On the Limitations of Gaussian Techniques for Security Analysis of BPSK-modulated CV-QKD Protocols

John A. Mora Rodríguez[1, 2], Leonardo J. Pereira[1], Maron F. Anka[1], Alexandre Baron Tacla[1]
[1] *QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845. 41650-010, Salvador, BA, Brazil*
[2] *IMECC-Unicamp, Departamento de Matemática Aplicada, Universidade Estadual de Campinas (Unicamp), Rua Sérgio Buarque de Holanda 651, Cidade Universitária Zeferino Vaz. 13083-859, Campinas - SP, Brazil*

Abstract: We study the effect of the symmetrization procedure commonly used in the security analysis of continuous-variable quantum key distribution (CV-QKD) protocols with discrete modulation. Focusing on the BPSK protocol with homodyne detection, we show that such symmetrization, which artificially extends the modulation to both quadratures, is not necessary to recover a covariance matrix compatible with Gaussian analysis. By exploiting only the natural π-rotation symmetry of the BPSK constellation, we obtain a structure closely matching that used in Gaussian security proofs. Our numerical results for a pure-loss channel indicate that the standard symmetrization procedure tends to overestimate Eve's information, while simpler approaches without symmetrization still exhibit analogous behavior without requiring any additional construction. This result highlights that the non-Gaussian structure of the modulation is a fundamental challenge that cannot be easily circumvented, suggesting that protocols with unidimensional modulation may be analyzed without relying on artificial Gaussianization, paving the way for future security proofs adapted to their true structure. A unidimensional protocol (asymmetric in the quadratures) allows the sender to use only a single modulator instead of two, which can potentially lead to more cost-effective implementations. For this reason, studying the BPSK protocol, which is the simplest example of unidimensional modulation, can provide valuable insights into the performance and characteristics of more general schemes.

Keywords: Continuous-variable quantum key distribution (CV-QKD), Discrete modulation, Unidimensional modulation, BPSK protocol, Gaussian states, Symmetrization procedure, Security analysis, Holevo quantity.

Continuous-variable quantum key distribution (CV-QKD) protocols (see [1, 2]) with discrete modulation have attracted growing interest due to their practical advantages, including ease of implementation, compatibility with standard telecom components, and low cost. Among them, one-dimensional (1D) modulation schemes, where information is encoded in quantum states of a single quadrature of the electromagnetic field, offer a particularly simple yet effective framework for secure quantum communication.

One of the simplest examples of such a scheme is the 1D BPSK (Binary Phase-Shift Keying) protocol. In this protocol, the sender, Alice, prepares a coherent state chosen from the binary set $\{|\alpha\rangle,|-\alpha\rangle\}$, modulated only along the x-quadrature (with $\alpha \in \mathbb{R}$), and sends it to the receiver, Bob, through a lossy Gaussian channel. Bob performs homodyne detection in the modulated quadrature to recover the bit of information encoded by Alice. In QKD, the channel is assumed to be insecure and controlled by an evesdropper, Eve. For instance, Eve could tap the communication channel, resulting in signal losses. However, despite the signal leak, QKD protocolos leverage the principles of quantum mechanics to ensure that security in communication. This is done via classical post-processing steps, which result in the Generation of a secret key. In the first step, the amount of loss is estimated in order to determine how much information could be leaking to Eve, then Alice and Bob reconcile their correlated data (here we assume reverse reconciliation), correct errors,

and, finally, apply privacy amplification using a hash function, to produce a symmetric secret key [3]. The security of this protocol can be quantified using the Devetak–Winter bound [4], which estimates the difference between the information shared by Alice and Bob (quantified by Alice and Bob's mutual information) and an upper bound on Eve's accessible information (quantified through the Holevo information) [5].

The analysis of 1D protocols has been previously considered in the literature. In [6], Zhao et al. introduced a CV-QKD protocol based on binary modulation, while in [7], Usenko and Grosshans analyzed the case of Gaussian modulation limited to a single quadrature. These works highlight the relevance of 1D schemes, both for simplifying experimental setups and for understanding fundamental security limits.

