Modulação Gaussiana versus PCS-64-QAM em CV-QKD: Demanda por Bits Aleatórios e Desempenho em SKR

Caroline S. M. Alves[1,2], **Nelson A. F. Neto**[1], **Paulo C. M. A. Farias**[2], **Wagner L. A. de Oliveira**[2]

[1]QuIIN – Quantum Industrial Innovation, Centro de Competências EMBRAPII CIMATEC em Tecnologias Quânticas – Salvador, BA – Brazil

[2]Programa de Pós-Graduação em Engenharias Elétrica e de Computação – PPGEEC, Escola Politécnica, Universidade Federal da Bahia (UFBA) – Salvador, BA – Brasil.

caroline.morais@fieb.org.br,nelson.neto@fieb.org.br,

paulo.farias@ufba.br,oliveira.wagner@ufba.br

Abstract. *This work investigates the impact of the modulation scheme on QRNG randomness consumption and SKR performance in CV-QKD systems with heterodyne detection. Gaussian modulation, implemented via the Box–Muller transform, requires a precision of $L \approx 17$ bits per quadrature to reach the Gaussian regime, resulting in a consumption of approximately 34 bits per complex symbol. In contrast, discrete modulation with PCS, based on CCDM with block lengths of $N \approx 10^4$, enables the approximation of Gaussian distributions at a lower cost. The results show that PCS 64-QAM achieves performance close to Gaussian modulation, with a transmission distance exceeding 300 km and a consumption of approximately 4.9 bits per symbol.*

Resumo. *Este trabalho investiga o impacto do esquema de modulação na demanda por aleatoriedade do QRNG e no desempenho de SKR em sistemas CV-QKD com detecção heteródina. A modulação gaussiana, implementada via transformada de Box–Muller, requer precisão de $L \approx 17$ bits por quadratura para atingir o regime gaussiano, resultando em consumo de aproximadamente 34 bits por símbolo complexo. Em contraste, a modulação discreta com PCS, baseada em CCDM com blocos de $N \approx 10^4$, permite aproximar distribuições gaussianas com menor custo. Os resultados mostram que a PCS 64-QAM alcança desempenho próximo à modulação gaussiana, com alcance superior a 300 km e consumo de aproximadamente $4{,}9$ bits/símbolo.*

1. Introdução

A distribuição quântica de chaves (*Quantum Key Distribution* – QKD) é uma área da criptografia quântica que possibilita a duas partes legítimas (Alice e Bob) estabelecer uma chave secreta compartilhada por meio de um canal quântico inseguro e um canal clássico autenticado [Bennett and Brassard 1984]. No protocolo QKD do tipo *Prepare-and-Measure* (P&M), Alice codifica a informação clássica em estados quânticos não ortogonais e, em seguida, transmite a Bob por meio de um canal quântico. Nesse cenário,

a segurança da QKD é garantida teoricamente pelas leis da mecânica quântica e independem da capacidade computacional de um adversário.

Em relação à forma de detecção, os protocolos P&M podem ser categorizados em protocolos de variáveis discretas (DV) e de variáveis contínuas (CV). Em CV-QKD, a informação é codificada nas amplitudes de quadratura do campo eletromagnético, possibilitando o uso de detectores homódinos ou heteródinos amplamente implantados em comunicações ópticas clássicas [Pirandola et al. 2020]. Em contraste, os protocolos DV requerem detecção de fótons únicos e frequentemente necessitam de resfriamento criogênico [Pirandola et al. 2020].

Em CV-QKD, a modulação gaussiana permite provas de segurança rigorosas [Leverrier 2017], mas é pouco prática devido às limitações físicas dos moduladores, à elevada demanda sobre o QRNG (*Quantum Random Number Generator*) e ao alto custo computacional da reconciliação em regimes de baixa relação sinal-ruído (*Signal-to-Noise Ratio* – SNR) [Zhang et al. 2024]. Protocolos com modulação discreta reduzem essas exigências ao empregar constelações finitas de estados coerentes, permitindo o uso de técnicas clássicas eficientes de correção de erros [Leverrier and Grangier 2009], com provas de segurança já estabelecidas para o regime assintótico [Kaur et al. 2021, Denys et al. 2021]. Nesse contexto, a formatação probabilística de constelações (*Probabilistic Constellation Shaping* – PCS) surge como estratégia para aproximar a distribuição discreta de uma gaussiana, conciliando a praticidade da modulação discreta com o desempenho da modulação gaussiana [Roumestan et al. 2024].

