Heliyon 9 (2023) e16670

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Effects of experimental impairments on the security of continuous-variable quantum key distribution

Andres Ruiz-Chamorro *, Daniel Cano, Aida Garcia-Callejo, Veronica Fernandez

Spanish National Research Council (CSIC), Institute of Physical and Information Technologies (ITEFI), Serrano 144, 28006 Madrid, Spain

ARTICLE INFO

Keywords:
Quantum Key Distribution
Continuous variable
CV-QKD
Impairments
Simulations
Secret key rate
Frequency drift
Imperfections

ABSTRACT

Quantum Key Distribution (QKD) is a cutting-edge communication method that enables secure communication between two parties. Continuous-variable QKD (CV-QKD) is a promising approach to QKD that has several advantages over traditional discrete-variable systems. Despite its potential, CV-QKD systems are highly sensitive to optical and electronic component impairments, which can significantly reduce the secret key rate. In this research, we address this challenge by modeling a CV-QKD system to simulate the impact of individual impairments on the secret key rate. The results show that laser frequency drifts and small imperfections in electro-optical devices such as the beam splitter and the balanced detector have a negative impact on the secret key rate. This provides valuable insights into strategies for optimizing the performance of CV-QKD systems and overcome limitations caused by component impairments. By offering a method to analyze them, the study enables the establishment of quality standards for the components of CV-QKD systems, driving the development of advanced technologies for secure communication in the future.

1. Introduction

Quantum Key Distribution (QKD) is a secure communication method that enables two parties, Alice and Bob, to generate a secret key that is only known by them [1–4]. The key feature of QKD is its ability to detect the presence of any eavesdropper through the principles of quantum mechanics. The variables used to encode the quantum key are classified into two groups: continuous variables (CV), such as the quadratures of coherent states [5–9] and discrete variables (DV), such as the polarization states of single photons [1,10–13]. CV-QKD has several important advantages over DV-QKD, such as cost-effectiveness and ease of implementation [9,14]. In fact, CV-QKD does not require single-photon detectors, which makes it possible to use standard telecommunication devices, such as coherent receivers, instead. This presents an opportunity for the implementation of CV-QKD in current network infrastructures.

While the theoretical security of Quantum Key Distribution (QKD) is guaranteed by quantum principles, the quantum key rate of real experiments is highly sensitive to the impairments of optical and electronic components. Previous works have investigated the effects of these instrumental impairments or experimental imperfections [15–18]. However, a detailed analysis of individual impairments is still needed to fully understand the causes of decreased secret key rate in real CV-QKD systems, taking specific experimental imperfections into account. For example, imperfect basis choice and state preparation can reduce the security of the

* Corresponding author.
E-mail address: andres.ruiz@csic.es (A. Ruiz-Chamorro).

https://doi.org/10.1016/j.heliyon.2023.e16670
Received 11 May 2023; Received in revised form 23 May 2023; Accepted 24 May 2023