One challenge with discrete modulation is the lack of Gaussian structure, which prevents direct application of powerful security tools developed for Gaussian states [8]. To address this, recent studies (e.g., [9, 10, 11]) have introduced a symmetrization procedure that effectively makes the overall state more Gaussian by artificially extending the modulation to both quadratures of the field. While this helps simplify the security analysis (particularly when leveraging the optimality of Gaussian attacks [12, 13]) it also alters the structure of the protocol by removing its inherent restriction to modulation along a single direction in phase space.

In this work, we revisit the need for symmetrization in the BPSK protocol. We demonstrate that by choosing a natural purification of the modulation state and exploiting only the intrinsic symmetry of the BPSK constellation, namely, invariance under a π-rotation in phase space, one can recover a covariance matrix structure that is already very close to that of a Gaussian unidimensional protocol. This allows the use of standard Gaussian techniques without artificially modifying the protocol.

Furthermore, through numerical simulations in the pure-loss channel model, we show that the key rates obtained from the natural (non-symmetrized) covariance matrix match closely the results from more accurate numerical methods for distances over 40 km, which corresponds to a regime of low signal-to-noise ratio. For shorter distances, our symmetrization approach is no longer a faithful approximation, due to the non-gaussian nature of the BPSK. These results suggest that enforcing Gaussianity through symmetrization may be unnecessary, and even suboptimal, for 1D BPSK CV-QKD protocols.

1. BPSK modulation

The 1D BPSK protocol operates according to the following scheme: Alice prepares a coherent state chosen from the binary set $\{|\alpha\rangle,|-\alpha\rangle\}$, each selected with equal probability 1/2, and transmits it through a bosonic Gaussian channel characterized by transmittance T and excess noise ξ. Upon reception, Bob performs homodyne detection, primarily measuring the x-quadrature (the modulated component).

While the protocol is designed around x-quadrature modulation, reliable estimation of

channel parameters necessitates occasional sampling of the unmodulated p-quadrature. To achieve this, Bob sporadically switches to p-quadrature measurements. However, if the number of rounds of the protocol tends to infinity the impact of this sampling on the key rate becomes negligible, as discussed in [14].

Following the quantum communication and data acquisition phase, Alice and Bob apply the classical postprocessing steps mentioned above [15] to extract a shared secret key based on Bob's measurement outcomes in the x-quadrature (in the case of reverse reconcilliation). The achievable key rate in the asymptotic regime is lower bounded by the Devetak-Winter formula [4]:

$$K = I(A;B) - \sup \chi\,(B;E),$$

where $I(A;B)$ denotes the mutual information between Alice's and Bob's classical data, and $\chi(B;E)$ is the Holevo quantity that bounds Eve's accessible information.

To numerically evaluate a lower bound on the key rate in the context of discrete modulation, we follow the approach developed by Denys et al. in [9], where the problem is formulated as a semidefinite program (SDP). In that work, a symmetrization procedure is applied that effectively Gaussianizes the state [11], removing the underlying structure tied to modulation along a specific direction in phase space. This enables the use of standard Gaussian techniques by leveraging the extremality property of Gaussian states [12, 13] for the security analysis, but no longer accurately captures the directional asymmetries inherent to the original protocol, and used in practical implementations.

The covariance matrix after this symmetrization takes the form:

$$\Gamma = \begin{pmatrix} X & Z\sigma_z \\ Z\sigma_z & Y \end{pmatrix},$$

where σ_Z is the Pauli Z matrix. This symmetrization procedure effectively extends the modulation to both quadratures of phase space. Although Alice initially prepares coherent states $|\alpha\rangle$ or $|-\alpha\rangle$ modulated solely along the x-quadrature, applying this symmetrization, which includes averaging over discrete phase-space reflections or rotations, requires operations that involve both x and p. In particular, implementing random phase rotations implies the ability to generate states with support in bothquadratures, even if the original modulation is strictly one-dimensional.

