Aspects of measurement device independent continuous variable quantum key distribution protocols

Douglas F. Pinto[*,1] **and Alexandre B. Tacla**[1]

[1] *QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Salvador, BA, Brazil*

[*] *douglas.pinto@fieb.org.br*

Abstract: Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) protocols were introduced to address vulnerabilities related to detector side-channel attacks in traditional QKD systems. In conventional architectures, imperfections or inadequate protection of detectors may be exploited by an eavesdropper to compromise security without violating the principles of quantum mechanics. In contrast, MDI-QKD removes the need to trust the detectors by delegating the measurement stage to a central relay, which may even be controlled by an adversary, without compromising the security of the key shared between legitimate users. The integration of the MDI paradigm with the advantages of continuous-variable QKD (CV-QKD), such as compatibility with telecommunication technologies, room-temperature operation, and the elimination of the need for single-photon sources, makes MDI-CV-QKD a highly promising approach for metropolitan-scale quantum networks. Additionally, it supports high key rates over short distances. In the prepare-and-measure version, Alice and Bob encode data into modulated coherent (or squeezed) states using Gaussian or non-Gaussian distributions and send them to an untrusted relay, where a continuous-variable Bell measurement is performed using balanced beam splitters and homodyne detectors. The measurement results are publicly announced but do not reveal information about Alice's and Bob's original states, preserving security through sufficient statistical correlations. In this work, we present a study of the MDI-CV-QKD protocol in a symmetric scenario under symmetric attacks. Although this configuration is not the most efficient from a theoretical standpoint, it holds practical relevance. Moreover, the assumed symmetry enables a simplified security analysis, allowing for the derivation of feasible analytical expressions.
Keywords: Continuous variable quantum key distribution. Measurement device independent. Coherent states. Bell measurement.

1. Introduction

Quantum cryptography has emerged as one of the most mature quantum technologies for ensuring secure communication in the era of rapidly advancing quantum computing [1-6]. Among the various quantum key distribution (QKD) protocols, CV-QKD systems stand out due to their compatibility with existing optical infrastructures and their ability to deliver high secret key rates [6]. However, the practical implementation of CV-QKD still faces significant challenges over long distances, mainly due to optical channel loss, limited detection efficiency, and vulnerabilities associated with measurement devices [2,6]. In this context, measurement-device-independent QKD (MDI-QKD) protocols represent a promising alternative for mitigating attacks that exploit detector imperfections [1]. By combining the advantages of CV-QKD and MDI-QKD protocols, MDI-CV-QKD aims to enable secure key distribution at high rates over metropolitan distances while simultaneously removing trust assumptions on measurement devices. The first MDI-CV-QKD protocol was proposed in [2-3], employing Gaussian modulation of coherent states and continuous-variable Bell detection. This approach laid the groundwork for a new class of protocols capa-

ble of leveraging the practicality of continuous-variable systems with the enhanced security of MDI architectures.

2. MDI-CV-QKD Protocol

MDI-CV-QKD protocols represent a class of quantum key distribution (QKD) schemes that combine two key approaches:

- Continuous Variables (CV-QKD): Information is encoded in continuous properties of light, such as the amplitude and phase quadratures of coherent or squeezed states.
- Measurement device independence: The need to trust measurement devices is eliminated by delegating detection to an untrusted central relay.

As in conventional CV-QKD protocols, MDI-CV-QKD also admits two distinct yet equivalent representations: the prepare-and-measure version, which enables practical implementation of the protocol, and the entanglement-based version, which provides the mathematical framework necessary for security analysis. In the prepare-and-measure version of MDI-CV-QKD protocols, Alice and Bob encode the key into modulated coherent states, which are sent to a central station (Charlie).

