

Practical Non-Gaussian Detection for Enhanced Security in CV-QKD Protocols

Joás J. Lacerda, Lucas F. Melo and Alexandre B. Tacla

Abstract—Continuous-variable quantum key distribution (CV-QKD) has emerged as a leading protocol for provably secure cryptographic key exchange, leveraging quantum properties of optical signals while remaining compatible with existing telecom infrastructure. In these systems, the receiver’s detection capability directly impacts the rate at which cryptographic keys can be generated, making it a critical factor for real-time secure communications. Conventional coherent reception schemes (based solely on Gaussian operations) are fundamentally limited in their ability to distinguish quantum states, performing below the ultimate limit allowed by quantum mechanics. Overcoming this limitation requires non-Gaussian detection strategies, which can approach this theoretical bound and unlock higher key generation rates. In this work, we investigate the optimized displacement receiver (ODR) — a non-Gaussian strategy that combines a signal preprocessing step with photon counting — as an alternative to conventional homodyne detection for CV-QKD protocols employing binary phase-shift keying (BPSK) modulation. We evaluate its security performance under realistic conditions by modeling practical detector imperfections such as efficiency loss and noise. Our results show that the ODR achieves higher secret key rates than conventional homodyne detection for all detector efficiencies, at all distances, and across the range of detector noise relevant for practical devices, directly translating into enhanced cryptographic performance and extended transmission range.

Keywords—Quantum cryptography, CV-QKD, BPSK modulation, displacement receiver.

I. INTRODUCTION

In CV-QKD protocols, the choice of measurement scheme at the receiver directly determines how efficiently cryptographic keys can be extracted from the transmitted quantum signals. Standard protocols rely on conventional coherent (homodyne/heterodyne) detection, which correspond to Gaussian measurement schemes [1]. The widespread adoption of these schemes is mainly justified by their seamless integration with standard optical network infrastructure and the existence of well-established security proofs for Gaussian detections [1], [2]. However, these schemes are fundamentally limited in their signal discrimination capability [4]–[6], which ultimately impacts the secret key rate and the security guarantees of the

protocol. This limitation is formalized by the so-called standard quantum limit (SQL), which represents the best discrimination performance achievable by Gaussian schemes [3]. For arbitrary (non-Gaussian) measurements, however, the ultimate bound for discrimination permitted by quantum mechanics is known as the Helstrom limit, which exponentially surpasses the SQL [8]. Several non-Gaussian detection strategies have been proposed in order to approach the Helstrom limit [3], [7], most relying on photon counting techniques, such as on/off detector and photon-number-resolving detection (PNRD) [4], [6], [7]. Recent proposals have shown that incorporating a non-Gaussian operation prior to conventional Gaussian detection achieves near-optimum results [9].

Motivated by the potential security gains in CV-QKD protocols, non-Gaussian receivers have been increasingly investigated as alternatives to conventional coherent detection [4], [10]–[12]. One important example is the optimized displacement receiver (ODR), which consists of performing an amplitude displacement operation on the incoming signal, followed by an on-off photo-detection [3]. However, these studies were conducted only under direct reconciliation—a scheme that significantly limits the achievable secure transmission distance—and under idealized detector models.

In this work, we investigate the ODR as a practical reception strategy for binary phase-shift keying (BPSK) CV-QKD protocols under reverse reconciliation, which enables longer secure transmission distances. To the best of our knowledge, this is the first evaluation of the ODR under reverse reconciliation and realistic detector models, addressing the two main limitations of prior work. Its performance is benchmarked against a conventional homodyne receiver (HR) under both ideal and realistic conditions, with detector imperfections explicitly modeled for each receiver. Using the secret key rate as our security metric, we demonstrate that the ODR outperforms the HR in both ideal and realistic scenarios. Although the ODR exhibits higher sensitivity to detector imperfections, this non-Gaussian strategy outperforms homodyne detection for all values of detector efficiency and noise levels within a realistic range of values.