As a result, the symmetrized version of the protocol is no longer strictly 1D and is more accurately described as a two-dimensional modulation with Gaussian-like characteristics. While this allows the security analysis to leverage the optimality of Gaussian attacks, it should be noted that the original structure of the protocol is fundamentally altered by the symmetrization.

On the other hand, if we disregard the symmetrization process, the covariance matrix of the 1D BPSK protocol, derived from an appropriate choice of purification that respects the intrinsic symmetries of the protocol, takes the form:

$$\gamma = \begin{pmatrix} X & Z \\ Z & X \end{pmatrix},$$

where and $Z = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}$, with $V = \langle x_A^2 \rangle = \langle x_B^2 \rangle$, $z_1 = \langle x_A x_B \rangle$ and $z_2 = \langle p_A p_B \rangle$.

This structure already closely resembles the covariance matrix of the Gaussian case with modulation along a single quadrature, as described by Usenko and Grosshans in [7]. Therefore, the claim that symmetrization is required to "Gaussianize" the state appears to be unjustified in this setting, where modulation is confined to a specific phase-space direction.

Even without explicitly selecting an optimal purification, one can obtain this covariance matrix structure by applying a minimal symmetrization procedure. In particular, exploiting only the natural symmetry of the BPSK constellation, namely, invariance under a π-rotation in phase space, is sufficient. This discrete symmetry effectively enforces the necessary structure in the covariance matrix, aligning it with the one used in Gaussian-based analyses, without requiring access to both quadratures or full phase-space symmetrization.

2.1. Purification

Following the widely studied purification construction described by Denys et al. and Ghorai et al. in [9] and [10], respectively, we consider any mixed state $\tau = \sum_k p_k |\alpha_k\rangle\langle\alpha_k|$, where each $|\alpha_k\rangle$ is a coherent state, and construct a purification $|\Phi\rangle$ in the standard way for an equivalent entanglement-based protocol:

$$|\Phi\rangle = (I \otimes \tau^{1/2}) \sum_n |n\rangle|n\rangle.$$

Let $\tau = \sum_k \lambda_k |\varphi_k\rangle\langle\varphi_k|$ be its spectral decomposition, then:

$$|\Phi\rangle = \sum_k \sqrt{\lambda_k}\, |\bar{\varphi}_k\rangle\, |\varphi_k\rangle$$

Now define the states:

$$|\psi_k\rangle = \sqrt{p_k}\, \bar{\tau}^{-1/2}\, |\alpha_k\rangle$$

when $|\alpha_k\rangle = |\alpha\rangle$ or $|-\alpha\rangle$ for k=0 or 1, respectively. Then:

$$|\Phi\rangle = \sum_k \sqrt{p_k}\, |\psi_k\rangle\, |\alpha_k\rangle$$

is a valid purification of τ.

Interpretation: The states $|\psi_k\rangle$ define the projective measurement Alice must perform on her half of the entangled state $|\Phi\rangle$ in the entanglement-based protocol to recover the PM scheme. If Alice measures and obtains outcome k, the second mode collapses to $|\alpha_k\rangle$, which is sent to Bob.

This purification structure is essential for analyzing the security of continuous-variable QKD protocols with discrete modulation.

In particular, for unidimensional modulation, this construction has the remarkable property that the reduced state on Alice's side is also τ, meaning that both parties share maximal correlations in the modulated quadrature. This is analogous to the bidimensional case, where the reduced state on Alice's side becomes $\bar{\tau}$.

