Finite-size effects in continuous-variable quantum key distribution

Lucas Q. Galvão [*,1] **and Nelson Alves Ferreira Neto** [1]

[1] *QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845, 41650-010, Salvador, BA, Brazil*

[*] *Corresponding author: lucas.queiroz@fbter.org.br*

Abstract: In this work, we derive all finite-size corrections required to ensure the composable security of continuous-variable quantum key distribution (CV-QKD) protocols under collective Gaussian attacks. Unlike asymptotic analyses that assume infinite data, our approach accounts for realistic constraints imposed by finite sample sizes—crucial for practical implementations. We systematically examine how each postprocessing step contributes to the final security guarantees in terms of both correctness and secrecy. Particular attention is given to the statistical limitations of conventional estimation techniques in the finite-key regime. We analyze how inaccuracies in parameter estimation can compromise security and identify the conditions under which secure key generation remains viable. Our results help bridge the gap between theoretical security proofs and operational CV-QKD systems, supporting the development of reliable quantum communication technologies.

Keywords: Continuous-Variable Quantum Key Distribution. Finite-size effects. Composable security.

Abbreviations: CV-QKD, Continuous-Variable Quantum Key Distribution. MLE, Maximum Likelihood Estimation

1. Introduction

Security in communication is a fundamental pillar of contemporary society, as it enables the exchange of information without the risk of potential leaks [1]. However, recent algorithmic developments pose a threat to this security, particularly quantum algorithms capable of factoring integers in logarithmic time [2]. In light of these challenges, research in quantum communication has sought to exploit the intrinsic properties of quantum physics to enable unconditionally secure communication [3, 4]. Within this framework, continuous-variable quantum key distribution (CV-QKD) has emerged as a promising approach [5], due to its greater compatibility with current components used in coherent optical telecommunication systems [6, 7, 8].

In general, the proofs often rely on theoretical models of CV-QKD protocols that assume an infinite number of shared signals. However, postprocessing data is mainly based on statistical methods [9]. In principle, the statistical law of large numbers guarantees that the postprocessing results hold in the asymptomatic scenario [10], but this assumption is obviously impossible to achieve in practical implementations, such that one must consider *finite-size correlations* [11, 12] in order to ensure genuine *composable security* [13].

In this work, we derive all the essential finite-size corrections for the security assurance against collective Gaussian attacks. Thus, we discussed the effect of postprocessing procedures in correctness, secrecy and parameter estimation of the protocol in order to discuss more realistic CV-QKD deployments.

2. Continuous-variable quantum key distribution

In a typical CV-QKD protocol, quantum information can be encoded onto coherent states by modulating the amplitude and phase quadratures of laser light, typically using electro-optic modulators at the transmitter [6, 7]. This modulation enables the establishment of a secret-key between two legitimate QKD users (Alice and Bob). The modulated coherent states are then transmitted through a quantum channel, which is assumed to be entirely controlled by a potential eavesdropper (Eve) [14].

The security of CV-QKD protocols employing Gaussian-modulated coherent states was initially proven in the asymptotic regime [15, 16], and subsequently extended to the finite-size scenario, guaranteeing universal composability against both collective [17] and general coherent attacks [18]. Eve's optimal attack, accounting for finite-size effects, has been demonstrated to be a Gaussian attack [15]. Consequently, the collective state shared between Alice and Bob can be assumed to be Gaussian. In the entanglement-based picture [19], this state is fully characterized by its covariance matrix

$$\Gamma = \begin{pmatrix} (V_A+1)\mathbb{I}_2 & tZ\sigma_z \\ tZ\sigma_z & (t^2V_A+\sigma^2)\mathbb{I}_2 \end{pmatrix}, \tag{1}$$

where σ_z is the Pauli matrix and $Z = \sqrt{V_A^2+2V_A}$ for Gaussian modulation [6].