Este trabalho compara modulações gaussiana, discreta uniforme e PCS-QAM em sistemas CV-QKD, considerando a demanda de bits aleatórios de QRNG e o desempenho da taxa de chave secreta (*Secret Key Rate* – SKR). Para isso, são realizadas simulações numéricas que avaliam: (i) o consumo de aleatoriedade na modulação gaussiana gerada via transformada de Box–Muller em função da precisão de amostragem; (ii) a convergência estatística do *Constant Composition Distribution Matching* (CCDM) [Schulte and Böcherer 2016] na geração de símbolos para PCS 64-QAM em função do tamanho de bloco; e (iii) o desempenho de SKR para constelações PCS-QAM com otimização conjunta dos parâmetros de modulação. Todos os experimentos assumem canal ideal e não envolvem implementações experimentais. O artigo está organizado da seguinte forma: a Seção 2 apresenta os fundamentos; a Seção 3 descreve a metodologia; a Seção 4 apresenta os resultados; e a Seção 5 conclui o trabalho.

2. Fundamentação Teórica

2.1. Modulação Gaussiana

Na modulação gaussiana, as quadraturas q e p são amostradas independentemente de uma distribuição normal $\mathcal{N}(0, \tilde{V}_m)$. Em implementações práticas, são geradas a partir de variáveis uniformes $U_1, U_2 \sim \mathcal{U}(0, 1)$ via transformada de Box–Muller:

$$q = \sqrt{-2 \ln U_1} \cos(2\pi U_2), \tag{1}$$

$$p = \sqrt{-2 \ln U_1} \sin(2\pi U_2). \tag{2}$$

Esse processo impõe elevada demanda sobre o QRNG, que fornece sequências uniformes a serem continuamente transformadas, constituindo um gargalo na geração de ale-

atoriedade [Zhang et al. 2024]. Alternativas como o uso de PRNGs introduzem determinismo e podem comprometer a segurança [Pirandola et al. 2020], enquanto QRNGs com saída gaussiana nativa ainda apresentam taxas insuficientes para aplicações práticas [Huang et al. 2020].

2.2. Modulação Discreta com PCS

Na modulação discreta, os estados coerentes pertencem a uma constelação finita $\{|\alpha_k\rangle\}$, selecionados com probabilidades p_k. Na PCS, p_k segue uma distribuição de Maxwell–Boltzmann:

$$p_k = \frac{1}{Z(\nu)} \exp\left(-\nu|\alpha_k|^2\right), \tag{3}$$

onde $\nu > 0$ controla a potência média e $Z(\nu)$ é o fator de normalização.

Na prática, Alice dispõe de bits uniformes do QRNG e deve mapeá-los em símbolos com distribuição não uniforme p_k, o que requer algoritmos de *distribution matching*. O CCDM é a abordagem de referência, com desempenho assintoticamente ótimo para blocos longos, porém com elevada complexidade computacional [Schulte and Böcherer 2016]. Alternativas mais adequadas para implementações em hardware, como o Hi-DM [Civelli and Secondini 2020], têm sido propostas para reduzir esse custo. A qualidade da aproximação à distribuição alvo é avaliada pela divergência de Kullback–Leibler:

$$D_{\mathrm{KL}}(p\|q) = \sum_k p_k \log \frac{p_k}{q_k}, \tag{4}$$

que decresce com o tamanho do bloco, convergindo no limite assintótico.

3. Metodologia

Considera-se três esquemas de modulação, a saber, gaussiana, QAM uniforme e PCS-QAM, em um sistema CV-QKD com detecção heteródina, reconciliação reversa, atenuação de $0{,}2$ dB/km, ruído de excesso $\xi = 0{,}02$ SNU e eficiência $\beta = 0{,}95$. A modulação gaussiana é gerada via transformada de Box–Muller com precisão $L \in \{4, \ldots, 32\}$ bits por quadratura, consumindo $2L$ bits por símbolo complexo. A qualidade da aproximação gaussiana é avaliada pelo excesso de curtose da distribuição gerada, adotado como métrica principal por refletir desvios de alta ordem em relação ao modelo gaussiano assumido nas provas de segurança.

A modulação discreta utiliza constelações M-QAM com $M \in \{16, 64, 256\}$. Na PCS, os símbolos seguem uma distribuição de Maxwell–Boltzmann parametrizada por ν (3), gerada via CCDM. A qualidade do *distribution matching* é avaliada pela divergência KL em função do tamanho de bloco $N \in \{10^2, 10^3, 10^4, 10^5\}$. A demanda por aleatoriedade é $2(H_{MB} + 1)$ bits por símbolo complexo. A SKR assintótica é calculada conforme [Denys et al. 2021] para modulações discretas e [Weedbrook et al. 2012] para a gaussiana. As probabilidades de Maxwell-Boltzmann são calculadas analiticamente para cada ν e fornecidas diretamente ao modelo, assumindo operação do CCDM no regime assintótico.