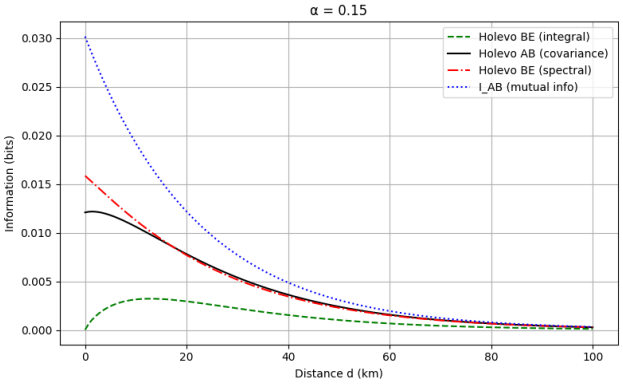
2.2. Numerical results

We investigate the hypothesis that the symmetrization procedure, as proposed in prior works, does not provide a reliable method for approximating a valid lower bound on the secret key rate in the 1D BPSK protocol. This analysis is conducted in the context of a pure-loss channel, which models optical attenuation without added thermal noise, representing one of the most fundamental and idealized Gaussian channels in continuous-variable quantum communication. In this setting, the optimal Gaussian attack by an eavesdropper corresponds to a wiretap, or equivalently, an entangling cloner with vacuum input, where Eve collects the reflected mode from a beam splitter interaction. This attack captures all losses and defines the purification structure relevant for security analysis.

As illustrated in Figure 1, the symmetrization process does not offer any advantage in estimating Eve's information. For BPSK modulation, the inherent non-Gaussianity of the signal places fundamental limits on how well one can force Gaussianity in the global state. This, in turn, constrains the effectiveness of Gaussian-based estimations such as those derived from symmetrized purifications. In contrast, the covariance matrix approach applied directly to a natural purification, without enforcing artificial symmetries, closely reproduces the numerically computed Holevo bound.

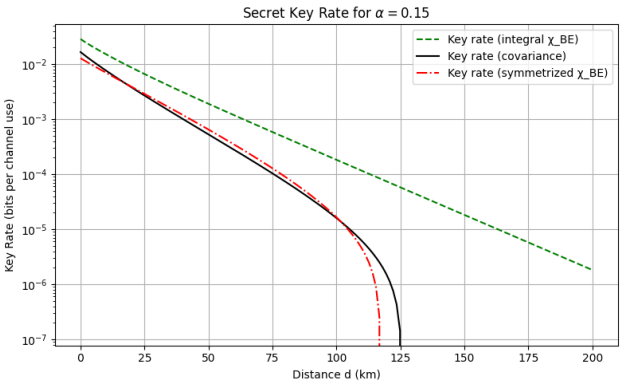
In Figure 2, we observe that accurate and secure key rates can be obtained without symmetrization, using standard Gaussian techniques applied directly to the non-symmetrized covariance matrix. Surprisingly, this approach even yields higher secure communication distances, further demonstrating that enforcing Gaussianity via symmetrization is not necessary for BPSK-based protocols and may in fact be suboptimal.

Figure 1. Comparison of mutual information $I(A;B)$ and Holevo quantities $\chi(B;E)$ for BPSK modulation with amplitude $\alpha = 0.15$, plotted against transmission distance.



The dotted blue curve shows the mutual information between Alice and Bob. The dashed green curve corresponds to the numerically computed Holevo information (integral method), serving as a reference. The solid black curve shows the Holevo quantity estimated from the covariance matrix without symmetrization. The dashed red curve represents the Holevo information estimated from the symmetrized purification (spectral method). Results highlight that symmetrization overestimates Eve's information, while the covariance-based approach closely matches the actual value.

Figure 2. Secret key rate $K = \beta I(A;B) - \chi(B;E)$ as a function of distance for BPSK modulation with $\alpha = 0.15$.



The dashed green line shows the key rate using the Holevo quantity $\chi(B;E)$ computed via the numerical integration method (considered the most accurate). The solid black curve corresponds to the covariance matrix approach without symmetrization, while the red dash-dot curve uses the symmetrized version of the protocol. The reconciliation efficiency is set to β=0.95.

