EPJ.org
EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

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

Daniel Pereira[1,2*], Margarida Almeida[3], Margarida Facão[4], 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
Full list of author information is available at the end of the article

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 show the impact of receiver device imperfections on the estimated channel parameters, performance and security of a CV-QKD system. The presented results show that, due to the erroneously estimated channel parameters, non-monitored imbalances can pose a security risk or even reduce the system's performance. Our results show the importance of monitoring these imbalances and hint at the possibility of compensating for some receiver imbalances by tuning other components.

Keywords: Continuous variables; Quantum key distribution; Device imperfections; Excess noise

1 Introduction

The expected near-future emergence of a practical quantum computer is a threat to classical cryptography [1–3], with prime number based classical cryptography being particularly affected [4]. In that scenario, Quantum Key Distribution (QKD) tackles the problem of the generation and distribution of symmetric cryptographic keys without assuming any computational limitations [5]. Recently, protocols based on the use of Continuous Variables (CV) have attracted considerable interest, due to the possibility to implement QKD with standard telecom equipment [6]. However, the low power of the signals used in CV-QKD, associated with a very low signal-to-noise ratio, demands a precise measurement of the noise in the communication channel and its amplitude in relation to the noise sources of the receiver [7]. Therefore, a precise characterization of the receiver is mandatory for the implementation of efficient and secure CV-QKD systems [8, 9].

QKD was first proposed in 1984, using the polarization of single photons as a coding basis [3]. Nevertheless, the use of single photons poses difficulties in their practical implementation, namely the specialized equipment needed for single photon generation and detection [10]. As an alternative, coherent-state CV-QKD was proposed, which encoded the information in the phase and amplitude of weak coherent states, thus allowing for implementation with current modulation methods and telecom-based equipment [6]. The initial CV-QKD protocols employed a level of randomness in the detection stage, by Bob randomly choosing his measurement basis [6]. A technique that does not require random basis switching was introduced in [11] and implemented in [12]. Furthermore, the first implementations of CV-QKD protocols were carried out by using a transmitted local oscillator (LO) setup [10]. Nevertheless, that was found to be a security flaw, because an eavesdropper could manipulate the LO, thus hiding their tampering on the quantum signal itself [13–17]. In that scenario, local LO (LLO) aided by digital signal processing (DSP) techniques are today the most common implementations of CV-QKD systems [13, 18]. These LLO techniques usually employ a relatively high power pilot tone, with the pilot being multiplexed with the quantum signal, to allow for frequency and phase recovery between the different lasers at the transmitter and receiver [13, 18–22]. Lately, LLO CV-QKD implementations using single-sideband modulation with heterodyne detection have been proposed, avoiding low-frequency noise [20–22]. In order to further maximize noise rejection, CV-QKD implementations using root-raised-cosine (RRC) signal modulation have been explored [20, 21]. Alongside the experimental implementations, the security bounds of CV-QKD systems have been established. In [7], an unconditional proof of security for 2-state and 4-state CV-QKD was presented, where the security is evaluated via the channel parameters (transmission and excess noise). This method was adapted into an 8-state protocol in [23]. These proofs assumed a scenario where a possible eavesdropper is only bounded by quantum laws and all excess noise is due to the action of a third party [7, 9]. In all of these security proofs, the optical system itself is assumed to be balanced [7, 9, 23]. In [9], the authors studied the relative contributions of different sources of noise to the final observed excess noise and their subsequent impact on the security of the protocol, in the case of a balanced optical system. Meanwhile, in [24–26], the authors studied the impact of different receiver imbalances on multiple parameters of the output voltage of the receiver. Nevertheless, the role of device imperfections on the performance and security of a heterodyne based LLO CV-QKD transmission system has not been explored. Moreover, the impact of device imperfections on the relative contributions of different noise sources remains an open question, to the best of our own knowledge.

In this paper, we describe the impact of device imperfections at the receiver side on the security and performance of a discrete-modulated CV-QKD system, employing true heterodyne detection and RRC modulation. We show that, under realistic imbalance scenarios, the key rate may be overestimated by 44%, resulting in almost a third of the generated secret key bits being unsafe.

This work is divided into four sections. In Sect. 2, we describe the generic system 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 receiver imbalances. In Sect. 4, we present numerical results showing the impact, on both the performance and security of the system, of the previously identified imbalances. We finalize this work with a summary of the major conclusions in Sect. 5.

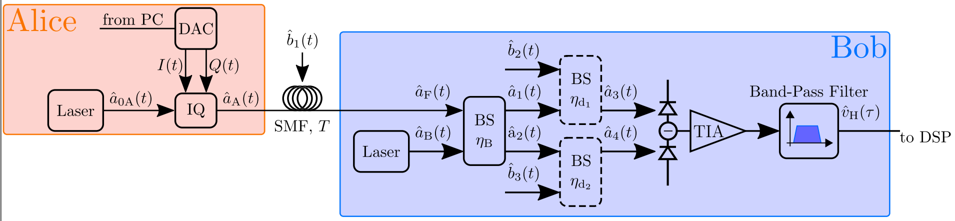

Figure 1 Block diagram of the locally generated local oscillator CV-QKD communication system

2 System description

In this section, we describe the theoretical and numerical models used to describe the role of device imperfections at the receiver stage on the performance of a discrete-modulated CV-QKD system with heterodyne detection.