J. J. Lacerda, QuIIN - Quantum Industrial Innovation, Centro de Competência EMBRAPPII CIMATEC, SENAI CIMATEC, Salvador, Brazil, e-mail: joas.lacerda@fbter.org.br; L. F. Melo, QuIIN - Quantum Industrial Innovation, Centro de Competência EMBRAPPII CIMATEC, SENAI CIMATEC, Salvador, Brazil, email: lucas.felipe@fbter.org.br; A. B. Tacla, QuIIN - Quantum Industrial Innovation, Centro de Competência EMBRAPPII CIMATEC, SENAI CIMATEC, Salvador, Brazil, e-mail: alexandre.tacla@fieb.org.br. This work has been fully funded by the project ‘Nonconventional Receivers in CV-QKD’ supported by QuIIN - Quantum Industrial Innovation, EMBRAPPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPPII.

II. PROTOCOL DESCRIPTION AND SECURITY ASSUMPTIONS

We consider the standard two-party communication scenario, where Alice acts as the transmitter and Bob as the legitimate receiver, communicating over a quantum channel controlled by an eavesdropper Eve. We consider a protocol based on BPSK modulation where in each round, Alice prepares with uniform probability a coherent state from the set $\{|\alpha_k\rangle\}_{k=0}^1$,

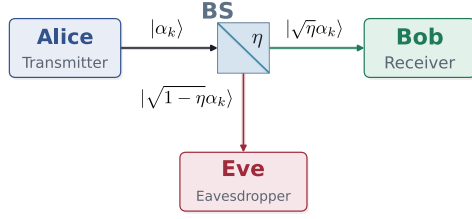


Fig. 1: Wiretap channel model for CV-QKD. Alice randomly transmits coherent states $|\alpha_k\rangle$ to Bob over a pure-loss channel of transmissivity $\eta \in (0, 1)$. Channel losses are modeled by a beam splitter (BS): the transmitted signal $|\sqrt{\eta}\alpha_k\rangle$ reaches Bob, while the reflected signal $|\sqrt{1-\eta}\alpha_k\rangle$ is fully intercepted by Eve — representing the worst-case eavesdropping scenario for this channel model.

where $\alpha_k = (-1)^k \alpha$ with amplitude $\alpha \in \mathbb{R}^+$. These states have the same amplitude but carry opposite phases, enabling their discrimination through a suitable reception strategy at Bob's side. For this preparation, Alice encodes her bit values $\{a_0, a_1\}$ following the mapping rule

$$\begin{aligned} a_0 &\longrightarrow |\alpha\rangle, \\ a_1 &\longrightarrow |-\alpha\rangle. \end{aligned} \quad (1)$$

After encoding, Alice sends the coherent signal through the quantum channel to Bob.

For the security analysis, we consider a wiretap channel (also known as a beam-splitter attack), where Eve passively intercepts all signal losses, representing the worst-case eavesdropping scenario for a pure-loss channel with transmissivity $\eta \in (0, 1)$, i.e., a channel with no excess noise [22]. In this scenario, Bob receives an attenuated state $|\sqrt{\eta}\alpha_k\rangle$, while Eve holds the complementary split state $|\sqrt{1-\eta}\alpha_k\rangle$, as illustrated in Fig. 1. Alice's input state undergoes the transformation

$$|\alpha_k\rangle \longrightarrow |\sqrt{\eta}\alpha_k\rangle_B |\sqrt{1-\eta}\alpha_k\rangle_E, \quad (2)$$

where the subscript B (E) stands for Bob (Eve).

Afterwards, Bob applies one of the reception strategies detailed in Sections III and IV to obtain his measurement outcomes and decode Alice's information. Error correction is then performed through reverse reconciliation, in which Bob's measurement outcomes serve as the reference and he sends correction information to Alice over a public authenticated classical channel.

III. HOMODYNE RECEIVER

The homodyne receiver is a discrimination scheme based on the quadrature measurements of a homodyne detection. For BPSK modulation the usual discrimination strategy consists of associating positive quadrature values with state $|\alpha\rangle$ and negative values with state $|-\alpha\rangle$ [14]. This strategy is described by the measurement operators

$$\hat{\Pi}_0 = \int_0^\infty |x\rangle\langle x|; \quad \hat{\Pi}_1 = 1 - \hat{\Pi}_0, \quad (3)$$

where, $|x\rangle\langle x|$ is a projection operator onto the eigenstates of the quadrature operator $\hat{x}$. Using the HR, Bob builds its raw

key from the set $B = \{b_0, b_1\}$ by the rule

$$B = \begin{cases} b_0 & \text{if } x > 0, \\ b_1 & \text{if } x < 0, \end{cases} \quad (4)$$

where x is the measurement outcome, and $b_0(b_1)$ is the decoded Bob's bit 0(1). From those operators (3), the probability of Bob finding result b_j given that Alice sent bit a_k is $p(b_j|a_k) = \text{Tr}(\hat{\Pi}_j|\alpha_k\rangle\langle\alpha_k|)$, where $\text{Tr}(\cdot)$ is the trace operation.