Available online 29 May 2023

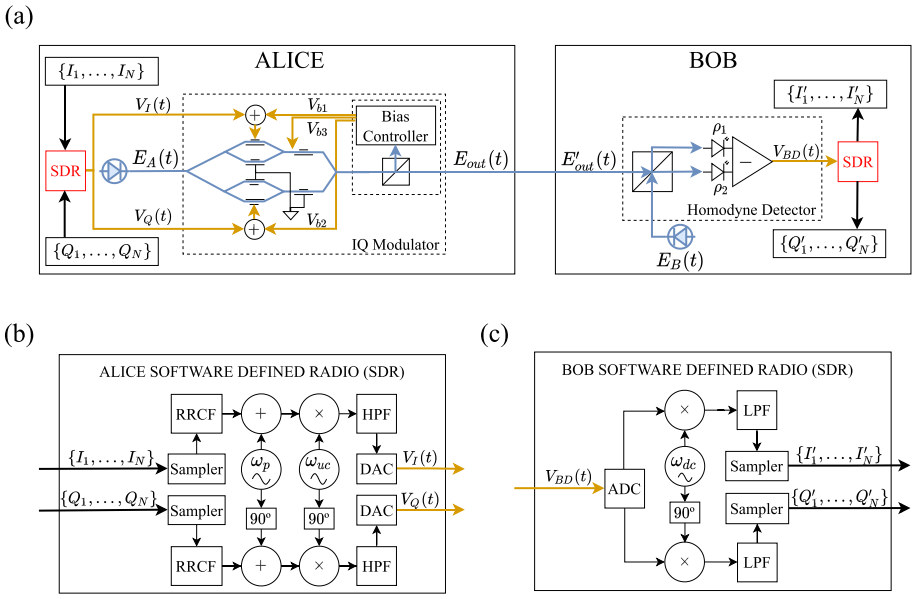

Fig. 1. (a) Schematic of the CV-QKD system. Alice encodes the key in two sets of random values, $\{I_1,...,I_N\}$ and $\{Q_1,...,Q_N\}$. These are transformed into the signals $V_I(t)$ and $V_Q(t)$, which are used to modulate a laser field $E_A(t)$ in an IQ modulator. Bob carries out the low-complexity heterodyne detection using a local laser field $E_B(t)$, a beam splitter, and a balanced detector, whose output signal, $V_{BD}(t)$, is used to obtain $\{I'_1,...,I'_N\}$ and $\{Q'_1,...,Q'_N\}$. (b) Software Defined Radio in Alice. Two root-raised cosine filters (RRCF) smooth the symbols. Digital up-conversion is accomplished with a mixer and two high-pass filters (HPF). The analog signals are generated with two digital-to-analog converter (DAC). (c) Software Define Radio in Bob. The analog signal is acquired in an analog-to-digital converter (ADC). Digital down-conversion is accomplished with a mixer and two low-pass filters (LPF).

system by introducing inaccuracies in the estimation of channel properties [19,20]. Additionally, receiver imperfections can impact the performance and security of CV-QKD systems, underscoring the importance of careful monitoring and compensation [21].

In this paper, we model a CV-QKD system to simulate the detrimental effects of individual impairments on the secret key. The model provides insights on optimization strategies to reduce excess noise and improve the secret key rate. The results are essential to establish the quality standards that each component must meet before being integrated into a CV-QKD network.

2. Model system for CV-QKD

To study the effects of instrumental impairments on the secret key rate, we simulate a model system based on the most common and cost-effective implementations of CV-QKD [22]. In our system (see Fig. 1), Alice sends a secret key by modulating the in-phase and quadrature components of weak coherent states using a single-mode laser and an IQ (In-Phase and Quadrature) modulator. The receiver (Bob) measures the signal using low-complexity heterodyne detection. This is the most cost-effective method implemented to date since it allows to obtain the in-phase and quadrature components by means of only one detector in combination with a software post-processing of the signal [22].

The basic operation of the system is described as follows. The protocol starts with the generation of a key, consisting of two sets of values, $\{I_1, I_2, ..., I_N\}$ and $\{Q_1, Q_2, ..., Q_N\}$, representing the in-phase and quadrature components of the coherent state modulation at a sampling rate f_s. To create hardware-implementable signals, each key string is filtered by a root-raised cosine filter (RRCF), producing two smooth signals as shown in Fig. 2a and Fig. 2b.

Since we use Gaussian modulation, the raw symbols are defined by $x \in \mathcal{N}(0,\sigma^2)$ at the sampling times and zero otherwise, being $\mathcal{N}(0,\sigma^2)$ a Gaussian distribution with zero mean and variance σ^2. The raw symbols are then filtered with the RRCF, generating the symbol signals that will be combined with a pilot tone, up-converted in frequency, and high-pass filtered before being sent to the IQ modulator.

A pilot tone of frequency ω_p is added to the symbol signals to provide a frequency reference and clock recovery method [25,26]. Then, to avoid degradation of the low-frequency components, these signals are up-converted by mixing them with a signal of frequency ω_{uc}, which is typically in the GHz domain. Two high-pass filters remove the redundant frequency components generated by the up-conversion mixing process. Finally, a digital-to-analog converter (DAC) generates the analog modulation signals, $V_I(t)$ and $V_Q(t)$, that are applied to the IQ modulator. All the steps required to generate $V_I(t)$ and $V_Q(t)$ (and to demodulate $V_{BD}(t)$) are shown in Fig. 1b (Fig. 1c).

We perform a numerical simulation of the aforementioned steps and present the results in Fig. 3a. The left part of the spectrum displays the symbol band, which contains the information being transmitted. In addition to the symbol band, the right part of the spectrum is dominated by a single pilot tone, which is usually located far away from the symbol band to prevent it from interfering with the information being transmitted. It is important to note that the spectrum of the signal $V_Q(t)$ would be similar to that of $V_I(t)$.