3. Conclusion and outlook

As we have seen in the BPSK scenario, standard security analysis techniques based on symmetrization may not provide optimal results. The inherent non-Gaussianity of the modulated state limits the effectiveness of Gaussian approximations, and the symmetrization procedure, which artificially transforms the protocol into a more symmetric, Gaussian-like version, does not offer a clear advantage in this unidimensional setting for shorter distances.

It is possible that similar limitations apply to other unidimensional discrete modulation schemes beyond BPSK. These findings suggest that relying on symmetrized versions of the protocol may not be appropriate for accurately estimating key rates in such scenarios.

A natural next step would be to develop a security proof against arbitrary Gaussian attacks that does not depend on symmetrization, but instead leverages the actual structure of the unidimensional protocol.

Later on, it may be possible to introduce corrections to the Gaussian-based results in order to better match the true Holevo quantity. Such corrections could be understood as capturing the effect of the residual non-Gaussianity in the shared state between Alice and Bob, thus bridging the gap between Gaussian approximations and the exact non-Gaussian behavior of the protocol.

Acknowledgement

The authors acknowledge support from the project "Comparative Analysis of PM Protocols for Quantum Cryptography", funded 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, under grant number 053/2023, signed with EMBRAPII.

References

[1] Grosshans F, Acín A, Cerf NJ. Continuous-variable quantum key distribution. In: Quantum Information with Continuous Variables of Atoms and Light. Singapore: World Scientific; 2007. p. 63–83. doi:10.1142/9781860948169_0004.
[2] Laudenbach F, Pacher C, Fung CHF, Poppe A, Peev M, Schrenk B, et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. Adv Quantum Technol. 2018;1(1):1800011. doi:10.1002/qute.201800011.
[3] Usenko VC, Acín A, Alléaume R, Andersen UL, Diamanti E, Gehring T, Hajomer AAE, Kanitschar F, Pacher C, Pirandola S, Pruneri V. Continuous-variable quantum communication [Preprint]. arXiv:2501.12801 [quant-ph]. 2025. Available from: https://arxiv.org/abs/2501.12801
[4] Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proc R Soc A. 2005;461(2053):207–235. doi:10.1098/rspa.2004.1372.
[5] Holevo AS. Bounds for the quantity of information transmitted by a quantum communication channel. Probl Inf Transm. 1973;9(3):177–183.
[6] Zhao YB, Heid M, Rigas J, Lütkenhaus N. Asymptotic security of binary modulated continuous-variable quantum key distribution. Phys Rev A. 2009;79(1):012307. doi:10.1103/PhysRevA.79.012307.
[7] Usenko VC, Grosshans F. Unidimensional continuous-variable quantum key distribution. Phys Rev A. 2015;92(6):062337. doi:10.1103/PhysRevA.92.062337.
[8] Serafini A, Illuminati F, De Siena S. Symplectic invariants, entropic measures and correlations of Gaussian states. J Phys B At Mol Opt Phys. 2004;37(2):L21–L28. doi:10.1088/0953-4075/37/2/L02
[9] Denys A, Brown P, Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum. 2021;5:540. doi:10.22331/q-2021-09-13-540.
[10] Ghorai S, Grangier P, Diamanti E, Leverrier A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys Rev X. 2019;9(2):021059. doi:10.1103/PhysRevX.9.021059.
[11] Leverrier A. Symmetrization technique for continuous-variable quantum key distribution. Phys Rev A. 2012;85(2):022339. doi:10.1103/PhysRevA.85.022339.
[12] García-Patrón R, Cerf NJ. Unconditional optimality of Gaussian attacks against continuous-variable quantum key

distribution. Phys Rev Lett. 2006;97(19):190503. doi:10.1103/PhysRevLett.97.190503.
[13] Navascués M, Grosshans F, Acín A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys Rev Lett. 2006;97(19):190502. doi:10.1103/PhysRevLett.97.190502.
[14] Lo HK, Chau HF, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security. J Cryptol. 2005;18(2):133–165. doi:10.1007/s00145-004-0142-y.
[15] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. Nature. 2003;421(6920):238–241. doi:10.1038/nature01289.