Homodyne detection consists of a Gaussian operation in the sense that it preserves the Gaussian nature of the incoming state [14]. As shown by Sasaki and Takeoka [3], this strategy reaches the minimum discrimination error probability for binary coherent states achievable by Gaussian operations — the so-called *standard-quantum-limit* (SQL) — which is given by

$$P_e^H = \frac{1}{2}[1 - \text{erf}(\sqrt{2}\alpha)], \quad (5)$$

where $\text{erf}(\cdot)$ is the error function. On the other hand, the lowest discrimination error allowed by quantum mechanics is referred to as the *Helstrom bound* [8]. For the states $\{|\alpha_k\rangle\}_{k=0}^1$, it takes the form $P_{\text{Hel}} = \frac{1}{2}[1 - \sqrt{1 - e^{-4\alpha^2}}]$, and it lies exponentially below the SQL corresponding to the homodyne receiver. Therefore, reaching the quantum discrimination limit necessitates employing non-Gaussian operations.

Generally, an imperfect homodyne detector is characterized by its efficiency γ and electronic noise ν_e (expressed in shot-noise units). These parameters can be modeled considering an ideal detection preceded by a beam-splitter of transmittance $\tau = \gamma$ in which the incident state is mixed with a thermal state of $\bar{n} = \frac{\nu_e}{2(1-\gamma)}$ mean photon number [15]. This way, the imperfection parameters of the detector can be taken into account by the state description. We introduce a subscript in the efficiency parameter γ_h and change the detector electronic noise index ($\nu_e \rightarrow \nu_h$) in order to distinguish the homodyne detector parameters from those that will be defined below.

For an incoming coherent state $|\alpha_k\rangle$, after the beam splitter, it undergoes the transformation

$$\hat{\rho} = |\alpha_k\rangle\langle\alpha_k| \longrightarrow \hat{\rho}_{\text{th}}(\sqrt{\gamma}\alpha_k, \bar{n} = \frac{1}{2}\nu_h), \quad (6)$$

where

$$\hat{\rho}_{\text{th}}(\sqrt{\gamma}\alpha_k, \bar{n} = 1/2 \nu_h) = \int d^2c \frac{e^{-2\frac{|c - \sqrt{\gamma}\alpha_k|^2}{\nu_e}}}{\pi\nu_h/2} |c\rangle\langle c|, \quad (7)$$

is a thermal displaced state centered at α and with mean photon number $\bar{n} = 1/2 \nu_h$, described here by their Glauber-Sudarshan P -representation [13]. The measurement outcomes of a coherent state by an imperfect homodyne detector is equivalent to that of a reciprocal thermal displaced state by an ideal detector.

As a result, the probability that Bob obtains a measurement outcome x given that Alice sent state $|\alpha_k\rangle$, when considering imperfect homodyne detectors, is given by

$$p(x|\alpha_k) = \sqrt{\frac{2}{\pi(1+\nu_h)}} e^{-2\frac{(x - \sqrt{\gamma}\alpha_k)^2}{1+\nu_h}}, \quad (8)$$

and the discrimination error probability becomes $P_e^{\text{IH}} = \frac{1}{2}[1 - \text{erf}(\sqrt{2\gamma_h\alpha}/\sqrt{1+\nu_h})]$, where the superscript “IH” stands for “imperfect homodyne”. Equation (8) is obtained by $\text{Tr}[\hat{\rho}_{\text{th}}(\sqrt{\gamma}\alpha_k, \bar{n} = 1/2 \nu_h)|x\rangle\langle x|]$.

