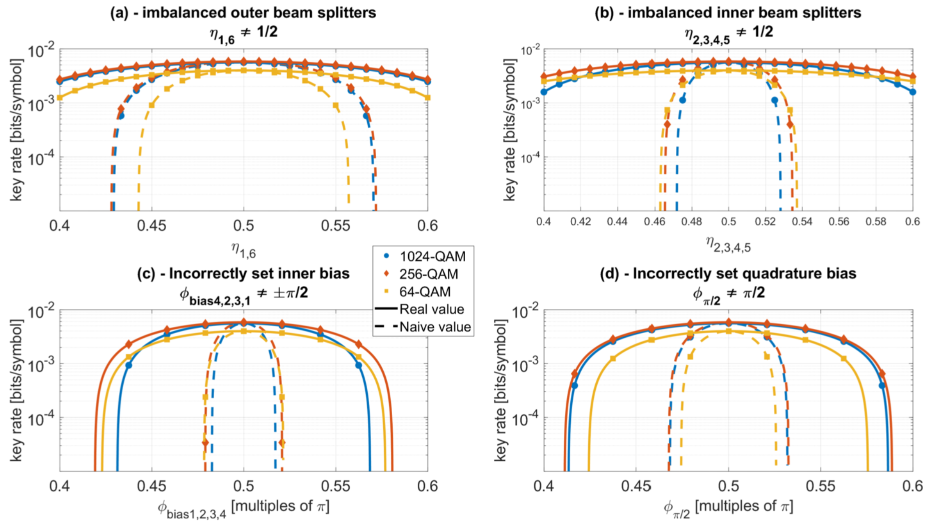

Figure 7 Real (full line) and naively (dashed line) estimated secret key rates for an imbalanced IQ modulation stage. Shapes and colours indicate the different constellation formats, blue circles indicate the 1024-QAM constellation, orange diamonds indicate the 256-QAM constellation and yellow squares indicate the 64-QAM constellation. The parameters assumed were $T = 01585$, $\nu = 0.9$, $\epsilon_{\text{thermal}} = 0.3$ SNU and $\epsilon = 0.01$ SNU. In the naive scenario the excess noise ϵ is added to the contribution of the deformation of the constellations

all the results in Fig. 7, the performance estimated by Alice and Bob in the naive scenario is lower than its corresponding real value.

4 Conclusion

We study the impact of modulation imbalances on both the intrinsic key rate available and on the key rate naively estimated by Bob. We observe that modulation stage imbalances reduce the maximum achievable secure key rate, however, much more impacted is the naively estimated key rate, meaning that there is a considerable loss of performance. However, and rather importantly, working in the naive scenario does not cause the secure key rate to be over-estimated, as a result the security of the generated keys is not impacted. We also see that, under certain imbalance scenarios and for both the real and naive values, the optimal constellation can vary, as a result the choice of constellation to be used in a given system should take possible imbalances in consideration. This clearly indicates that a precise characterization of the CV-QKD transmitter should be performed *a priori* in order to choose the best constellation.

Acknowledgements
Not applicable.

Funding
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 SFRH/BD/139867/2018, projects QuantumPrime (PTDC/EEI-TEL/8017/2020) and Quantagenomics (QuantERA/0001/2021).

Abbreviations
QKD, Quantum Key Distribution; CV, Continuous Variables; LO, Local Oscillator; LLO, Local Local Oscillator; RRC, Root-Raised-Cosine; PSK, Phase Shift Keying; RIN, Random Intensity Noise; SNU, Shot Noise Units; BS, Beam Splitter.

Availability of data and materials
The code used to obtain the results presented in this work is available from the corresponding author request.

Declarations

Competing interests

The authors declare no competing interests.

Author contributions

The bulk of the work was done by DP, expanding on an idea from NAP. MA, and ANP all checked the validity of the results and helped both in their interpretation and in writing the manuscript. All authors reviewed the manuscript.