A widely adopted method to quantifies the average number of secure bits that Alice and Bob can distill per signal, after accounting for any information that may have been gained by a potential eavesdropper (Eve), is the Devetak–Winter bound [20], expressed as

$$I(x:y) - \sup_{\mathcal{N}:A'\to B} H(y:E) \tag{2}$$

where $I(x:y)$ denotes the mutual information between Alice's and Bob's classical variables x and y [21], while $H(y:E)$ represents the Holevo information between Bob's variable y and the adversary's quantum system E [22] — computed using the simpletic eigenvalues of the covariance matrix. The supremum is taken over all quantum channels $\mathcal{N}: A \to B$ that are consistent with the statistics observed by Alice and Bob during the parameter estimation step.

The measured data $\{y\}_N$ is related to the transmitted signals $\{x\}_N$ by the linear normal model

$$y_i = t\frac{x_i}{\sqrt{\mu}} + z_i \tag{3}$$

where $t = \sqrt{T}$ and z is a random variable related to the noise with variance $\sigma^2 = 1 + t^2\xi$ [17]. Considering that both, Alice and Bob, have access only to the signals x and y, one needs to estimate V_A, t and σ^2, where the latter has a drastic impact for long distances [23].

For operational purposes, we use the Protocol op-

eration 1 to describe the sequence of steps required to implement a CV-QKD scheme under realistic assumptions. In summary, this protocol begins with the quantum signal preparation and transmission, followed by coherent detection at the receiver's end. Subsequently, classical post-processing steps are applied, including sifting, parameter estimation, information reconciliation, and privacy amplification. At the end of the protocol, Alice must have a string S_A and Bob a string S_B, such that $S_A = S_B$ with high probability, and this shared string is secret with respect to any potential eavesdropper. Considering these characteristics, this protocol is characterized as a *prepare and measure* protocol [6].

Protocol operation 1 — *Prepare and Measure*

1. ***State preparation:*** *Alice modulates coherent states by applying a Gaussian modulation to both quadratures, independently drawn from a centered normal distribution with variance V_A, and sends them through the quantum channel to Bob.*
2. ***State measurement:*** *Bob performs heterodyne detection on each incoming state, simultaneously measuring both quadratures.*
3. ***Information reconciliation:*** *Bob sends classical information to Alice over an authenticated public channel in order to correct her data. A forward error correction code is used, where Bob's data serves as the reference.*
4. ***Parameter estimation:*** *Alice uses a randomly selected subset of the correlated data to estimate channel parameters ensuring they fall within acceptable thresholds for security.*
5. ***Privacy amplification:*** *Alice and Bob apply a privacy amplification protocol to distill a shared secret key, reducing any partial information potentially held by an eavesdropper to a negligible level, thus ensuring composable security.*

3. Finite-size effects

Finite-size effects have a significant impact on the security of CV-QKD protocols, as they introduce statistical fluctuations that must be carefully accounted [12]. In practical implementations, only a finite number of signals can be exchanged, which limits the precision with which parameters can be estimated. As a result, incorporating finite-size effects is essential for achieving composable security, where the generated key can be securely used in subsequent cryptographic tasks even in the presence of an adversary with unbounded quantum capabilities [17, 11].

A protocol is said to be *secure* if it is both *correct* and *secret* [24]. The correctness means that the final keys generated by Alice and Bob must be perfectly identical ($S_A = S_B$). Also, the protocol must ensure *secrecy*, requiring that Alice's key

S_A follows a uniform probability distribution and remains completely independent of any quantum system E controlled by an eavesdropper.

For a protocol to be considered ideal, it must simultaneously satisfy a third fundamental criteria. The protocol should demonstrate *robustness*, which means it will never terminate prematurely in the absence of any eavesdropping activity, continuing to function properly when the communication channel is undisturbed [18]. Here, we are interested only in security of the protocol, so we assume a perfect robustness protocol without any aborting probability.

3.1. Correctness

To ensure the correctness of the protocol, the measured data must allow for efficient information reconciliation, such that $S_A = S_B$ [24]. This procedure takes place immediately after the state measurement step, where Bob obtains a classical outcome from the received quantum states. A key parameter used to quantify how much information can be recovered during reconciliation is the reconciliation efficiency $\beta \in [0,1]$, where $\beta = 1$ corresponds to a perfectly efficient reconciliation scheme.