IV. OPTIMIZED DISPLACEMENT RECEIVER

In general, usual non-Gaussian receivers encompass the so-called *direct detection*, i.e., measurement of photon number statistics [16]. Most schemes rely on *on-off* type photo-detectors, i.e., devices that distinguish between the absence or presence of photons. In fact, the first proposal of a receiver to overcome the SQL for binary coherent states $\{|-\alpha\rangle, |\alpha\rangle\}$ comprises a displacement operation $\hat{D}(\alpha)$ where $|-\alpha\rangle$ is sent to vacuum $|0\rangle$ followed by an on-off detection [7]. This strategy, known as Kennedy receiver, identifies a non-detection event as measurement of state $|-\alpha\rangle$ and the detection of any photons as coming from state $|\alpha\rangle$ with an average error probability $P_e^K = 1/2 e^{-4\alpha^2}$. This receiver is regarded as *near-optimal* since for $\alpha^2 \gg 1$, its error probability is roughly a factor of two larger than the Helstrom bound.

Besides being near-optimum, mapping one of the states to vacuum is not the displacement operation that minimizes the discrimination error probability. Choosing a displacement parameter that minimizes this quantity defines a new strategy known as *optimized displacement receiver* [3]. For this case, the displacement operation transforms the input states as

$$|\pm\alpha\rangle \longrightarrow |\beta \pm \alpha\rangle \quad (9)$$

where β is the displacement parameter to be optimized.

This strategy is described by the measurement operators

$$\hat{\Pi}_1 = \hat{D}^\dagger(\beta)\hat{\Pi}_{\text{off}}\hat{D}(\beta); \quad \hat{\Pi}_0 = \hat{D}^\dagger(\beta)\hat{\Pi}_{\text{on}}\hat{D}(\beta) \quad (10)$$

where $\{\hat{\Pi}_{\text{off}}, \hat{\Pi}_{\text{on}}\}$ are the operators that describe an imperfect on-off detection, defined as $\hat{\Pi}_{\text{off}} = e^{-\nu_d} \sum_{n=0}^{\infty} (1-\gamma_d)^n |n\rangle\langle n|$ and $\hat{\Pi}_{\text{on}} = \mathbf{1} - \hat{\Pi}_{\text{off}}$, where $|n\rangle\langle n|$ denotes the projector onto the state of n photons, $\gamma_d \in [0, 1]$ is efficiency of the detector and ν_d is the mean number of dark counts, i.e., Poissonian distributed noise that are random and independent of the incident signal [17]. The subscript “d” stands for “displacement”. From this strategy, Bob yields his bit string by the rule

$$b_k = \begin{cases} b_0 & \text{if } n > 0, \\ b_1 & \text{if } n = 0. \end{cases} \quad (11)$$

Analogously to the modeling of imperfections in homodyne detection, a realistic on-off detector can be represented as an ideal detector preceded by a beam splitter with transmittance $\tau = \gamma_d$. At this beam splitter, the incoming state is combined with a phase-averaged coherent state, with ν_d mean photons, to yield the Poissonian distribution of the dark noise — this contrasts with homodyne detection, where the noise is instead modeled by a thermal state.

The probability of outcome $n = 0$ photons, given that was sent state $|\alpha_k\rangle$, is

$$p(b_1|a_k) = \text{Tr}[\hat{\Pi}_1|\alpha_k\rangle\langle\alpha_k|] = e^{-\nu_d - \gamma_d(\beta + \alpha_k)^2}, \quad (12)$$

from which the probability of measuring $n > 0$ can be obtained through $p(b_0|a_k) = 1 - p(b_1|a_k)$. The average probability error for this strategy is given by

$$P_e^{\text{IOD}} = \frac{1}{2} \left[1 - e^{-\nu_d - \gamma_d(\beta - \alpha)^2} + e^{-\nu_d - \gamma_d(\beta + \alpha)^2} \right], \quad (13)$$

and can be minimized by the parameter β that satisfies $\partial P_e(\beta)/\partial\beta = 0$, resulting in the transcendental equation $\beta_{\text{opt}} = \alpha \coth(2\gamma_d\beta_{\text{opt}}\alpha)$ [3], which can be solved numerically for each α . The superscript “IOD” in Eq. (13) stands for “imperfect optimized displacement”. We can see that the optimum displacement parameter does not depend on the dark count rate. This is related to the fact that dark count is a background noise that equally affects the photon-number statistics of both states $|\pm\alpha\rangle$. From this equation we can find that the optimum displacement parameter β approaches the value α as the amplitude increases, i.e., becomes equivalent to the Kennedy receiver case. This behavior is characteristic of the on-off detection such that photo-detectors with higher resolution present a more involved pattern [18].