Charlie performs a continuous-variable Bell measurement, and the results are publicly announced, allowing Alice and Bob to share a secret key without revealing sensitive information to a potential eavesdropper (Eve), even if she controls the relay. In the entanglement-based representation, there is a difference in the state preparation stage: Alice and Bob independently prepare two-mode squeezed vacuum (TMSV) states, sending one mode to the relay while retaining the other. These retained modes are measured locally via heterodyne detection at Alice's and Bob's stations, while the transmitted modes undergo the same Bell measurement procedure as in the preparation-and-measure case.

This version can be interpreted as an entanglement swapping protocol, where the Bell measurement on the transmitted modes generates a Gaussian entangled state between the modes held by Alice and Bob.

2.1. Protocol Steps

Quantum State Preparation: Alice and Bob independently encode your information into the quadratures of coherent states, using randomly modulated amplitudes. Consequently, Alice initiates the protocol by preparing mode A in a coherent state $|\alpha\rangle$ where the complex amplitude α is modulated according to a two-dimensional Gaussian distribution with zero mean and variance φ in each quadrature. Similarly, Bob prepares mode B in a coherent state $|\beta\rangle$, where β follows the same Gaussian modulation. These states

are then transmitted through potentially insecure quantum channels to a central relay, which performs a continuous-variable Bell measurement [2-5]. In the entanglement-based representation, Alice and Bob prepare a two-mode squeezed vacuum (TMSV) state. By performing a heterodyne measurement on one mode of their entangled pair, both Alice and Bob effectively prepare a coherent state through the resulting projection on the complementary mode. This correspondence establishes the statistical and operational equivalence between the prepare-and-measure and entanglement-based models [2]. Continuous-Variable Bell Measurement: The relay performs a Bell measurement by mixing modes A and B on a balanced (50:50) beam splitter, whose action is described by the following unitary transformation: $\hat{a}_C = (\hat{a}_A - \hat{a}_B)\sqrt{2}$ and $\hat{a}_D = (\hat{a}_A + \hat{a}_B)\sqrt{2}$ representing the annihilation operators of the output modes, which can be rewritten in terms of $\hat{q}_C = (\hat{q}_A - \hat{q}_B)\sqrt{2}$ and $\hat{p}_D = (\hat{p}_A + \hat{p}_B)\sqrt{2}$, the relay measures the conjugate quadratures $\hat{q}_C$ and $\hat{p}_D$ via homodyne detection, yielding the following classical values $\langle \hat{q}_C \rangle = q_-$ and $\langle \hat{p}_D \rangle = p_+$. These outcomes are combined into the complex variable $\gamma = (q_- + ip_+)/\sqrt{2}$. The probability distribution $p(\gamma)$ depends on the Gaussian modulations applied by Alice and Bob. The value of γ is then publicly announced, via a classical and authenticated channel, allowing Alice and Bob to establish classical correlations without revealing their individual data [2].

Interception Strategies: The most general eavesdropping strategy consists of a coordinated attack targeting both Charlie's measurement device and the communication channels along links L_{AC} and L_{BC} effectively modeling a global unitary attack on the whole system accessible to Eve. In this case, since the protocol employs Gaussian modulation and Gaussian-state detection, the optimal attack necessarily involves Gaussian unitary operations. This is justified in the asymptotic regime against collective attacks, where the extremality of Gaussian states ensures that, for fixed covariance matrices, Gaussian attacks maximize the accessible information to the eavesdropper. This greatly simplifies the security analysis [7]. Taking into account the reconciliation efficiency β, the secret key rate is given by

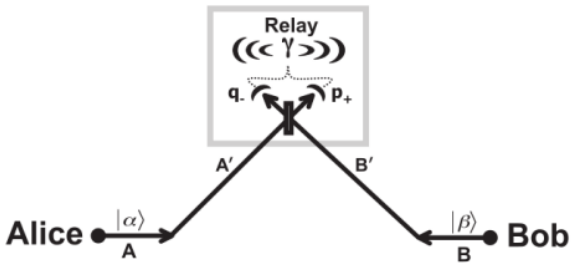
$$K := \beta I(A:B) - I_E \tag{1}$$

where $I(A:B)$ denotes the mutual information between Alice and Bob, and I_E denotes Eve's Holevo information with respect to the reference party [2, 6]. Both the mutual information and Eve's Holevo information are conditioned on the variable γ.