A simplified block diagram of the CV-QKD system assumed in this work is presented in Fig. 1. The system used for this work is based on the one presented in [20]. According to convention, we will be naming the transmitter Alice, the receiver Bob and the possible eavesdropper Eve. Alice's setup is composed by an optical laser signal (coherent state), represented by the annihilation operator $\hat{a}_{0A}(t)$, and an IQ-modulator for constellation generation. The action of $\hat{a}_{0A}(t)$ on the coherent state obtained from Alice's laser is given by

$$\hat{a}_{0A}(t)\big|\alpha_A(t)\big\rangle = \alpha_A(t)\big|\alpha_A(t)\big\rangle, \tag{1}$$

where

$$\alpha_A(t) = |\alpha_A|e^{i(\omega_A t+\phi_A(t))}, \tag{2}$$

and $|\alpha_A|$ represents the amplitude of Alice's laser such that $|\alpha_A|^2$ is the photon-flux, ω_A is the optical frequency of the laser and $\phi_A(t)$ is the unknown optical phase of the laser at instant t. The IQ modulator is driven by signals $I(t)$ and $Q(t)$, generated by a PC controlled digital-to-analogue converter (DAC). The discrete-modulated quantum signal consists of an 8-PSK root-raised-cosine (RRC) constellation inserted at an intermediate frequency f_Q. A frequency multiplexed pilot tone is also included in the modulation, consisting of a complex sine-wave inserted at an intermediate frequency f_P, chosen to be outside of the bandwidth of the quantum signal. The modulated laser signal is thus given by

$$\hat{a}_A(t) = \hat{a}_{0A}(t)M(t), \tag{3}$$

where $M(t)$ is the modulation applied to Alice's signal, given by

$$M(t) = q(t)e^{i2\pi f_Q t} + Pe^{i2\pi f_P t} + \epsilon_{\text{Mod}}, \tag{4}$$

with $q(t)$ being a complex valued function containing the 8-PSK RRC signal, P the amplitude of the pilot tone and ϵ_{Mod} a noise parameter that accounts for imperfections in the modulation. Modulation imperfections may arise due to noise in the driving signals or due to an improper balancing of the modulator itself.

In Fig. 1, the optical fibre is modelled as a beam-splitter with a transmission coefficient of T, where it is mixed with the vacuum state at port $\hat{b}_1(t)$. The fibre output signal is in that case given by

$$\hat{a}_{\mathrm{F}}(t) = \sqrt{T}\hat{a}_{\mathrm{A}}(t) + \sqrt{1-T}\hat{b}_1(t). \tag{5}$$

At Bob's side, the quantum signal $\hat{a}_{\mathrm{F}}(t)$ is sent to a beam-splitter with transmittance η_{B}, where it is mixed with Bob's LLO, $\hat{a}_{\mathrm{B}}(t)$. The beam-splitter outputs are described by

$$\hat{a}_1(t) = \sqrt{\eta_{\mathrm{B}}}\hat{a}_{\mathrm{F}}(t) + \sqrt{1-\eta_{\mathrm{B}}}\hat{a}_{\mathrm{B}}(t), \tag{6}$$

$$\hat{a}_2(t) = \sqrt{1-\eta_{\mathrm{B}}}\hat{a}_{\mathrm{F}}(t) - \sqrt{\eta_{\mathrm{B}}}\hat{a}_{\mathrm{B}}(t). \tag{7}$$

Note that this beam-splitter ideally would have $\eta_{\mathrm{B}} = \frac{1}{2}$. The action of $\hat{a}_{\mathrm{B}}(t)$ on the coherent state extracted from Bob's laser is given by

$$\hat{a}_{\mathrm{B}}(t)\big|\alpha_{\mathrm{B}}(t)\big\rangle = \alpha_{\mathrm{B}}(t)\big|\alpha_{\mathrm{B}}(t)\big\rangle, \tag{8}$$

where

$$\alpha_{\mathrm{B}}(t) = |\alpha_{\mathrm{B}}|e^{i(\omega_{\mathrm{B}}t+\phi_{\mathrm{B}}(t))}, \tag{9}$$

and $|\alpha_{\mathrm{B}}|$ represents the amplitude of Bob's laser such that $|\alpha_{\mathrm{B}}|^2$ is the photon-flux, ω_{B} is the optical frequency of the laser and $\phi_{\mathrm{B}}(t)$ is the unknown optical phase of the laser at instant t. The beam-splitter outputs, $\hat{a}_1(t)$ and $\hat{a}_2(t)$, are then detected by a pair of photodiodes. The quantum efficiency of each photodiode, η_{d1} and η_{d2}, is modelled by a virtual beam-splitter with a transmission coefficient equal to the quantum efficiency of the real photodiode followed by an ideal photodiode [27]. As a result, the signals are mixed with the vacuum states at ports $\hat{b}_2(t)$ and $\hat{b}_3(t)$, resulting in the outputs

$$\hat{a}_3(t) = \sqrt{\eta_{\mathrm{d}_1}}\hat{a}_1(t) + \sqrt{1-\eta_{\mathrm{d}_1}}\hat{b}_2(t), \tag{10}$$

$$\hat{a}_4(t) = \sqrt{\eta_{\mathrm{d}_2}}\hat{a}_2(t) + \sqrt{1-\eta_{\mathrm{d}_2}}\hat{b}_3(t). \tag{11}$$

Ideally, the quantum efficiencies of the two photodetectors would be equal, but experimentally this may not be the case. The pair of optical signals in (10) and (11) is then converted to an electrical current according to

$$\hat{I}_1(t) = q_e\hat{a}_3^{\dagger}(t)\hat{a}_3(t), \tag{12}$$

$$\hat{I}_2(t) = q_e\hat{a}_4^{\dagger}(t)\hat{a}_4(t), \tag{13}$$

where q_e is the elementary electron charge. The currents $\hat{I}_1(t)$ and $\hat{I}_2(t)$ at the photodiodes' output are expressed as quantum operators due to the fact that they are proportional to the quantum creation and annihilation operators of the optical field that reaches the photodiodes. Dark currents originating in the photodiodes are not considered, as their value will be negligible when compared to the other sources of noise, such as thermal and shot noise [28].