Furthermore, one must ensure that error correction succeeds with probability p_{ec}, or equivalently fails with probability $\text{FER} = 1 - p_{\text{ec}}$, known as the *frame error rate* [6]. The value of p_{ec} depends on several factors, including the signal-to-noise ratio, the target reconciliation efficiency β, and the ϵ-correctness parameter ϵ_{cor}, which bounds the probability that Alice's and Bob's strings differ after error correction and successful verification of their hashes [11]. In particular, a protocol it is called $\epsilon_{\text{cor}}-$correct if $\Pr[S_A \neq S_B] \leq \epsilon_{\text{cor}}$.

Considering this aspects, the finite-size correlation related to the correctness are given by

$$k^{\epsilon_{\text{cor}}} = p_{\text{EC}}(\beta I(x:y) - H(y:E)). \tag{4}$$

3.2. Secrecy

The finite number of exchanged quantum signals introduces statistical uncertainty in the estimation of Eve's information and affects the secrecy of the final key. To ensure security even in this finite-size regime, a correction term $\Delta(n)$ that depends on the probability of failure of the secrecy ϵ_{sec} procedure is introduced in the key-rate expression [12]. This term accounts for the deviation between the estimated and actual amount of information potentially leaked to an eavesdropper, written as

$$\Delta(n) \equiv (2\dim\mathcal{H}_x + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2\left(\frac{1}{\epsilon_{\text{PA}}}\right), \tag{5}$$

where $\mathcal{H}_x$ is the Hilbert space associated with the raw key variable x and $\epsilon_{\text{sec}} = \epsilon_{\text{PA}} + \bar{\epsilon}$, with $\bar{\epsilon}$ being a smoothing parameter and ϵ_{PA} the failure proba-

bility of the privacy amplification step [11]. Both parameters are chosen to ensure composable security and must be numerically optimized in order to obtain a key ϵ_{sec}-indistinguishable from Eve's measurement.

The first term in $\Delta(n)$ captures the statistical fluctuation in the estimation of Eve's knowledge and quantifies how the smooth min-entropy approaches the von Neumann entropy as n increases [17]. The second term reflects the impact of the privacy amplification procedure, ensuring that the compression of the raw key is sufficient to eliminate any residual information available to an eavesdropper [11].

As a result, the secret key rate in the finite-size scenario becomes:

$$k^{\epsilon_{\text{cor}}+\epsilon_{\text{sec}}} = p_{\text{EC}}\left[\beta I(x:y) - H(y:E) - \Delta(n)\right]. \quad (6)$$

3.3. Parameter estimation

In CV-QKD, parameter estimation plays a central role in ensuring the security of the protocol. Unlike the asymptotic regime, where the law of large numbers guarantees convergence of estimators to true values, finite-size implementations require careful statistical treatment. In particular, the uncertainty in estimating t and σ^2 limits the achievable secret key rate, as underestimating Eve's information can compromise security [17].

The maximum likelihood estimation (MLE) method provides estimators for t and σ^2 in a linear model:

$$\hat{t} = \sum_{i=1}^{m} \frac{y_i x_i}{x_i^2}, \quad \hat{\sigma}^2 = \sum_{i=1}^{m} \frac{(y_i - \hat{t}x_i)^2}{m}. \quad (7)$$

and confidence intervals are derived by defining conservative bounds:

$$t_{\text{min}} \approx \hat{t} - z_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}^2}{mV_A}}, \quad (8)$$

$$\sigma^2_{\text{max}} \approx \hat{\sigma}^2 + z_{\epsilon_{PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \quad (9)$$

where $z_{\epsilon_{PE}/2} = \text{erf}^{-1}(1-\epsilon_{PE}/2)$, with erf() being the error function [25].

These bounds ensure that, except with probability $\epsilon_{PE}/2$, the true values of t and σ^2 lie within the estimated intervals. Incorporating these estimates, the worst-case covariance matrix becomes

$$\Gamma_{\epsilon_{PE}} = \begin{pmatrix} (V_A+1)\mathbb{I}_2 & t_{\text{min}} Z\sigma_z \\ t_{\text{min}} Z\sigma_z & (t^2_{\text{min}} V_A + \sigma^2_{\text{max}})\mathbb{I}_2 \end{pmatrix}, \quad (10)$$

which defines a confidence region with security parameter ϵ_{PE}. This approach ensures composable security under collective attacks in finite-size implementations. Finally,

$$k_\epsilon = \frac{n p_{\text{EC}}}{N}(\beta I(x:y) - H_{\epsilon_{\text{PE}}}(x:E) - \Delta(n)) \quad (11)$$

where $\epsilon = p_{\text{EC}}\epsilon_{\text{PE}} + \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$, which means that one must ensure that the key is secure against any

eavesdropper attack, up to a probability of failure ϵ [26].