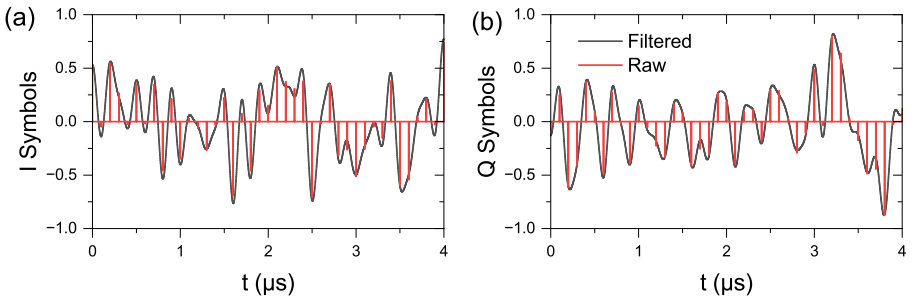

Fig. 2. (a). In-Phase component of the symbols generated in Alice's Software Defined Radio before up-conversion. (b) Quadrature component of the same symbols. Note that all signals represented in this figure are obtained from numerical simulations and they are normalized for simplicity, as they could either be expressed in SI Units (Volts) or Shot Noise Units (SNU) [23,24].

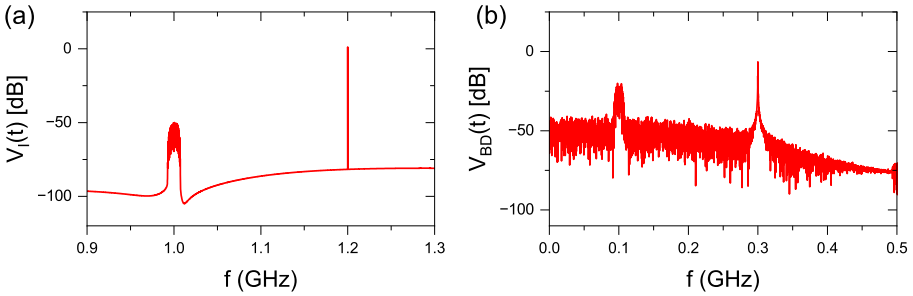

Fig. 3. (a) The spectrum of the modulating signal $V_I(t)$. (b) Spectrum of the balanced detector output signal $V_{BD}(t)$. Note that both signals are obtained from numerical simulations.

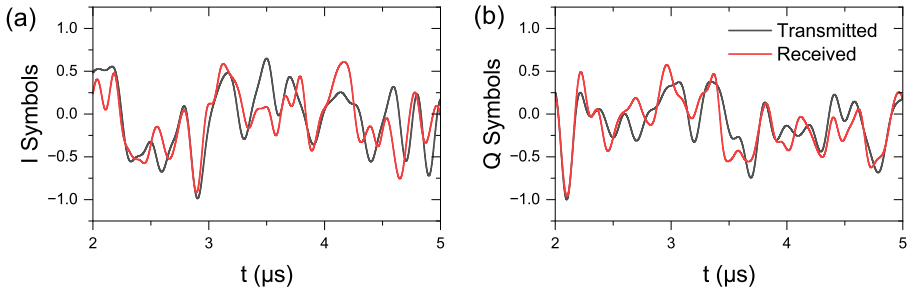

Fig. 4. (a) In-Phase component of the symbol signal obtained in Bob's Software Defined Radio after low-complexity heterodyne detection (red) versus the symbol signal generated in Alice's Software Defined Radio (black). (b) Quadrature component of the same signals. Note that both signals are normalized such as in Fig. 2.

In order to maximize the security of the quantum key transmission, the modulation amplitude of the symbols should be set to a low level to maintain the desired level of uncertainty in the quadrature measurements.

The signal is transmitted from Alice to Bob through an optical fiber, typically several kilometers long. Bob measures the in-phase and quadrature components of the quantum signal by means of a low-complexity heterodyne detection setup [22]. For this, the incoming laser field interferes with Bob's local oscillator in a beam splitter, and a balanced detector is employed to measure the difference between both outputs of the beam splitter. The output of the balanced detector reflects the combined effects of the modulating signal, the noise introduced by the channel, and the finite bandwidth of the detector itself, which in this case is assumed to be 400 MHz. It is important to note that the simulation of the output spectrum includes all of these factors, so that the true performance of the system can be accurately assessed. This procedure is numerically simulated step by step, as described in the next Section, to obtain the output signal of the balanced detector shown in Fig. 3b.

The signal is then down-converted using a frequency of ω_{dc} in combination with software post-processing that provides the in-phase and quadrature signals. Both in-phase and quadrature signals of Alice and Bob are shown in Fig. 4a and Fig. 4b. After recovering these signals, a parallel-to-serial encoder (P2S) is used to obtain two sets of random values, $\{I'_1, I'_2, ..., I'_N\}$ and $\{Q'_1, Q'_2, ..., Q'_N\}$, which should be correlated with those sent by Alice. In continuous-variable protocols, the security of the transmission can be estimated calculating the Secret Key Rate (SKR), which essentially depends on the difference between the mutual information shared between Alice and Bob, and the Holevo bound of the information shared between Eve and Bob, which represents the maximum amount of information that Eve could extract performing collective attacks on the channel [27,23,2].