The two currents in (12) and (13) are subtracted and the thermal noise originating in the trans-impedance amplifier, $\hat{n}_{\mathrm{th}}$, is added to the resulting current

$$\hat{I}(t) = \hat{I}_2(t) - \hat{I}_1(t) + \hat{n}_{\mathrm{th}}(t), \tag{14}$$

where $\hat{n}_{\mathrm{th}}(t)$ is a Gaussian distributed random variable with null mean and variance $\varepsilon^2_{\mathrm{th}}$. This subtraction current is then passed through a trans-impedance amplifier in which process it is filtered by a bandpass filter, resulting in

$$\hat{v}_{\mathrm{H}}(\tau) = g_{\mathrm{TIA}}\bigl(h_{\mathrm{BP}}(t) * \hat{I}(t)\bigr)(\tau), \tag{15}$$

where g_{TIA} is the gain of the trans-impedance amplifier, $h_{\mathrm{BP}}(t)$ represents the impulse response of the bandpass filter and the $*$ symbol represents convolution. This amplified signal is then digitized and fed into a DSP system that allows for frequency and phase recovery. For the purposes of this work, we assume this DSP to be ideal, not introducing any extra noise.

3 Impact of imbalances

In this section, we describe the impact of devices imperfections at Bob's detection system on the expected value and variance of the measured voltage. Moreover, we also consider the role of those imperfections on the estimation of the channel's transmission coefficient, excess noise and secret key rate. For the purposes of this work, both lasers were assumed to be tuned to a wavelength of 1550 nm (corresponding to $\omega_{\mathrm{A}} = \omega_{\mathrm{B}} = 193.41$ THz), and the frequencies at which the signal and the pilot were inserted were assumed to take the values $f_Q = 215$ MHz and $f_P = 55$ MHz.

The expected value of the output voltage $\hat{v}_{\mathrm{H}}(\tau)$ of the coherent receiver in Fig. 1 is given by (16).

$$\begin{aligned}\bigl\langle \hat{v}_{\mathrm{H}}(\tau)\bigr\rangle = {} & g_{\mathrm{TIA}} q_e\bigl[\eta_{\mathrm{d}_1}\eta_{\mathrm{B}} - \eta_{\mathrm{d}_2}(1-\eta_{\mathrm{B}})\bigr] T|\alpha_{\mathrm{A}}|^2\bigl(h_{\mathrm{BP}}(t) * \bigl|M(t)\bigr|^2\bigr)(\tau) \\ & + g_{\mathrm{TIA}} q_e\bigl[\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) - \eta_{\mathrm{d}_2}\eta_{\mathrm{B}}\bigr]|\alpha_{\mathrm{B}}|^2\bigl(h_{\mathrm{BP}}(t) * 1\bigr)(\tau) \\ & + 2g_{\mathrm{TIA}} q_e(\eta_{\mathrm{d}_1} + \eta_{\mathrm{d}_2})\sqrt{\eta_{\mathrm{B}}(1-\eta_{\mathrm{B}})T}|\alpha_{\mathrm{A}}||\alpha_{\mathrm{B}}| \\ & \times \bigl\{h_{\mathrm{BP}}(t) * \cos\bigl[(\omega_{\mathrm{A}} - \omega_{\mathrm{B}})t + \phi_{\mathrm{A}}(t) - \phi_{\mathrm{B}}(t)\bigr]\mathrm{Re}\bigl[M(t)\bigr]\bigr\}(\tau),\end{aligned} \tag{16}$$

In (16), the first and second terms are due to an imperfect subtraction of Alice's and Bob's average power, respectively, and the last term is due to the interference between Alice's modulated signal and Bob's local oscillator. The $(h_{\mathrm{BP}}(t) * 1)(\tau)$ term in (16) is due to the constant power nature of Bob's laser signal.

The performance of the CV-QKD system can be assessed through the estimation of the excess noise added to the measured voltage in (16). To quantify that, we must calculate the signal variance at Bob's detection system. This variance will have to be computed using a time-sampled numerical code with sampling time dt, in which situation the Dirac delta function is defined as [29]

$$\delta(t) = \begin{cases} \frac{1}{dt}, & 0 < t \leq dt, \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

The variance for $\hat{\nu}_{\mathrm{H}}(\tau)$ is given by (18), where $\mathrm{RIN}^{\mathrm{A}}_{\Delta f}$ and $\mathrm{RIN}^{\mathrm{B}}_{\Delta f}$ are, respectively, the power spectral densities of Alice's and Bob's lasers random intensity noise (RIN).