V. SECURITY ANALYSIS

For the security analysis, we consider a trusted-noise scenario, i.e., the detector imperfection parameters are not under control of Eve [15]. In a CV-QKD protocol the security is based on the concept that the mutual information achievable between Alice and Bob must exceed the possible information that Eve holds. This idea is quantified by the secret key rate per channel use, which under collective attacks and in the asymptotic limit is given by [23]

$$R = \beta_{\text{rec}} I(A : B) - \chi_{\text{E:B}}, \quad (14)$$

where $\beta_{\text{rec}} \in [0, 1]$ is the efficiency of the information reconciliation, $I(A : B)$ is the mutual information between the trusted parties and $\chi_{\text{E:B}}$ is the Holevo bound that gives the maximum information achievable by Eve conditioned on Bob’s measurement [24].

The mutual information is defined as $I(A : B) = H(A) - H(A|B)$, where $H(A)$ is the classical Shannon entropy of Alice’s variable and $H(A|B)$ is the conditional entropy of Alice given Bob’s measurement [25]. For our equiprobable preparation of binary coherent states $H(A) = 1$ and the mutual information becomes

$$I(A : B) = 1 - \sum_{k=0}^1 p(b_k) H(\{p(a_j|b_k)\}) \quad (15)$$

where $p(b_k) = 1/2 \sum_j p(b_k|a_j)$ is the probability of obtaining the outcome b_k and the conditional probabilities can be obtained by Bayes’s rule $p(a_j|b_k) = p(b_k|a_j)/(2p(b_k))$. Therefore, the mutual information is determined solely by the measurement probabilities of the reception strategy.

As discussed in Section II, in each round Eve receives a state in the set $\{\hat{\rho}_l^E = |\sqrt{1-\eta}\alpha_l\rangle\langle\sqrt{1-\eta}\alpha_l|\}_{l=0}^1$. The Holevo bound on Eve’s information is given by

$$\chi_{\text{E:B}} = S(\hat{\rho}_E) - \sum_k p(b_k) S(\hat{\rho}_{E:b_k}) \quad (16)$$

where $S(\hat{\rho})$ is the von Neumann entropy of the state $\hat{\rho}$, $\hat{\rho}_E = \frac{1}{2} \sum_{l=0}^1 \hat{\rho}_l^E$ is the average state of Eve and $\hat{\rho}_{E:b_k} = \sum_{l=0}^1 p(a_l|b_k) \hat{\rho}_l^E$ is the state of Eve given that Bob's measurement outcome is b_k . Both quantities $S(\hat{\rho}_E)$ and $S(\hat{\rho}_{E:b_k})$ can be calculated by rewriting Eve's average state in its diagonal form through the proper orthonormal basis $\{|\phi_j\rangle\}_{j=0}^1$ [26]:

$$\hat{\rho}_E = \sum_{j=0}^1 \lambda_j^E |\phi_j\rangle \langle \phi_j|, \quad (17)$$

where $\lambda_0^E = e^{-(1-\eta)\alpha^2} \cosh[(1-\eta)\alpha^2]$, and $\lambda_1^E = e^{-(1-\eta)\alpha^2} \sinh[(1-\eta)\alpha^2]$.

In this basis the state $\hat{\rho}_l^E$ of Eve when Alice sends $|\alpha_l\rangle$ is then rewritten as

$$\hat{\rho}_l^E = \sum_{j,k=0}^1 (-1)^{\ell(j+k)} \sqrt{\lambda_j^E \lambda_k^E} |\phi_j\rangle \langle \phi_k|. \quad (18)$$

From these expressions, the von Neumann entropies in Eq. (16) are computed, yielding the Holevo bound and, through Eq. (14), the secret key rate.

VI. NUMERICAL RESULTS AND DISCUSSION

For all plots we consider transmission over an optical fiber with loss parameter 0.2 dB/km which corresponds to a transmittance $\eta = 10^{-0.02L}$ where L is the distance in kilometers, and assume a reconciliation efficiency $\beta_{\text{rec}} = 0.9$.