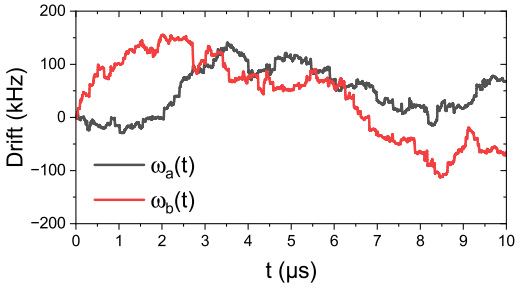

Fig. 5. Simulation of a random drift in the frequencies of Alice and Bob's lasers, $\omega_A(t)$ and $\omega_B(t)$. We use a cubic interpolator to smooth the drift between two steps.

To determine the secret key rate in the finite-size regime we reproduce the Parameter Estimation stage of the protocol using the algorithm of [28], where Alice and Bob randomly select a part of the transmitted data to study the correlation between the data strings that they have sent and received. This correlation allows them to compute the transmittance T and excess noise ξ of the channel. More details about Parameter Estimation and secret key rate calculation can be found in [27,29,30,23]

In the final steps of the protocol, Alice and Bob distill the key by means of privacy amplification and error correction algorithms [31]. The security of the transmission is characterized by its secret key rate, from which one can estimate an upper bound to the maximum information gained by a potential eavesdropper (Eve). If it exceeds the acceptable upper limit, Alice and Bob abort the protocol and discard the key. Otherwise, Alice and Bob perform error correction and privacy amplification techniques to finally distill a shared secure key.

3. Instrumental impairments

3.1. Frequency drifts of the laser fields

Frequency drifts of the laser fields degrade the demodulation processes. Although small drifts can be partially corrected by off-line software post-processing [32,33], their effect on the secret key rate of the transmitted signal cannot be neglected. We simulate the frequency drifts by considering time-dependent frequencies, $\omega_A(t)$ and $\omega_B(t)$, for Alice and Bob's laser fields, which are respectively given by

$$E_A(t) = |E_A| \exp(i\omega_A(t)t), \quad E_B(t) = |E_B| \exp(i\omega_B(t)t). \tag{1}$$

In Eq. (1), the frequencies $\omega_A(t)$ and $\omega_B(t)$, which vary over time, are generated by random walks with step sizes based on a logistic distribution. To achieve a realistic simulation, the distribution was derived from experimental measurements of an external-cavity InP-based diode laser at 1550 nm. The simulation results are depicted in Fig. 5.

3.2. Stability of the bias controller in the IQ modulator

The IQ modulator is made up of a main Mach-Zehnder interferometer with two nested Mach-Zehnder interferometers, as shown in Fig. 1a. Small deviations or noise in the input signals or the parameters of the three Mach-Zehnders can result in significant degradation of the final secret key rate. The output of the IQ modulator can be expressed as

$$E_{\text{out}}(t) = \frac{E_A(t)}{2}\left[\cos\left(\frac{\pi}{2}\frac{V_{b1}+V_I(t)}{V_{\pi 1}}\right) + \exp\left(i\pi\frac{V_{b3}}{V_{\pi 3}}\right)\cos\left(\frac{\pi}{2}\frac{V_{b2}+V_Q(t)}{V_{\pi 2}}\right)\right], \tag{2}$$

where V_{b1}, V_{b2} and V_{b3} are the bias voltages which set the operating points of each Mach-Zehnder interferometer, $V_{\pi 1}$, $V_{\pi 2}$ and $V_{\pi 3}$ are their half-wave voltages; and $V_I(t)$ and $V_Q(t)$ are the analog modulation signals used to modulate each quadrature of the phase space. To implement the CV-QKD protocol, the bias voltages should be set to the quadrature operating point of the IQ modulator. This is achieved when $V_{b1} = -V_{\pi 2}$, $V_{b2} = -V_{\pi 2}$ and $V_{b3} = V_{\pi 3}/2$. In this case, Eq. (2) is simplified to Eq. (3),

$$E_{\text{out}}(t) = \frac{E_A(t)}{2}\left[\sin\left(m_1 V_I(t)\right) + i\sin\left(m_2 V_Q(t)\right)\right], \tag{3}$$

where $m_i = \pi/2V_{\pi i}$ $(i = 1, 2)$ are the modulation indexes that depend only on the half-wave voltage of the Mach-Zehnder modulators. In the ideal case, $m_1 = m_2$ as $V_{\pi 1} = V_{\pi 2}$. It should be noted that in this analysis, we are specifically examining these particular electronic impairments. However, other studies [20,19] have demonstrated how imperfect Gaussian state preparation can contribute to an increase in excess noise.