$$\begin{aligned}
&\langle \hat{\nu}_{\mathrm{H}}(\tau)^2 \rangle - \langle \hat{\nu}_{\mathrm{H}}(\tau)\rangle^2 \\
&\quad = g^2_{\mathrm{TIA}} \varepsilon^2_{\mathrm{th}} \\
&\qquad + g^2_{\mathrm{TIA}} q^2_e \bigl[\eta_{\mathrm{d}_1}\eta_{\mathrm{B}} - \eta_{\mathrm{d}_2}(1-\eta_{\mathrm{B}})\bigr]^2 T^2 \frac{1}{dt} |\alpha_{\mathrm{A}}|^4 \mathrm{RIN}^{\mathrm{A}}_{\Delta f} \bigl(h^2_{\mathrm{BP}}(t) * \bigl|M(t)\bigr|^4\bigr)(\tau) \\
&\qquad + g^2_{\mathrm{TIA}} q^2_e \bigl[\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) - \eta_{\mathrm{d}_2}\eta_{\mathrm{B}}\bigr]^2 \frac{1}{dt} |\alpha_{\mathrm{B}}|^4 \mathrm{RIN}^{\mathrm{B}}_{\Delta f} \bigl(h^2_{\mathrm{BP}}(t) * 1\bigr)(\tau) \\
&\qquad + g^2_{\mathrm{TIA}} q^2_e \bigl[\eta_{\mathrm{d}_1}\eta_{\mathrm{B}} + \eta_{\mathrm{d}_2}(1-\eta_{\mathrm{B}})\bigr] \frac{1}{dt} T |\alpha_{\mathrm{A}}|^2 \bigl(h^2_{\mathrm{BP}}(t) * \bigl|M(t)\bigr|^2\bigr)(\tau) \\
&\qquad + g^2_{\mathrm{TIA}} q^2_e \bigl[\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) + \eta_{\mathrm{d}_2}\eta_{\mathrm{B}}\bigr] \frac{1}{dt} |\alpha_{\mathrm{B}}|^2 \bigl(h^2_{\mathrm{BP}}(t) * 1\bigr)(\tau) \\
&\qquad + 2 g^2_{\mathrm{TIA}} q^2_e (\eta_{\mathrm{d}_1} - \eta_{\mathrm{d}_2}) \sqrt{\eta_{\mathrm{B}}(1-\eta_{\mathrm{B}})T} \frac{1}{dt} |\alpha_{\mathrm{A}}||\alpha_{\mathrm{B}}| \\
&\qquad \times \bigl\{h^2_{\mathrm{BP}}(t) * \cos\bigl[(\omega_{\mathrm{A}} - \omega_{\mathrm{B}})t + \phi_{\mathrm{A}}(t) - \phi_{\mathrm{B}}(t)\bigr] \mathrm{Re}\bigl[M(t)\bigr]\bigr\}(\tau),
\end{aligned} \tag{18}$$

In (18), the first term is the noise variance due to the thermal noise of the receiver, whereas the second and third terms represent the noise variance due to the RIN from Alice's and Bob's lasers, respectively. The fourth and fifth terms correspond, respectively, to Alice's and Bob's shot noise. The sixth and final term in (18) is the shot noise of the interference between Alice's modulated signal and Bob's LO. The final term in (18) will take a negative value when $\eta_{\mathrm{d}_1} < \eta_{\mathrm{d}_2}$, this however is not an instance of negative noise but rather a correction to the fourth and fifth terms of the equation. In fact, the last three terms of (18) can be rewritten as

$$\begin{aligned}
&g^2_{\mathrm{TIA}} q^2_e \frac{1}{dt} \eta_{\mathrm{d}_1} \bigl\{h^2_{\mathrm{BP}}(t) * \bigl|\sqrt{\eta_{\mathrm{B}} T}\alpha_{\mathrm{A}}(t)M(t) + \sqrt{1-\eta_{\mathrm{B}}}\alpha_{\mathrm{B}}(t)\bigr|^2\bigr\}(\tau) \\
&\quad + g^2_{\mathrm{TIA}} q^2_e \frac{1}{dt} \eta_{\mathrm{d}_2} \bigl\{h^2_{\mathrm{BP}}(t) * \bigl|\sqrt{(1-\eta_{\mathrm{B}})T}\alpha_{\mathrm{A}}(t)M(t) - \sqrt{\eta_{\mathrm{B}}}\alpha_{\mathrm{B}}(t)\bigr|^2\bigr\}(\tau),
\end{aligned} \tag{19}$$

where it becomes clear that the combination of the shot noises from both lasers with the interference variance will always have a positive value.

Both channel parameters, transmission, T, and excess noise, ϵ, can be estimated from (16) and (18). Bob can estimate T through his measured average voltage via [8]

$$\tilde{T} = \left(\frac{\langle \hat{\nu}_{\mathrm{H}}(\tau)\rangle}{2 g_{\mathrm{TIA}} q_e \eta_{\mathrm{d}} |\alpha_{\mathrm{A}}||\alpha_{\mathrm{B}}| \{h_{\mathrm{BP}}(t) * \cos[(\omega_{\mathrm{A}} - \omega_{\mathrm{B}})t + \phi_{\mathrm{A}}(t) - \phi_{\mathrm{B}}(t)] \mathrm{Re}[M(t)]\}(\tau)}\right)^2, \tag{20}$$

where $\eta_{\mathrm{d}} = \frac{\eta_{\mathrm{d}_1} + \eta_{\mathrm{d}_2}}{2}$ is the mean value of the quantum efficiency of the two photodiodes. In this definition, the transmittance is effectively estimated from the average value of the constellation. Bob can estimate the thermal noise of his receiver by turning off both the signal from the fibre and his receiver laser and then estimate the noise added by his laser by turning on his receiver laser and subtracting the previously observed thermal noise variance from the now observed variance. However, Bob will not be able to distinguish between his laser's shot noise and RIN, as a result his estimation for the shot noise will be given by

$$\begin{aligned}\tilde{\Sigma} &= g_{\mathrm{TIA}}^{2} q_e^{2}\big[\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) - \eta_{\mathrm{d}_2}\eta_{\mathrm{B}}\big]^{2}\frac{1}{dt}|\alpha_{\mathrm{B}}|^{4}\mathrm{RIN}^{\mathrm{B}}_{\Delta f}\big(h^{2}_{\mathrm{BP}}(t) * 1\big)(\tau) \\ &\quad + g_{\mathrm{TIA}}^{2} q_e^{2}\big[\eta_{\mathrm{d}_1}(1-\eta_{\mathrm{B}}) + \eta_{\mathrm{d}_2}\eta_{\mathrm{B}}\big]\frac{1}{dt}|\alpha_{\mathrm{B}}|^{2}\big(h^{2}_{\mathrm{BP}}(t) * 1\big)(\tau).\end{aligned} \tag{21}$$