3. Symmetric MDI-CVQKD model

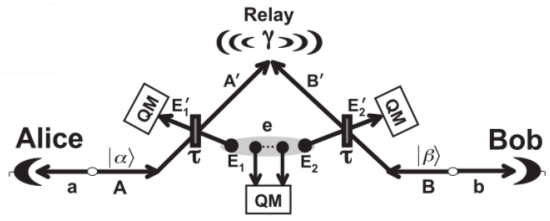
The theoretical analysis of the MDI-CV-QKD protocol begins with the modeling of the quantum states prepared by Alice and Bob. In the entanglement-based representation both parties generate EPR pairs, whose covariance matrix

Figure 1: Prepare-and-Measure scheme configuration of the protocol extracted from [10].



Symmetric setup with the untrusted relay located midway between the parties.

Figure 2: Illustration of the entanglement-based scheme of the protocol extracted from the article [10].



Entanglement-based picture of the protocol under a two-mode Gaussian attack. Eve introduces ancillary modes through two beam splitters with transmissivity τ.

(CM) is given by [8, 9]:

$$V(\mu) = \begin{pmatrix} \mu\mathbb{I} & \sqrt{\mu^2-1}\sigma_z \\ \sqrt{\mu^2-1}\sigma_z & \mu\mathbb{I} \end{pmatrix} \quad (2)$$

where $\mu = \varphi + 1$ describes the noise variance in the quadratures (associated with the degree of squeezing), $\mathbb{I}$ is the 2x2 identity matrix and $\sigma_z = diag(1,-1)$ is the Pauli Z matrix. This state encodes quadrature correlations that are essential for the protocol.

3.1. State preparation with local detection

To transform these EPR states into coherent states to be sent through the channel, modes a and b from Alice and Bob, respectively, are measured locally via heterodyne detection. This measurement introduces vacuum noise and projects modes A and B into coherent states $|\alpha\rangle$ and $|\beta\rangle$ (with a certain attenuation relative to the coherent state prepared in the PM model), with a resulting conditional covariance matrix [8]:

$$V_{A|a} = V_{B|b} = \mu\mathbb{I} - \frac{\mu^2-1}{\mu+1}\mathbb{I} = \mathbb{I}, \quad (3)$$

this transformation results in the transmission of coherent states to the untrusted central relay (Charlie), which performs a Bell measurement.

3.2. Central relay action and Eve's Attack

The global quantum system is then composed of the modes of Alice, Bob, and Eve, structured in a global CM: $V_{aABbE_1E_2} = V_{aA} \oplus V_{bB} \oplus V_{E_1E_2}$, where Eve's contribution is modeled as a two-mode Gaussian state. It is convenient to permute the modes such that the covariance matrix is arranged in the order of action of the beam splitters, with $V_{abAE_1E_2B}$ and $\mathbb{I}_a \oplus \mathbb{I}_b \oplus BS$, where $BS = S(\tau) \oplus S(\tau)^T$.

The characterization of the two-mode Gaussian attack performed by Eve involves the reduced state of two auxiliary modes, E_1 and E_2, extracted from

a reservoir and interacting with modes A and B through two beam splitters with transmissivity τ (symmetric model). The mixing of the modes via this interaction accounts for the losses in the Alice–Charlie and Bob–Charlie channels. After the action of the beam splitters, the output auxiliary systems E_1 and E_2, are stored in a quantum memory, along with the remaining auxiliary systems of the reservoir. The covariance matrix of Eve's two-mode state, in the symmetric normal form associated with the reduced state, is given by:

$$V_{E_1E_2} = \begin{pmatrix} \omega\mathbb{I} & G \\ G & \omega\mathbb{I} \end{pmatrix}, \tag{4}$$

where $G = diag\,(g, g')$ determines the correlations between E_1 and E_2 , while ω represents the variance of the thermal noise introduced at the beam splitters. For given values of thermal noise, Eve's covariance matrix is fully determined by the correlation parameters, which must satisfy a set of bona fide conditions (derived by the uncertainty principle) and can be represented as a point in a correlation plane. Due to the symmetry of the protocol, it is possible to reduce the number of parameters and derive a simple analytical expression for the secret-key rate. This allows for the analysis of symmetric attacks in terms of the correlation parameters g and g'.