Figure 2 illustrates the secret key rate (R) as a function of transmission distance for the HR and the ODR under both ideal and realistic scenarios. The considered imperfection parameters are $\nu_h = 0.01, \gamma_h = 0.70$ for the HR, and $\nu_d = 0.001, \gamma_d = 0.75$ for the ODR, which are typical values for realistic conditions [19]–[21]. For each distance the signal mean photon number is chosen to maximize the protocol's performance. It can be seen that the SKR exhibits a uniform decay rate with distance across all configurations, regardless of the receiver type or scenario. As expected, detector imperfections degrade the performance of both receivers relative to their ideal counterparts. However, the ODR consistently outperforms the HR in both ideal and realistic regimes. Furthermore, the performance of the realistic ODR remains remarkably close to that of the ideal HR across all distances, equaling it in the short-distance regime.

To better visualize the impact of imperfection parameters, Figure 3 plots the secret key rate against the efficiency and noise of the respective receivers. For both plots we set the distance at $L = 50$ km. The remaining parameters are fixed at $\gamma_h = 0.70$ and $\gamma_d = 0.75$ for the noise plot and $\nu_h = 0.01$ and $\nu_d = 0.001$ for the efficiency evaluation. Fig. 3a demonstrates that the ODR outperforms the HR across all evaluated detector efficiencies. To illustrate this advantage, we show the secret rate obtained by the HR for a detector efficiency of $\gamma_h = 0.70$, $R = 6.7 \times 10^{-3}$ (horizontal dashed line). This same key rate is attained by the ODR with a detector efficiency of only $\gamma_d = 0.57$.

The dependence of the key rate on the detector noise is more involved. Fig. 3b shows that for noise above $\nu > 0.195$, the HR outperforms the ODR, with the difference between

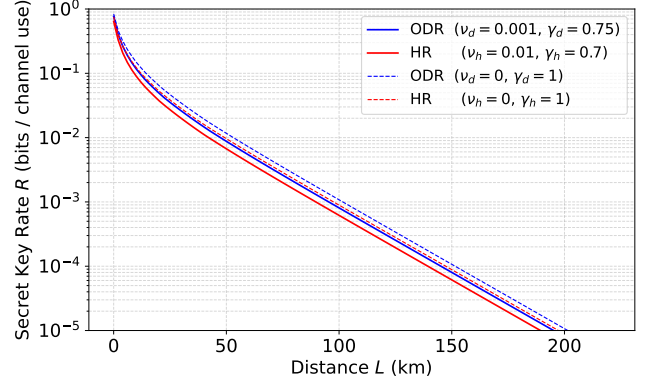


Fig. 2: Secret Key Rate R as a function of the transmission distance L for the optimized displacement receiver (ODR), blue lines, and homodyne receiver (HR), red lines, in the ideal (dashed lines) and realistic (solid lines). We consider a reconciliation efficiency $\beta = 0.9$ and imperfection parameters $\nu_d = 0.001, \gamma_d = 0.75$ for the realistic ODR and $\nu_h = 0.01, \gamma_h = 0.70$ for the realistic HR.