The excess noise measured by Bob, expressed in shot noise units (SNU), will then correspond to the total variance without Bob's thermal and laser noises (shot noise and RIN) and divided by $\tilde{\Sigma}$. Since the security model assumes that the excess noise is added at the channel input, the variance originating from this subtraction will have to be divided by the estimated channel transmission. In that scenario, the excess noise is estimated by

$$\tilde{\epsilon} = \frac{\langle \hat{v}_{\mathrm{H}}(\tau)^{2}\rangle - \langle \hat{v}_{\mathrm{H}}(\tau)\rangle^{2} - (g^{2}_{\mathrm{TIA}}\varepsilon^{2}_{\mathrm{th}} + \tilde{\Sigma})}{\tilde{\Sigma}\tilde{T}}. \tag{22}$$

The channel parameters $\tilde{T}$ and $\tilde{\epsilon}$ can then be used to estimate the secret key rate, given by

$$K = \beta I_{\mathrm{BA}} - \chi_{\mathrm{BE}}, \tag{23}$$

where

$$I_{\mathrm{BA}} = \log_2\left(1 + \frac{2\tilde{T}\eta\langle n\rangle}{2 + \tilde{T}\eta_{\mathrm{d}}\tilde{\epsilon} + 2\frac{g^{2}_{\mathrm{TIA}}\varepsilon^{2}_{\mathrm{th}}}{\tilde{\Sigma}}}\right), \tag{24}$$

where $\langle n\rangle$ is the average number of photons per symbol and χ_{BE} is obtained through equation (17) in [23].

4 Numerical results

In this section, we present numerical results illustrating the impact of device imperfections at Bob's detection system on the estimated channel parameters and subsequently on the estimated secret key rate. In Fig. 2 (a) we present the evolution of the estimated channel transmission, expressed in (20), as a function of the transmission parameter of Bob's beam-splitter, η_{B} in Fig. 1. From the results in Fig. 2 (a) we can see that when the system is balanced, i.e. §$\eta_{\mathrm{B}} = 0.5$, the transmission estimated by Bob will coincide with the real transmission. However, as it further imbalances, the estimated transmission will follow the curve dictated by $\sqrt{\eta_{\mathrm{B}}(1-\eta_{\mathrm{B}})}$. Note that the first term in (16) does not have a major contribution in (20), due to the low power of the quantum signal. The second term in (16), due to it being a purely DC contribution and DC being filtered out by the bandpass filter $h_{\mathrm{BP}}(t)$, also does not have a major contribution to (20).

As stated previously, Bob's shot noise estimate, Σ, will have contributions from both his laser's shot noise and RIN. In Fig. 2 (b), we show the dependency of the noise parameters in (21) with Bob's beam-splitter transmission coefficient. From the results in Fig. 2 (b) we can see that the shot noise contribution remains unchanged with the imbalances, which is to be expected, as the shot noise term in (21) is not dependent on η_{B} when $\eta_{\mathrm{d}_1} = \eta_{\mathrm{d}_2}$. Meanwhile, the RIN's contribution rises sharply and rapidly becomes the dominant factor