3.3. Noise in the transmission channel

For our simulations, we consider Gaussian noise as it represents the most comprehensive scenario for a transmission channel. This type of noise is generated by a class of attacks known as Gaussian attacks, which have been established as the most general attacks against CV-QKD [2,28]. The impact on the transmitted electric field can be thus described by Eq. (4),

Table 1
Parameters used in the simulations.

Parameter	Value
Alice's laser frequency (ω_A)	$2\pi \times 193.5000$ THz
Bob's laser frequency (ω_B)	$2\pi \times 193.5009$ THz
Pilot tone (ω_p)	$2\pi \times 200$ MHz
Up-converting frequency (ω_{uc})	$2\pi \times 1$ GHz
Symbol rate (f_s)	10 MHz
Channel attenuation	0.2 dB/km
Gaussian noise variance (σ^2)	1.11 SNU
Electronic noise variance (ν)	0.1 SNU
Detection efficiency (η)	0.8
Reconciliation efficiency (β)	0.922

$$E'_{\text{out}}(t) = \sqrt{10^{-\alpha L/10}} E_{\text{out}}(t) + x(t), \tag{4}$$

where L is the transmission channel length, α is the attenuation coefficient and $x(t)$ is a complex Gaussian noise signal. This signal is modeled following a normal distribution with mean 0 and variance σ^2 at the symbol sampling times. The noise variance σ^2 is defined as the sum of the shot noise unit (1 SNU), the excess noise variance (the noise generated in the channel, both from attacks and imperfections, assumed to be 0.1 SNU), and the variance of the electronic noise (fluctuations in the electronic components that affect the measurement of the optical signals, assumed to be 0.01 SNU) [28,23].

3.4. Incorrect ratio of the beam splitter

The output fields of the beam splitter are given by [34],

$$\begin{cases} E_1(t) = r_1 E'_{\text{out}}(t) + t_1 E_B(t) \\ E_2(t) = t_2 E'_{\text{out}}(t) - r_2 E_B(t) \end{cases}, \tag{5}$$

where r_1 and r_2 are the reflection coefficients, and t_1 and t_2 are the transmission coefficients of the beam splitter. In the ideal case of a 50/50 beam splitter, we would have Eq. (5) with $t_1 = t_2 = r_1 = r_2 = \sqrt{1/2}$. Deviations from the ideal 50/50 beam splitter lead to reduction of the secret key rate.

3.5. Unbalanced detector gains

The impact of the impairments of the balanced detector should also be taken into account. If the photo-detectors have different gains, the secret key rate also decreases. The output voltage is given by [23]

$$V(t) = \rho_1 P_1(t) - \rho_2 P_2(t). \tag{6}$$

The parameters ρ_1 and ρ_2 ($P_1(t)$ and $P_2(t)$) in Eq. (6) are the sensitivities (powers) of the photo-detectors respectively. The signal measured at the balanced detector is shown in Fig. 3b.

4. Results and discussion

In this section, we calculate the secret key rate including the effects of the instrumental impairments. All simulations are carried out using the parameters of Table 1. The values of the frequencies ω_A, ω_B, ω_p, ω_{uc} and f_s are standard values typically used in CV-QKD systems. The channel attenuation is the standard for single-mode telecommunication fibers ($\alpha = 0.2$ dB/km). For η, ν and β (a metric that represents the amount of information that is successfully extracted from the raw data), the values used are those from [28] since they represent typical values for an experimental CV-QKD setup.

The theoretical model used for the computation of the secret key rate follows A. Leverrier's thesis [27]. The analysis here performed is based on the entanglement-based version of the protocol and calculates the secret key rate as a trade-off between the mutual information shared by Alice and Bob and the Holevo bound on the information that Eve shares with Bob. This is represented mathematically by

$$K = \beta I(A;B) - S(E;B), \tag{7}$$

where $0 \leq \beta \leq 1$ is the reconciliation efficiency and $S(E;B)$ is the Holevo information between Eve and Bob (i.e., an upper bound on the information Eve has on Bob's data-measurement's random variable). $I(A;B)$, as in the classical setting, represents the mutual information between Alice and Bob. The main objective –and challenge– of the security analysis is to compute the highest bound on Eve's information of Bob's data, so as to obtain the lowest bound –and therefore safest– estimation of the secret key rate, defined as in Eq. (7).