Received: 13 December 2022 Accepted: 4 June 2023 Published online: 14 June 2023

References

1. Sergienko AV. Quantum communications and cryptography. Boca Raton: CRC Press; 2018.
2. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett. 2002;88(5):057902.
3. Leverrier A. Theoretical study of continuous-variable quantum key distribution. PhD thesis, Télécom ParisTech (2009).
4. Laudenbach F, Pacher C, Fung C-HF, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. Adv Quantum Technol. 2018;1(1):1800011.
5. Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A. 2010;81(6):062343.
6. Ralph TC. Continuous variable quantum cryptography. Phys Rev A. 1999;61:010303. https://doi.org/10.1103/PhysRevA.61.010303.
7. Qi B, Lougovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. Phys Rev X. 2015;5(4):041009.
8. Ma X-C, Sun S-H, Jiang M-S, Liang L-M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. Phys Rev A. 2013;87(5):052309.
9. Huang J-Z, Weedbrook C, Yin Z-Q, Wang S, Li H-W, Chen W, Guo G-C, Han Z-F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. Phys Rev A. 2013;87(6):062329.
10. Huang J-Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z-Q, Wang S, Chen W, Guo G-C, Han Z-F. Quantum hacking on quantum key distribution using homodyne detection. Phys Rev A. 2014;89(3):032304.
11. Jouguet P, Kunz-Jacques S, Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys Rev A. 2013;87(6):062313.
12. Kleis S, Rueckmann M, Schaeffer CG. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. Opt Lett. 2017;42(8):1588–91.
13. Pereira D, Silva NA, Pinto AN. A polarization diversity cv-qkd detection scheme for channels with strong polarization drift. In: 2021 IEEE international conference on quantum computing and engineering (QCE). New York: IEEE Press; 2021. p. 469–70.
14. Pereira D, Almeida M, Facão M, Pinto AN, Silva NA. Probabilistic shaped 128-apsk cv-qkd transmission system over optical fibres. Opt Lett. 2022;47(15):3948–51.
15. Liu W, Cao Y, Wang X, Li Y. Continuous-variable quantum key distribution under strong channel polarization disturbance. Phys Rev A. 2020;102(3):032625.
16. Kaur E, Guha S, Wilde MM. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. Phys Rev A. 2021;103(1):012412.
17. Liu W, Wang X, Wang N, Du S, Li Y. Imperfect state preparation in continuous-variable quantum key distribution. Phys Rev A. 2017;96(4):042312.
18. Weedbrook C, Pirandola S, García-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, Lloyd S. Gaussian quantum information. Rev Mod Phys. 2012;84(2):621.
19. Becir A, El-Orany F, Wahiddin M. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. Int J Quantum Inf. 2012;10(01):1250004.
20. Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys Rev X. 2019;9(4):041064.
21. Ghorai S, Grangier P, Diamanti E, Leverrier A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys Rev X. 2019;9(2):021059.
22. Denys A, Brown P, Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum. 2021;5:540
23. Roumestan F, Ghazisaeidi A, Renaudier J, Vidarte LT, Diamanti E, Grangier P. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-qam. In: 2021 European conference on optical communication (ECOC). New York: IEEE Press; 2021. p. 1–4.
24. Almeida M. Practical security limits of continuous-variable quantum key distribution. Master's thesis. University of Aveiro (2021).
25. Pereira D, Almeida M, Facão M, Pinto AN, Silva NA. Impact of receiver imbalances on the security of continuous variables quantum key distribution. EPJ Quantum Technol. 2021;8(1):1.
26. Silva NA, Almeida M, Pereira D, Facão M, Muga NJ, Pinto AN. Role of device imperfections on the practical performance of continuous-variable quantum key distribution systems. In: 2019 21st international conference on transparent optical networks (ICTON). 2019. p. 1–4.
27. Silva NA, Pereira D, Muga NJ, Pinto AN. Practical imperfections affecting the performance of cv-qkd based on coherent detection. In: 2020 22nd international conference on transparent optical networks (ICTON). New York: IEEE Press; 2020. p. 1–4.
28. Almeida M, Pereira D, Facão M, Pinto AN, Silva NA. Impact of imperfect homodyne detection on measurements of vacuum states shot noise. Opt Quantum Electron. 2020;52(11):1–13.
29. Shen Y, Yang J, Guo H. Security bound of continuous-variable quantum key distribution with noisy coherent states and channel. J Phys B, At Mol Opt Phys. 2009;42(23):235506.

30. Jouguet P, Kunz-Jacques S, Diamanti E, Leverrier A. Analysis of imperfections in practical continuous-variable quantum key distribution. Phys Rev A. 2012;86(3):032309.
31. Yang J, Xu B, Guo H. Source monitoring for continuous-variable quantum key distribution. Phys Rev A. 2012;86(4):042314.
32. Zheng Y, Huang P, Wang T, Peng J, Cao Z, Zeng G. The improvement of performance for continuous-variable quantum key distribution with imperfect Gaussian modulation. Int J Theor Phys. 2019;58:3414–35.
33. Ma H-X, Huang P, Wang T, Wang S-Y, Bao W-S, Zeng G-H. Security of continuous-variable measurement-device-independent quantum key distribution with imperfect state preparation. Phys Lett A. 2019;383(36):126005.
34. Pereira D, Silva N, Almeida M, Pinto A. Optimization of continuous variables quantum key distribution using discrete modulation. SPIE security + defence. Berlin 2022.
35. Encyclopedia of Physics, 2nd edn. VCH Publishers Inc. (1991)
36. Wang X, Zhang Y-C, Li Z, Xu B, Yu S, Guo H. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. 2017. arXiv preprint. arXiv:1703.04916.
37. Mani H, Andersen U, Gehring T, Pacher C, Forchhammer S, Mateo J, Vicente M. Error reconciliation protocols for continuous-variable quantum key distribution. Ph.D. dissertation. Technical University of Denmark (2021).

Publisher's Note

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