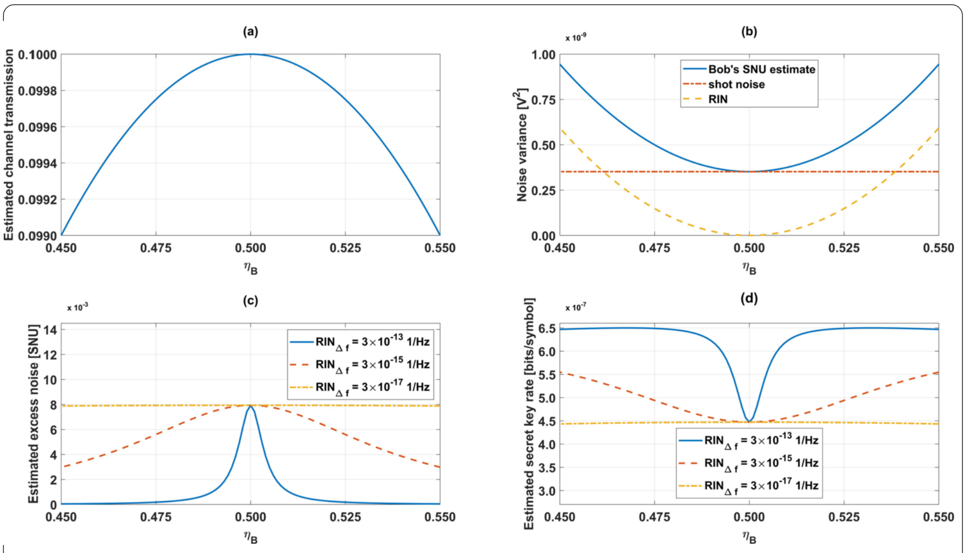

Figure 2 Evolution of (**a**) the estimated channel transmission, given by (20), (**b**) Bob's shot noise estimate, given by (21), (**c**) the estimated excess noise, given by (22), and (**d**) the estimated key rate, given by (23), as a function of Bob's beam-splitter transmission coefficient. We have used $T = 0.1$, $g_{\mathrm{TIA}} = 10^4$ V/A, $\varepsilon_{\mathrm{th}} = 1.44 \times 10^{-4}$ Vrms, $|\alpha_{\mathrm{A}}|^2 = 1.25 \times 10^8$ s^{-1}, $|\alpha_{\mathrm{B}}|^2 = 1.56 \times 10^{17}$ s^{-1}, $T_s = 4$ ns, $dt = 31.25$ ps, $\eta_{\mathrm{d}_1} = \eta_{\mathrm{d}_2} = 0.7$ and $\mathrm{RIN}^{\mathrm{A}}_{\Delta f} = \mathrm{RIN}^{\mathrm{B}}_{\Delta f} = 3 \times 10^{-15}$ Hz^{-1}

to the global noise at Bob's detection output. The result of the combined shot noise and RIN is an overestimation of the shot noise, which will influence the estimation of the excess noise in relation to it, which can be seen in Fig. 2 (c).

In Fig. 2 (c), we present the evolution of the estimated excess of noise given by (22) in SNU, as a function of Bob's beam-splitter imbalance. The excess noise presented here is due only to Alice's RIN, shot noise and the shot noise of the interference between Alice's modulated signal and Bob's LO, corresponding to the second, fourth and sixth terms of (18), respectively. In Fig. 2 (c), we can see that, for the different values of RIN, the excess noise will always follow roughly the same behaviour. The estimated excess noise is maximum when the system is balanced and decreases symmetrically around $\eta_{\mathrm{B}} = 0.5$ as it imbalances. This is due to Bob's estimation for the shot noise, Σ, increasing sharply as the system becomes unbalanced, as shown in Fig. 2 (b). The higher the RIN, the more pronounced the excess noise underestimation will be. The decrease of the estimated transmission will also have an impact on the estimated excess noise, as the estimated transmission decreases with the increasing imbalance of η_{B}, the estimated excess noise would also increase. However the effect of the increase of $\tilde{\Sigma}$ will be the dominant factor.

The secret key rate can then be estimated for the estimated values of transmission and excess noise following (23), yielding the results presented in Fig. 2 (d). For the lowest value of RIN the estimated secret key rate will decrease as the η_{B} deviates from 0.5, with this effect being dictated by the decreasing estimated transmission observed in Fig. 2 (a). This results in some lost system performance, as usable bits will be discarded. For the other two values of RIN, the underestimation of the excess noise observed in Fig. 2 (c) will cause an overestimation of the secure key rate, this poses a security risk as Alice and Bob will distill bits for the key at a rate higher than the channel parameters would allow for a secure key.

In Fig. 3 (a), we present the evolution of the estimated channel transmission, defined in (20), as a function of the difference between the quantum efficiencies of Bob's photodi-

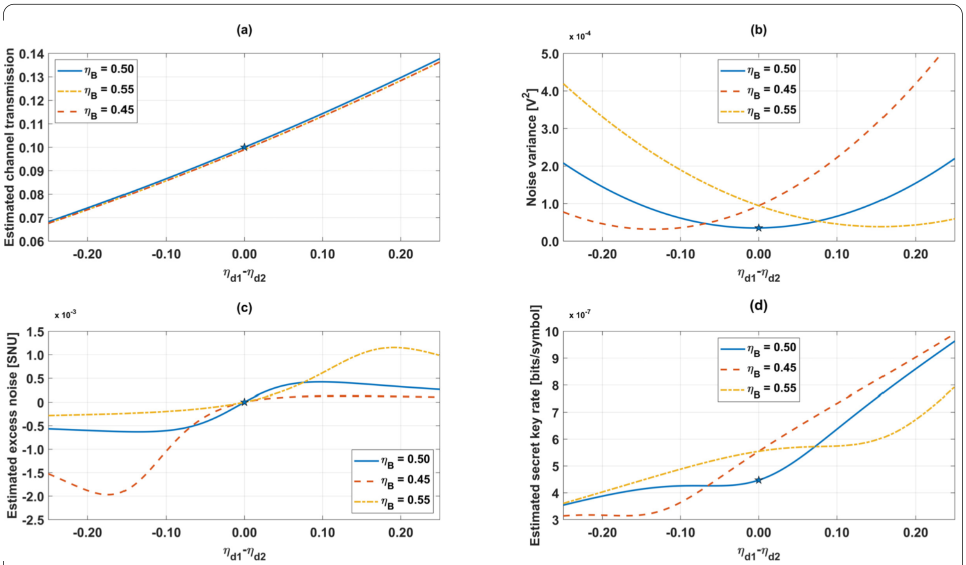

Figure 3 Evolution of (**a**) the estimated channel transmission, given by (20), (**b**) Bob's shot noise estimate, given by (21), (**c**) the estimated excess noise, given by (22), and (**d**) the estimated key rate, given by (23), as a function of Bob's photo detector imbalance. We have used $T = 0.1$, $g_{\mathrm{TIA}} = 10^4$ V/A, $\varepsilon_{\mathrm{th}} = 1.44 \times 10^{-4}$ Vrms, $|\alpha_{\mathrm{A}}|^2 = 1.25 \times 10^8$ s^{-1}, $|\alpha_{\mathrm{B}}|^2 = 1.56 \times 10^{17}$ s^{-1}, $T_s = 4$ ns, $dt = 31.25$ ps and $\mathrm{RIN}^{\mathrm{A}}_{\Delta f} = \mathrm{RIN}^{\mathrm{B}}_{\Delta f} = \mathrm{RIN}_{\Delta f} = 3 \times 10^{-15}$ Hz^{-1}. The point corresponding to the balanced system, i.e. the "real" value, is identified by a star