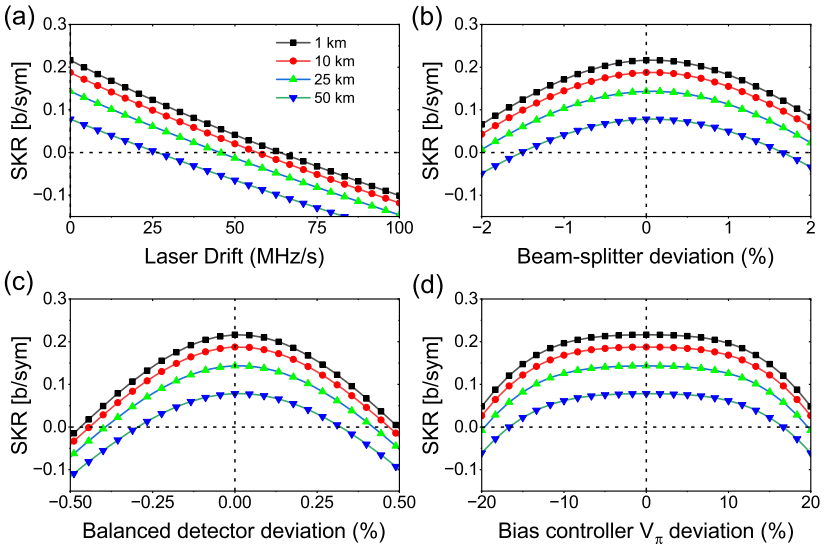

Fig. 6. (a) Secret Key Rate versus deviations in reflectance and transmittance coefficients from its ideal value of $\sqrt{1/2}$, assuming $|r_1|^2 + |t_1|^2 = 1$ and $|r_2|^2 + |t_2|^2 = 1$. (b) Secret Key Rate as a function of the deviation of the photo-detector sensitivity ρ_1 with respect to ρ_2. (c) Secret Key Rate versus lasers maximum frequency drift per second. (d) Relation between secret key rate and the deviation of the bias controller from the ideal operating point, defined as $V_b = -V_\pi$, assuming V_{b1} deviates from $-V_{\pi 1}$. Very similar result is obtained for deviations in V_{b2}, V_{b3}.

The Holevo bound can be computed considering a Gaussian state that shares with Alice and Bob's state of information the same first two moments, i.e., the same covariance matrix. The desired covariance matrix, therefore, is computed from the parties data correlation statistics. After a few symmetrization procedures [27], it takes the form:

$$\Gamma = \begin{pmatrix} (V_A + 1)I_2 & t_{min} Z \sigma_Z \\ t_{min} Z \sigma_Z & (t_{min}^2 + \sigma_{max}^2) I_2 \end{pmatrix}, \tag{8}$$

where t_{min} and σ_{max}^2 are the minimal and maximal values, respectively, of the maximum-likelihood estimators (MLE) from which the real values of transmission T and excess noise ξ are approximated (i.e., the worst-case estimations of the channel noise parameters). The expressions for the respective MLE's are given, respectively, by

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2}, \qquad \hat{\sigma^2} = \frac{1}{m} \sum_{i=0}^{m} (y_i - \hat{t} x_i)^2, \tag{9}$$

being m the number of states used to perform parameter estimation. The bound on the Holevo information for the Gaussian state with the covariance matrix of Eq. (8) is therefore given by a function of its eigenvalues ν_1 and ν_2, shown in Eq. (10),

$$S(E;B) = \sum_{k=1}^{3} g\left(\frac{\nu_i - 1}{2}\right), \tag{10}$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2(x)$ and ν_3 is the eigenvalue of the covariance matrix of Alice and Bob's mode. By including this mathematical analysis in our simulations, we are able to calculate the secret key rate for multiple transmissions. This is computed after sampling the signals and obtaining the symbols x_i and y_i, which are subsequently used to compute the transmittance and excess noise of the transmission using Eq. (9), ultimately leading to the estimation of the secret key rate.

Fig. 6 shows the secret key rate as a function of instrumental impairments. One of the most noticeable effects is a dramatic decrease in the SKR due to the frequency drifts of both lasers, as shown in Fig. 6a. The reason is that these drifts introduce additional noise in the low-complexity heterodyne detection affecting the secret key rate. In fact, the SKR is below the security threshold for frequency drifts of just a few tens of MHz/s. The secret key rate is also very sensitive to small impairments in the beam splitter and the balanced detector, as shown in Fig. 6b and Fig. 6c. A deviation of only 0.1% of the ideal r or t coefficients in the beam splitter, which is typical in standard beam splitters, can have a dramatic impact on the secret key rate. Interestingly, the SKR is hardly affected by small deviations of the bias voltage from its ideal operating point, as shown in Fig. 6d. This gives us some flexibility in the electronics used to stabilize the three interferometers of the IQ modulator by tuning its bias voltages.