In this work, we consider only the case where Eve's systems are uncorrelated ($g = g' = 0$). The symmetry also ensures the equivalence between direct and reverse reconciliation. After the attack, the output modes A' and B' are subjected to continuous-variable Bell detection, while Eve's output modes, E'_1 and E'_2, together with all other ancillary modes, are measured by a coherent measurement at the end of the protocol. We can compute the secret key rate from the conditional state of modes a and b after homodyne detections performed by Charlie and the communication of the outcome γ. In this case, the rate is given by $K = I_{ab|\gamma} - I_{E|\gamma}$, with $I_{E|\gamma}$ being the conditional mutual information between Alice and Bob, and $I_{ab|\gamma}$ represents the Holevo information accessible to Eve from the output ancillary states.

Since the output modes are in a global pure state, and given the nature of the homodyne and heterodyne detections performed, the von Neumann entropies associated with the post-relay conditional state of Alice and Bob, as well as the state of Bob conditioned on the detections by Alice and the central relay, allow the determination of Eve's Holevo information:

$$I_{E|\gamma} = S\left(\rho_{ab|\gamma}\right) - S\left(\rho_{b|\gamma\tilde{\alpha}}\right) \tag{5}$$

and the mutual information can be computed via signal-to-noise ratio [2]:

$$I_{AB} = \log\left(\frac{\mu}{\chi}\right) \tag{6}$$

where the noise term $\chi = \chi(\tau, \omega)$, can be de-

scribed by the reduced covariance matrices after the relay and after Alice's measurement.

From the covariance matrix $V_{ab|\gamma}$, all the information required to compute the secret key rate can be determined. Under the imposed symmetry conditions, it takes the following form:

$$V_{ab|\gamma} = \begin{pmatrix} \mu - xy & & xy & \\ & \mu - xy' & & -xy' \\ xy & & \mu - xy & \\ & -xy' & & \mu - xy' \end{pmatrix}, \tag{7}$$

with

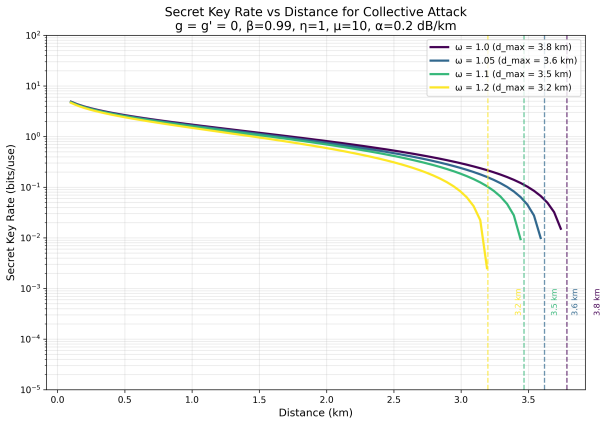
$$\begin{cases} x := \tau\left(\mu^2 - 1\right)/2 \\ y := 1/\left(\tau\mu + \lambda\right), \qquad y' := 1/\left(\tau\mu + \lambda'\right) \\ \lambda := (1-\tau)\left(\omega - g\right), \quad \lambda' := (1-\tau)\left(\omega - g'\right). \end{cases}$$