odes, identified by η_{d1} and η_{d2} in Fig. 1, for three different values of η_{B}. From the results in Fig. 3 (a) we can see that the estimated transmission follows the curve dictated by $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$, with the different values of η_{B} causing a small vertical shift to the curve. When $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} > 0$ the transmission will tend to be overestimated, while when $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}} < 0$ it will tend to be underestimated. Furthermore, we can see that equal deviations of η_{B} in either direction, i.e. $\eta_{\mathrm{B}} < 0.5$ and $\eta_{\mathrm{B}} > 0.5$, will result in the same deviation of the estimated channel transmission.

In Fig. 3 (b), we show the dependency of $\tilde{\Sigma}$, expressed in (21), with the difference between the quantum efficiencies of Bob's photodiodes. We see from Fig. 3 (b) that, when $\eta_{\mathrm{B}} = 0.5$, Bob's estimated shot noise has a minimum value, corresponding to the true shot noise, at $\eta_{\mathrm{d1}} = \eta_{\mathrm{d2}}$, and rises as the quantum efficiencies deviate, as the RIN contribution becomes more and more pronounced. Moreover, in Fig. 3 (b), we see that when the value of η_{B} deviates from 0.5, the point at which the value of Bob's estimated shot noise is minimum deviates to negative values of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ when $\eta_{\mathrm{B}} < 0.5$ and to positive values of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ when $\eta_{\mathrm{B}} > 0.5$. This hints at the fact that imbalances in Bob's beam-splitter may be compensated by tuning the relative values of η_{d1} and η_{d2} and vice versa. Additionally, the value of Bob's estimated shot noise at this minimum point will be slightly below the value observed with the balanced system when $\eta_{\mathrm{B}} < 0.5$ and, conversely, slightly above that value when $\eta_{\mathrm{B}} > 0.5$. This asymmetry is due to the average value of the quantum efficiencies of the photodiodes being lower when $\eta_{\mathrm{d1}} < \eta_{\mathrm{d2}}$ and higher when $\eta_{\mathrm{d1}} > \eta_{\mathrm{d2}}$, causing the second term of (21), which corresponds to Bob's laser's shot noise, to increase as the value of $\eta_{\mathrm{d1}} - \eta_{\mathrm{d2}}$ increases.

In Fig. 3 (c), we present the evolution of the estimated excess noise, given by (22), in SNU, as a function of the difference between the quantum efficiencies of Bob's photodiodes, for three different values of η_{B}. We can see from Fig. 3 (c) that all the estimated excess noise curves tend to the same value at $\eta_{d1} = \eta_{d2}$, with the excess noise being overestimated when $\eta_{d1} > \eta_{d2}$ and underestimated when $\eta_{d1} < \eta_{d2}$. When $\eta_{d1} < \eta_{d2}$, the estimated excess noise quickly becomes negative, this happens because, in this situation, the excess noise is dominated by the sixth term in (18), which itself becomes negative when $\eta_{d1} < \eta_{d2}$. Recall that in our case the only excess noise contributions are due to noise originating in Alice's transmission system and due to the interference noise between Alice's signal and Bob's LO, in the presence of other, likely higher, channel noise contributions, the excess noise would not take a negative value, but would rather have a reduced value when compared to a balanced system. Additionally, for $\eta_B = 0.5$, when $\eta_{d1} < \eta_{d2}$ the excess noise estimate will decrease until it reaches a minimum and when $\eta_{d1} > \eta_{d2}$ it increases until it reaches a maximum. However, this curve is not symmetric, with the minimum value observed not having the same absolute value as the maximum observed value. Meanwhile, when $\eta_B = 0.45$, the excess noise estimate will exhibit a minimum with a lower value and located at a lower value of $\eta_{d1} - \eta_{d2}$ and a maximum with a lower value located at a higher value of $\eta_{d1} - \eta_{d2}$, when compared to the values for $\eta_B = 0.5$. Conversely, when $\eta_B = 0.55$, the excess noise estimate will exhibit only the maximum observed when $\eta_{d1} > \eta_{d2}$, having a higher value and being located at a greater value of $\eta_{d1} - \eta_{d2}$, again when compared to the values for $\eta_B = 0.5$. These three curves show a very asymmetric dependency of the excess noise with the photodetector imbalances, this asymmetry is again due to the contribution of the sixth term in (18), which is itself asymmetric, and due to the excess noise's dependency on the estimated channel transmission, shown in Fig. 3 (a), which will cause the estimated excess noise values when $\eta_{d1} - \eta_{d2} < 0$ to have a higher absolute value than the ones estimated when $\eta_{d1} - \eta_{d2} > 0$.