In all figures, it can be observed that the secret key rate decreases with the distance between Alice and Bob, as expected. This is of particular relevance upon defining a range in which the characteristics of our experimental system must be found. As the distance increases, the range in which the SKR is positive becomes increasingly narrow, thus reducing the possibilities of transmitting a secure key. It is worth noting that standard commercial systems fall within these ranges. Lasers typically drift between 1 MHz/s and 50 MHz/s in frequency, beam-splitters typically deviate between 1% and 5% from the theoretical splitting ratio, balanced detectors usually have less than 1% deviation between photodetector gains, and the error to determine the operating point in the IQ modulator

bias controller is usually less than 5%. This implies that for long distances, these features of the laser and beam-splitter will play a critical role in maintaining the secret key rate above a certain level to transmit a secure key.

5. Conclusions

In our study, we analyze the impact of different instrumental impairments on the Secret Key Rate (SKR) in a Continuous-Variable Quantum Key Distribution (CV-QKD) system. The results of the simulations show that laser frequency drifts can significantly lower the secret key rate and that even minor impairments in the beam splitter ratios or the gains of the photodiodes in the balanced detector can have a noticeable impact on key transmission. In contrast, small variations in the IQ (In-Phase and Quadrature) modulator's bias controller from its ideal operating point did not substantially affect the SKR.

Our model and simulations are a valuable tool in the initial calibration of a CV-QKD system, making it faster and easier, and preventing the decrease of the SKR due to most commonly-known impairments in experimental implementations. By determining and fixing the range of several physical parameters that enhance the transmission we can optimize the experimental performance of these systems, opening the possibility of long-distance or high-speed CV-QKD transmission.

Overall, this study presents how to enhance the SKR through a detailed theoretical model and simulation of the impairments present in experimental systems. It provides a new method to study each component of the setup independently and characterize, correct or mitigate the effect of several identified impairments. This contributes to the development and optimization of CV-QKD systems, which can play a crucial role in ensuring secure communication in future quantum networks.

CRediT authorship contribution statement

Andres Ruiz-Chamorro: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper. Veronica Fernandez: Conceived and designed the experiments; Performed the experiments; Wrote the paper. Daniel Cano, Aida Garcia-Callejo: Analyzed and interpreted the data; Wrote the paper.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

We would like to express our gratitude to Natalia Denisenko and Alfonso Blanco for their invaluable support and contributions to this research project. Their expertise and dedication greatly enhanced the quality of this publication.

This work had the support of Grant PID2020-118178RB-C22 funded by AEI/10.13039/501100011033, TED2021-130369B-C33 funded by MCIN/AEI/10.13039/501100011033 and by the European Union NextGenerationEU/PRTR, by the Community of Madrid (Spain) under the CYNAMON project (P2018/TCS-4566), co-financed with European Social Fund and EU FEDER funds. We also acknowledge the support of CSIC's Interdisciplinary Thematic Platform (PTI+) on Quantum Technologies (PTI-QTEP+). This study was supported by CSIC's program for the Spanish Recovery, Transformation and Resilience Plan funded by the Recovery and Resilience Facility of the European Union, established by the Regulation (EU) 2020/2094; and MCIN with funding from European Union NextGenerationEU (PRTR-C17.I1).

References

[1] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, Theor. Comput. Sci. 560 (2014) 7–11, https://doi.org/10.1016/j.tcs.2014.05.025.

[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.S. Shaari, M. Tomamichel, V.C. Usenko, G. Vallone, P. Villoresi, P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics 12 (4) (2020) 1012–1236, https://doi.org/10.1364/AOP.361502.

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92 (2) (2020) 025002, https://doi.org/10.1103/RevModPhys.92.025002.

[4] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. 06 (01) (2008) 1–127, https://doi.org/10.1142/S0219749908003256.

[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics 7 (5) (2013) 378–381, https://doi.org/10.1038/nphoton.2013.63.

[6] A. Leverrier, F. Grosshans, P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A 81 (6) (2010) 062343, https://doi.org/10.1103/PhysRevA.81.062343.

[7] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. 2 (1) (2016) 1–12, https://doi.org/10.1038/npjqi.2016.25.