To determine the entropic quantity $S\left(\rho_{ab|\gamma}\right)$, in this context, it is sufficient to compute the symplectic eigenvalues of the covariance matrix. In the limit $\mu >> 1$, It is possible to obtain [2,9,10] $S\left(\rho_{ab|\gamma}\right) = \log e^2\sqrt{\lambda\lambda'}\mu/4\mu$, and now, for computing the double conditional covariance matrix, it is convenient put the $V_{ab|\gamma}$ in the block form and apply the heterodyne detection on Alice's mode a, getting

$$S\left(\rho_{b|\gamma\tilde{\alpha}}\right) = h\left(\sqrt{(\tau+2\lambda)\left(\tau+2\lambda'\right)}/\tau\right), \tag{8}$$

and therefore we have the Holevo quantity. The conditional mutual information between Alice and

Figure 3: (Color online) Secret key rate as a function of distance under collective attacks for different levels of thermal noise.



Secret key rate as a function of distance for a CV-QKD protocol under collective attacks, assuming a symmetric configuration and setting the correlation parameters $g = g' = 0$. The analysis considers thermal noise levels $\omega = \{1; 1.05; 1.1; 1.2\}$, reconciliation efficiency $\beta = 0.99$, modulation variance $\mu = 10$, and fiber loss rate 0.2 dB/km . The secret key rate is computed using analytical expressions derived under Gaussian collective attacks. The vertical dashed lines indicate the maximum secure distances $K = 0$ for each value of ω, beyond which key distribution is no longer secure.

Bob can be computed from the covariance matrix, and thus we can obtain the $\left(V_{ab|\gamma} + \mathbb{I}\right)/2$ expression for the secret key rate in the symmetric model [10]:

$$K = \log\left(\frac{\tau}{e^2\sqrt{\lambda\lambda'}\left(\tau+\lambda\right)\left(\tau+\lambda'\right)}\right) + h\left[\sqrt{(\tau+2\lambda)\left(\tau+2\lambda'\right)}/\tau\right]. \tag{9}$$

In the key rate calculations, we considered the particular case where $g = g' = 0$ and evaluated the distances that allow for a positive key rate under the presence of thermal noise and in the pure-loss regime. We identified a maximum distance of 3.8

km for pure loss and 3.2 km for the case with $\omega = 1.2$. These ranges are expected to increase in the asymmetric scenario, which will be addressed in the continuation of this work, along with the evaluation of other protocol parameters.

4. Final Remarks

In this work, we analyze the MDI-CV-QKD protocol based on Ref. [10], considering a symmetric scenario under symmetric attacks. Although this configuration is not the most efficient from a theoretical perspective, it remains relevant due to its potential for practical implementation in quantum network applications. Moreover, the symmetry allows for a simplified security analysis, enabling the derivation of more simple analytical expressions.

Acknowlegement

This work has been fully funded by the project "Comparative Analysis of PM protocols for Quantum Cryptography" supported by QuIIN - Quantum Industrial Innovation, EMBRAPII 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 EMBRAPII.

References

1. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett. 2012;108(13):130503.

2. Pirandola S, et al. High-rate measurement-device-independent quantum cryptography. Nat Photonics. 2015;9(6):397–402.

3. Ma XC, et al. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. Phys Rev A. 2014;89(4):042335.

4. Fletcher AI, et al. An overview of CV-MDI-QKD. arXiv Preprint. 2025;arXiv:2501.09818.

5. Li Z, et al. Continuous-variable measurement-device-independent quantum key distribution. Phys Rev A. 2014;89(5):052301.

6. Ghoreishi SA, et al. The future of secure communications: device independence in quantum key distribution. arXiv Preprint. 2025;arXiv:2504.06350.

7. García-Patrón R, Cerf NJ. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett.

2006;97(19):190503.

8. Laudenbach F, et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. Adv Quantum Technol. 2018;1(1):1800011.

9. Weedbrook C, et al. Gaussian quantum information. Rev Mod Phys. 2012;84(2):621–69.

10. Ottaviani C, Spedalieri G, Braunstein SL, Pirandola S. Continuous-variable quantum cryptography with an untrusted relay: detailed security analysis of the symmetric configuration. Phys Rev A. 2015;91(2):022320.