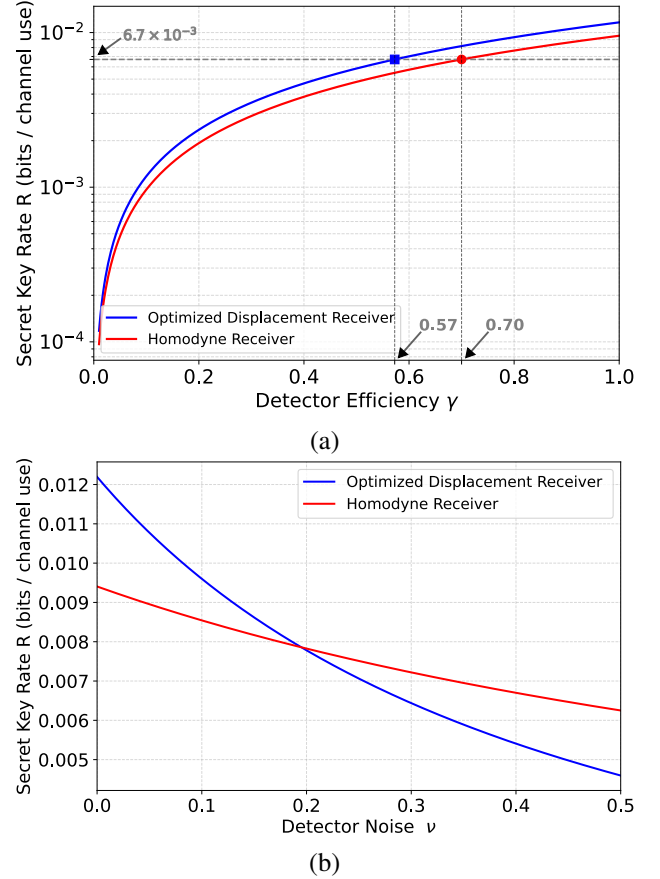


Fig. 3: (a) Plot of the secret key rate R as a function of detector efficiency γ . The detector noises were set $\nu_d = 0.001$, for the optimized displacement receiver and $\nu_h = 0.01$ for the homodyne receiver. (b) Plot of secret key rate as a function of detector noise. The detector efficiencies were considered $\gamma_d = 0.75$, and $\gamma_h = 0.70$ for the optimized displacement and homodyne receiver, respectively. Both plots were calculated for a distance $L = 50$ km and reconciliation efficiency $\beta_{\text{rec}} = 0.9$.

the performance of both receivers growing rapidly as noise values increase. However, for lower noise values the ODR presents a higher secret key rate. As noted earlier, the usual values for dark counts on the ODR and electronic noise on the HR are significantly lower than the intersection point $\nu = 0.195$. Consequently, the ODR exhibits superior secret key rate performance under realistic scenarios. On the other hand, this strategy exhibits a higher sensitivity to detector noise compared to the HR. This behavior is confirmed by evaluating the derivatives with respect to the correspondent noise of each detector. The ODR presents a minimum derivative of $dR/d\nu_d = -0.46$, whereas the HR displays enhanced robustness, yielding a minimum value of $dR/d\nu_h = -0.13$. The ODR is likewise more sensitive to changes in efficiency, although the discrepancy compared with HR is smaller. Specifically, the ODR exhibits a minimum derivative of $dR/d\gamma_d = 0.14$, compared with a minimum of $dR/d\gamma_h = 0.12$ for the HR.

VII. CONCLUSION

In this paper, we investigated the ODR as a practical non-Gaussian reception strategy for BPSK CV-QKD protocols under reverse reconciliation, comparing it against the conventional HR under both ideal and realistic detector conditions. By explicitly modeling the imperfection parameters that characterize each strategy, we determined the optimal displacement for the ODR within these parameters. Our numerical results show that the ODR outperforms the conventional HR in the ideal case and throughout the realistic regime of detector imperfections. The advantage holds for all detector efficiencies and at all distances considered. With respect to detector noise, the ODR remains superior up to a crossover at $\nu \approx 0.195$ above which the HR becomes advantageous. On the other hand, the HR is less sensitive to noise variation, which is why it eventually surpasses the ODR, but only at detector-noise values far above practical levels [19]–[21]. As future directions, we intend to extend this study to modulation schemes with a larger number of coherent states and to generalize the analysis to channels with excess noise, moving toward more realistic deployment conditions.

ACKNOWLEDGMENTS

This work has been fully funded by the projects “Receptores não-convencionais em CV-QKD”, “Análise de segurança de protocolos P&M CV-QKD” and “Design e arquiteturas de protocolos CV-QKD” supported by the EMBRAP II CIMATEC Competence Center in Quantum Technologies-Quantum Industrial Innovation (QuIIN), with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI Grant No. 053/2023, signed with EMBRAP II.