4. Numerical investigations

In this section, we investigate the impact of the finite-size scenario on the secret key rate of the CV-QKD protocol. For this purpose, we consider the protocol described in Protocol Operation 1, with heterodyne detection and reverse reconciliation. The protocol parameters used in the simulations are presented in Tab. 1, based on experimental implementations reported in the literature [7, 27, 28, 29, 12].

Table 1: Protocol parameters used in numerical investigations.

Protocol parameter	Symbol	Value
Hilbert space dimension	$\dim\mathcal{H}_x$	2 (bin.)
Quantum duty	μ	2 (het.)
Detector efficiency	η_{eff}	0.8
Excess noise	ξ	0.01 SNU
Modulation variance	V_A	5 SNU
Fraction of raw key	n/N	0.5
Reconciliation efficiency	β	0.95
Success probability of EC	p_{EC}	0.9

To compute the asymptotic secret key rate, we use Eq. (2), which assumes infinite statistics. For the finite-size analysis, we apply Eq. (11), which incorporates the statistical uncertainty through the penalty term $\Delta(n)$ as well as the confidence intervals for the estimated parameters $t_{\min}$ and $\sigma^2_{\max}$ obtained via MLE. Here, we adopt $\epsilon_{PE} = \epsilon_{\text{cor}} = \bar{\epsilon} = \epsilon_{PA} = 10^{-10}$ for the security parameters, yielding an overall composable security level of $\epsilon \approx 3.9 \cdot 10^{-10}$ against collective Gaussian attacks

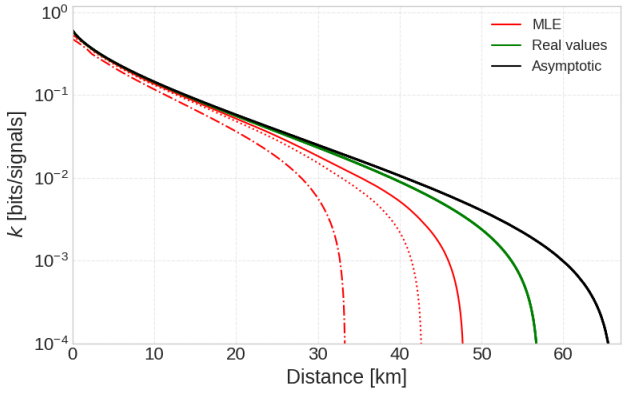

Figure 1: Secret-key rate using the discussed protocol with parameters from Table 1. The black solid line represents the asymptotic limit, the green line uses the real values of the channel with $N = 2 \cdot 10^8$, and the red lines correspond to the MLE-based estimation for $N = 2 \cdot 10^6$ (dot-dashed), $2 \cdot 10^7$ (dotted), and $2 \cdot 10^8$ (solid) signals. In all finite-size cases, the estimated key rate remains below the ideal case, ensuring security.

The results in Fig. 1 clearly show the severe impact of parameter estimation in finite-size scenarios. While the asymptotic and real-value curves extend to over 60 km, the MLE-based estimation leads to a significant reduction in achievable distance. This is especially evident for small block sizes ($N = 2 \cdot 10^6$), where the uncertainty in estimating transmittance and excess noise leads to a rapid drop in the secret key rate. As the block size increases, the estimated values converge toward the real values, and the secret key rate approaches the ideal scenario. These results highlight the importance of precise statistical estimation and the need for large data blocks to ensure secure key distribution in practical implementations.

5. Perspectives and conclusion remarks

Future improvements in CV-QKD protocols will likely focus on enhancing both error correction and privacy amplification in the finite-size regime. Optimizing reconciliation efficiency while minimizing leakage during information reconciliation remains a critical challenge, especially at low SNRs [28]. On the secrecy side, tighter finite-size bounds and improved estimations of the smooth min-entropy can increase the secret-key rate and reduce the block length required for secure key generation.