[8] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A 76 (4) (2007) 042305, https://doi.org/10.1103/PhysRevA.76.042305.
[9] F. Grosshans, P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. 88 (5) (2002) 057902, https://doi.org/10.1103/PhysRevLett.88.057902.
[10] A.K. Ekert, Quantum cryptography and Bell's theorem, in: P. Tombesi, D.F. Walls (Eds.), Quantum Measurements in Optics, in: NATO ASI Series, Springer US, Boston, MA, 1992, pp. 413–418.
[11] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81 (3) (2009) 1301–1350, https://doi.org/10.1103/RevModPhys.81.1301.
[12] H.-K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283 (5410) (1999) 2050–2056, https://doi.org/10.1126/science.283.5410.2050.
[13] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (2002) 145–195, https://doi.org/10.1103/RevModPhys.74.145.
[14] G. Zhang, J.Y. Haw, H. Cai, F. Xu, S.M. Assad, J.F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L.C. Kwek, A.Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics 13 (12) (2019) 839–842, https://doi.org/10.1038/s41566-019-0504-5.
[15] N.A. Silva, D. Pereira, N.J. Muga, A.N. Pinto, Practical imperfections affecting the performance of CV-QKD based on coherent detection, in: 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020, pp. 1–4.
[16] F. Laudenbach, C. Pacher, C.-H. Fung, M. Peev, A. Poppe, H. Hübel, Practical noise models for CV-QKD implementations, https://doi.org/10.13140/RG.2.2.24607.25767, 2017.
[17] P. Jouguet, S. Kunz-Jacques, E. Diamanti, A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, Phys. Rev. A 86 (3) (2012) 032309, https://doi.org/10.1103/PhysRevA.86.032309.
[18] N.A. Silva, M. Almeida, D. Pereira, M. Facão, N.J. Muga, A.N. Pinto, 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, pp. 1–4.
[19] W. Liu, J. Peng, J. Qi, Z. Cao, C. He, Imperfect basis choice in continuous-variable quantum key distribution, Laser Phys. Lett. 17 (5) (2020) 055203, https://doi.org/10.1088/1612-202X/ab7eb7.
[20] W. Liu, X. Wang, N. Wang, S. Du, Y. Li, Imperfect state preparation in continuous-variable quantum key distribution, Phys. Rev. A 96 (4) (2017) 042312, https://doi.org/10.1103/PhysRevA.96.042312.
[21] D. Pereira, M. Almeida, M. Facão, A.N. Pinto, N.A. Silva, Impact of receiver imbalances on the security of continuous variables quantum key distribution, EPJ Quantum Technol. 8 (1) (2021) 1, https://doi.org/10.1140/epjqt/s40507-021-00112-z.
[22] H.H. Brunner, L.C. Comandar, F. Karinou, S. Bettelli, D. Hillerkuss, F. Fung, D. Wang, S. Mikroulis, Q. Yi, M. Kuschnerov, A. Poppe, C. Xie, M. Peev, A low-complexity heterodyne CV-QKD architecture, in: 2017 19th International Conference on Transparent Optical Networks (ICTON), 2017, pp. 1–4.
[23] F. Laudenbach, C. Pacher, C.-H.F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations, Adv. Quantum Technol. 1 (1) (2018) 1800011, https://doi.org/10.1002/qute.201800011.
[24] Y. Zhang, Y. Huang, Z. Chen, S. Yu, H. Guo, An improved shot-noise unit calibration for continuous-variable quantum key distribution, in: OSA Quantum 2.0 Conference (2020), Paper QW6B.13, Optica Publishing Group, 2020, QW6B.13.
[25] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H.F. Fung, F. Karinou, A. Poppe, M. Peev, H. Hübel, Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator, Quantum 3 (2019) 193, https://doi.org/10.22331/q-2019-10-07-193.
[26] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, 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 28 (22) (2020) 32882–32893, https://doi.org/10.1364/OE.404611.
[27] A. Leverrier, Theoretical study of continuous-variable quantum key distribution, 2009.
[28] A.G. Mountogiannakis, P. Papanastasiou, B. Braverman, S. Pirandola, Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution, Phys. Rev. Res. 4 (1) (2022) 013099, https://doi.org/10.1103/PhysRevResearch.4.013099.
[29] A. Leverrier, R. García-Patrón, R. Renner, N.J. Cerf, Security of continuous-variable quantum key distribution against general attacks, Phys. Rev. Lett. 110 (3) (2013) 030502, https://doi.org/10.1103/PhysRevLett.110.030502.
[30] R. Renner, Security of quantum key distribution, arXiv:quant-ph/0512258, Jan. 2006.
[31] I. Devetak, A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A, Math. Phys. Eng. Sci. 461 (2053) (2005) 207–235, https://doi.org/10.1098/rspa.2004.1372.
[32] D.B. Soh, C. Brif, P.J. Coles, N. Lütkenhaus, R.M. Camacho, J. Urayama, M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, Phys. Rev. X 5 (4) (2015) 041010, https://doi.org/10.1103/PhysRevX.5.041010.
[33] T. Wang, Z. Zuo, L. Li, P. Huang, Y. Guo, G. Zeng, Continuous-variable quantum key distribution without synchronized clocks, Phys. Rev. Appl. 18 (1) (2022) 014064, https://doi.org/10.1103/PhysRevApplied.18.014064.
[34] U. Leonhardt, Quantum physics of simple optical instruments, Rep. Prog. Phys. 66 (7) (2003) 1207, https://doi.org/10.1088/0034-4885/66/7/203.