REFERENCES

- [1] M. F. Anka, J. A. Mora Rodríguez, D. F. Pinto, L. Q. Galvão, M. A. Dias, and A. B. Tacla, *An Introductory Review of the Theory of Continuous-Variable Quantum Key Distribution: Fundamentals, Protocols, and Security*. Brazilian Journal of Physics, vol. 56, no. 2, p. 72, 2026.
- [2] Y. Zhang, D. Huang, Z. Chen, and H. Guo, *Continuous-variable quantum key distribution system: Past, present, and future*. Applied Physics Reviews, vol. 11, no. 1, p. 011305, 2024.
- [3] M. Takeoka and M. Sasaki, *Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers*. Physical Review A, vol. 78, p. 022320, 2008.
- [4] C. Wittmann, U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, *Demonstration of Coherent-State Discrimination Using a Displacement-Controlled Photon-Number-Resolving Detector*. Physical Review Letters, vol. 104, p. 100505, 2010.
- [5] S. Izumi, J. S. Neergaard-Nielsen, S. Miki, H. Terai, and U. L. Andersen, *Experimental Demonstration of a Quantum Receiver Beating the Standard Quantum Limit at Telecom Wavelength*. Physical Review Applied, vol. 13, p. 054015, 2020.
- [6] F. E. Becerra, J. Fan, and A. Migdall, *Photon number resolution enables quantum receiver for realistic coherent optical communications*. Nature Photonics, vol. 9, no. 1, pp. 48–53, 2014.
- [7] R. S. Kennedy, *A Near-Optimum Receiver for the Binary Coherent State Quantum Channel*. MIT RLE Quarterly Progress Report No. 108, pp. 219–225, 1973.
- [8] C. W. Helstrom, *Quantum detection and estimation theory*. Journal of Statistical Physics, vol. 1, no. 2, pp. 337–354, 1969.
- [9] J. Moran, S. Kechrimparis, and H. Kwon, *Near-optimal coherent state discrimination via continuously labelled non-Gaussian measurements*. Quantum, vol. 10, p. 2016, 2026.
- [10] M. Cattaneo, M. G. A. Paris, and S. Olivares, *Hybrid quantum key distribution using coherent states and photon-number-resolving detectors*. Physical Review A, vol. 98, no. 1, p. 012333, 2018.
- [11] M. Zhao, R. Yuan, J. Cheng, and S. Han, *Security of Binary Modulated Continuous Variable Quantum Key Distribution Using Optimally Displaced Threshold Detection*. IEEE Communications Letters, vol. 25, no. 4, pp. 1089–1093, 2021.
- [12] M. Zhao, R. Yuan, C. Feng, S. Han, and J. Cheng, *Security of Coherent-State Quantum Key Distribution Using Displacement Receiver*. IEEE Journal on Selected Areas in Communications, vol. 42, no. 7, pp. 1871–1884, 2024.
- [13] R. J. Glauber, *Coherent and Incoherent States of the Radiation Field*. Physical Review, vol. 131, no. 6, pp. 2766–2788, 1963.
- [14] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*. Reviews of Modern Physics, vol. 84, no. 2, pp. 621–669, 2012.
- [15] J. Lin and N. Lütkenhaus, *Trusted Detector Noise Analysis for Discrete Modulation Schemes of Continuous-Variable Quantum Key Distribution*. Physical Review Applied, vol. 14, no. 6, p. 064030, 2020.
- [16] M. N. Notarnicola, *Quantum communications in continuous variable systems*. International Journal of Quantum Information, vol. 23, no. 03, p. 2550003, 2025.
- [17] S. M. Barnett, L. S. Phillips, and D. T. Pegg, *Imperfect photodetection as projection onto mixed states*. Optics Communications, vol. 158, no. 1, pp. 45–49, 1998.
- [18] M. T. DiMario and F. E. Becerra, *Robust Measurement for the Discrimination of Binary Coherent States*. Physical Review Letters, vol. 121, no. 2, p. 023603, 2018.
- [19] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental demonstration of long-distance continuous-variable quantum key distribution*. Nature Photonics, vol. 7, no. 5, pp. 378–381, 2013.
- [20] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, *Self-Referenced Continuous-Variable Quantum Key Distribution Protocol*. Physical Review X, vol. 5, no. 4, p. 041010, 2015.
- [21] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, *High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM*. Proceedings of the European Conference on Optical Communication (ECOC), pp. 1–4, 2021.
- [22] M. Heid and N. Lütkenhaus, *Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction*. Physical Review A, vol. 73, no. 5, p. 052316, 2006.
- [23] I. Devetak and A. Winter, *Distillation of secret key and entanglement from quantum states*. Proceedings of the Royal Society A, vol. 461, pp. 207–235, 2005.
- [24] A. S. Holevo, *Statistical problems in quantum physics*. Proceedings of the Second Japan-USSR Symposium on Probability Theory, Springer Berlin Heidelberg, vol. 330, pp. 104–119, 1973.
- [25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2nd ed., 2006.
- [26] A. Chefles and S. M. Barnett, *Optimum unambiguous discrimination between linearly independent symmetric states*. Physics Letters A, vol. 250, no. 4, pp. 223–229, 1998.