Parameter estimation is another key area for development, particularly in regimes with short block lengths and limited resources. Advanced techniques, including machine learning and adaptive estimators, may offer more accurate characterizations of the quantum channel and noise parameters. Recently, Galvão *et. al* (2025) have proven security against collective attacks for parameter estimation using neural networks [30]. This could lead to more accurate confidence intervals, and better key rate optimization.

In conclusion, the security of CV-QKD protocols in practical scenarios relies heavily on robust finite-size analysis, especially in the composable framework. As protocols move from laboratory demonstrations to real-world deployment, addressing these limitations through improved statistical methods, numerical optimization, and efficient implementation of classical post-processing will be essential for achieving reliable and scalable quantum communication networks.

Acknowledgement

This work was fully funded by the project *HW DSP: Development and Prototyping of Multicore SoC with Dedicated Accelerators and RISC-V DSP*, supported by QuIIN – Quantum Industrial Innovation, the EMBRAPII CIMATEC Competence Center in Quantum Technologies. Financial resources were provided by the PPI IoT/Industry 4.0 program of the Brazilian Ministry of Science, Technology and Innovation (MCTI), under grant number 053/2023, in partnership with EMBRAPII.

References

[1] United Nations. United nations global principles for information integrity, 2024. Accessed: 2025-07-12.

[2] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[3] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, 2006.

[4] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[5] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[6] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[7] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu,

and Hong Guo. Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1):011318, 03 2024.

[8] Vladyslav C. Usenko, Antonio Acín, Romain Alléaume, Ulrik L. Andersen, Eleni Diamanti, Tobias Gehring, Adnan A. E. Hajomer, Florian Kanitschar, Christoph Pacher, Stefano Pirandola, and Valerio Pruneri. Continuous-variable quantum communication, 2025.

[9] Yi Luo, Xi Cheng, Hao-Kun Mao, and Qiong Li. An overview of postprocessing in quantum key distribution. *Mathematics*, 12(14), 2024.

[10] George Casella and Roger Berger. *Statistical inference*. CRC press, 2024.

[11] Stefano Pirandola. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.*, 3:043014, Oct 2021.

[12] Nitin Jain, Hou-Man Chin, Hossein Mani, Cosmo Lupo, Dino Solar Nikolic, Arne Kordts, Stefano Pirandola, Thomas Brochmann Pedersen, Matthias Kolb, Bernhard Ömer, Christoph Pacher, Tobias Gehring, and Ulrik L. Andersen. Practical continuous-variable quantum key distribution with composable security. *Nature Communications*, 13(1):4740, Aug 2022.

[13] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2001.

[14] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01):1–127, 2008.

[15] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[16] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006.

[17] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[18] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109:100502, Sep 2012.

[19] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7):535–552, October 2003.

[20] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[21] Thomas M Cover. *Elements of information theory*. John Wiley & Sons, 1999.

[22] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[23] Duan Huang, Peng Huang, Dakai Lin, and Guihua Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6(1):19201, Jan 2016.

[24] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1):634, Jan 2012.

[25] A. Monfort. *Cours de statistique mathématique*. Collection "Economie et statistiques avancées". Economica, 1982.

[26] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[27] Qiming Lu, Qi Shen, Yuan Cao, Shengkai Liao, and Chengzhi Peng. Ultra-low-noise balanced detectors for optical time-domain measurements. *IEEE Transactions on Nuclear Science*, 66(7):1048–1055, 2019.

[28] Mario Milicevic, Chen Feng, Lei M. Zhang, and P. Glenn Gulak. Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography. *npj Quantum Information*, 4(1):21, Apr 2018.

[29] Hou-Man Chin, Nitin Jain, Darko Zibar, Ulrik L. Andersen, and Tobias Gehring. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):20, Feb 2021.

[30] Lucas Q. Galvão, Davi Juvêncio G. de Sousa, Micael Andrade Dias, and Nelson Alves Ferreira Neto. Neural network for excess noise estimation in continuous-variable quantum key distribution under composable finite-size security. *arXiv:2507.23117 [quant-ph]*, 2025.