The secret key rate can again be estimated for the estimated values of transmission and excess noise following (23), yielding the results presented in Fig. 3 (d). We can see from Fig. 3 (d) that, for both $\eta_B = 0.5$ and $\eta_B = 0.45$, the estimated secret key rate will, generally, increase as $\eta_{d1} - \eta_{d2}$ increases, apart from a short decreasing region. Meanwhile, when $\eta_B = 0.55$, the estimated secret key rate will always increase as $\eta_{d1} - \eta_{d2}$ increases. The evolution of the estimated key rate in function of the photodiode imbalance is dominated by the estimated value for the channel transmission, shown in Fig. 3 (a), which increases linearly with $\eta_{d1} - \eta_{d2}$. The regions where the growth of the estimated key rate slows down, and in the case of $\eta_B = 0.5$ and $\eta_B = 0.45$ stops, are due to the contribution of the excess noise, whose maximum and minimums roughly coincide with these regions. Depending on the exact position in the x-axis, this means that these combined beam-splitter and photodiode quantum efficiencies will result in either an over or under estimation of the secret key rate. In the scenario of an overestimation of the secret key rate, this will pose a security risk as Alice and Bob will distillate bits for the key at a rate higher than the channel parameters would allow for a secure key, while in the case of an underestimation there will be lost performance, as Alice and Bob will discard more bits than they had to.

5 Conclusion

We study the impact of receiver imbalances on the channel parameters estimated by Bob and the subsequent impact on the estimated secure key rate. We observe that non-monitored imbalances in the receiver beam-splitter and photodiode quantum efficiencies may pose a security risk, as it will cause Alice and Bob to overestimate their secret key rate. For example, a 2% imbalance of the transmission coefficient of Bob's beam-splitter transmission coefficient will lead up to a 44% overestimation of the key rate. Physically, this overestimation arises mainly from Bob's inclusion of his laser's RIN in his estimation of the shot noise, which will cause an underestimation of the value of the excess noise in relation to the shot noise. Moreover, receiver imbalances may also lead to a reduced performance of the key distribution system, as the wrongly estimated channel parameters can also lead to a slight underestimation of the secret key rate. For example, in the absence of other receiver imbalances, a 2% deviation between the values of the quantum efficiencies of the photodiodes may lead to either a 3% underestimation or a 4% overestimation of the key rate. However, when the 2% deviation between the values of the quantum efficiencies of the photodiodes is combined with a 5% imbalance of the transmission coefficient of Bob's beam-splitter, the key rate can then be overestimated by 30%, when $\eta_B = 0.45$, or by 25%, when $\eta_B = 0.55$.

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 Q.DOT (POCI-01-0247-FEDER-039728), UIDB/50008/2020-UIDP/50008/2020 (action QuRUNNER and QUESTS), and project i3N, UIDB/50025/2020 & UIDP/50025/2020, financed by national funds through the FCT/MEC.

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.

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

Declarations

Competing interests
The authors declare that they have no competing interests.

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

Author details
[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. [3]Department of Physics, University of Aveiro, Campus de Santiago, 3810-193, Aveiro, Portugal. [4]I3N and Department of Physics, University of Aveiro, Campus de Santiago, 3810-193, Aveiro, Portugal.

Publisher's Note

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

Received: 26 May 2021 Accepted: 7 October 2021 Published online: 18 October 2021

References

1. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6.
2. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory. 1985;31(4):469–72.
3. Bennett CH, Brassard G. Quantum cryptography: public key distribution and con tos5. In: Proceedings of the international conference on computers, systems and signal processing. 1984.
4. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Foundations of computer science, 1994 proceedings, 35th annual symposium on. IEEE; 1994. p. 124–34.
5. Sergienko AV. Quantum communications and cryptography. Boca Raton: CRC Press; 2018.

6. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett. 2002;88(5):057902.
7. Leverrier A. Theoretical study of continuous-variable quantum key distribution. PhD thesis, Télécom ParisTech. 2009.
8. Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A. 2010;81(6):062343.
9. 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.
10. Ralph TC. Continuous variable quantum cryptography. Phys Rev A. 1999;61:010303. https://doi.org/10.1103/PhysRevA.61.010303.
11. Weedbrook C, Lance AM, Bowen WP, Symul T, Ralph TC, Lam PK. Quantum cryptography without switching. Phys Rev Lett. 2004;93(17):170504.
12. Lance AM, Symul T, Sharma V, Weedbrook C, Ralph TC, Lam PK. No-switching quantum key distribution using broadband modulated coherent light. Phys Rev Lett. 2005;95(18):180503.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. Soh DB, Brif C, Coles PJ, Lütkenhaus N, Camacho RM, Urayama J, Sarovar M. Self-referenced continuous-variable quantum key distribution protocol. Phys Rev X. 2015;5(4):041010.
19. Marie A, Alléaume R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. Phys Rev A. 2017;95(1):012316.
20. 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.
21. Brunner HH, Comandar LC, Karinou F, Bettelli S, Hillerkuss D, Fung F, Wang D, Mikroulis S, Yi Q, Kuschnerov M et al. A low-complexity heterodyne cv-qkd architecture. In: 2017 19th international conference on transparent optical networks (ICTON). IEEE; 2017. p. 1–4.
22. Laudenbach F, Schrenk B, Pacher C, Hentschel M, Fung C-HF, Karinou F, Poppe A, Peev M, Hübel H. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. Quantum. 2019;3:193.
23. Becir A, El-Orany F, Wahiddin M. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. Int J Quantum Inf. 2012;10(1):1250004.
24. 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.
25. 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). IEEE; 2020. p. 1–4.
26. 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.
27. Loudon R. The quantum theory of light. 3rd ed. London: Oxford University Press; 2000.
28. Agrawal GP. Lightwave technology: telecommunication systems. New York: Wiley; 2005.
29. Dirac PAM. The principles of quantum mechanics. vol. 27. London: Oxford University Press; 1981.