4. Resultados e Discussão

A Figura 1 apresenta o excesso de curtose da distribuição gerada pela transformada de Box–Muller em função da precisão L. Para $L = 4$, observa-se curtose negativa

($\approx -0{,}30$), indicando caudas mais leves devido ao truncamento de U_1 com 2^L níveis. A curtose converge para zero para $L \gtrsim 15$, estabilizando-se em $L \approx 16$–17, o que define um limiar de precisão a partir do qual a distribuição gerada se aproxima do regime gaussiano assumido nas provas de segurança [Leverrier 2017]. Esse limiar implica um consumo mínimo de aproximadamente 34 bits por símbolo complexo do QRNG, como indicado na Tabela na Figura 3b. Considerando taxas típicas de sistemas CV-QKD na ordem de centenas de MBaud a GHz [Tian et al. 2023, Pi et al. 2023], essa demanda implica demandas de QRNG na ordem de dezenas de Gbit/s. Esse requisito motiva a investigação de esquemas de modulação discreta com menor demanda de aleatoriedade.

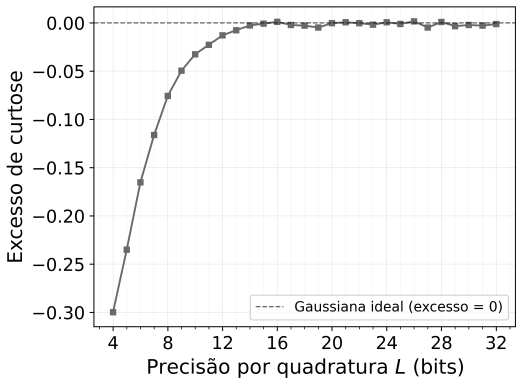


Figura 1. Excesso de curtose da modulação gaussiana gerada via Box–Muller em função da precisão por quadratura L.

A Figura 2a mostra que constelações maiores requerem distribuições mais concentradas e menor variação de ν (3), com valores entre $0{,}143$ e $0{,}200$ (16-QAM), $0{,}053$ e $0{,}069$ (64-QAM) e $0{,}008$ (256-QAM). Os valores de ν obtidos no limite de maior distância, são adotados como referência para o cálculo da demanda de bits/símbolo, da divergência KL e da SKR. A Figura 2b mostra a convergência da divergência KL do CCDM em $N \approx 10^4$, definindo o menor tamanho de bloco que fornece boa aproximação da distribuição alvo com baixa complexidade.

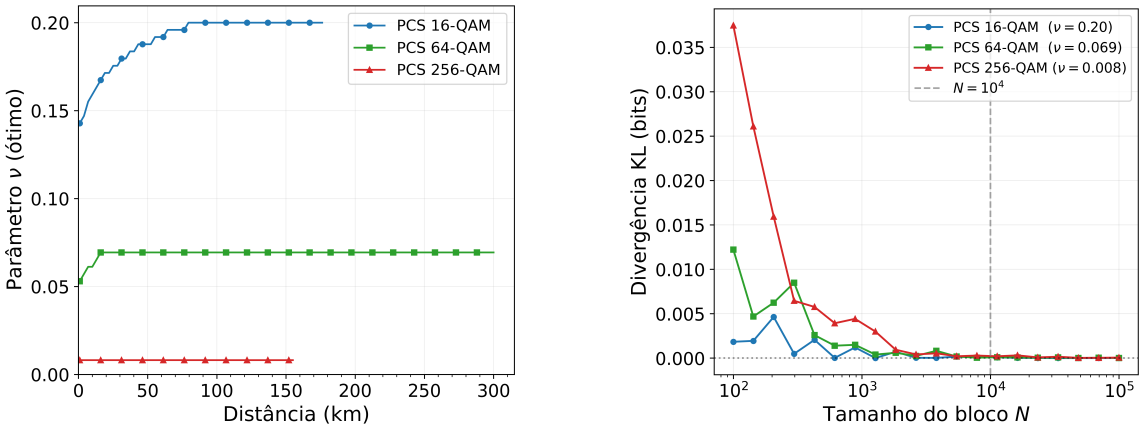
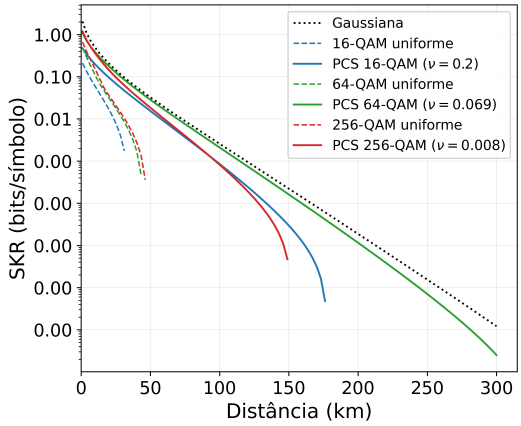


Figura 2. a) Parâmetro de formatação ótimo ν em função da distância; b) Divergência KL do CCDM em função do tamanho de bloco N.

A Figura 3 apresenta a SKR em função da distância para os três esquemas de modulação. A PCS 64-QAM alcança desempenho próximo à referência gaussiana, com

alcance superior a 300 km e consumo de aproximadamente $4{,}91$ bits/símbolo (Figura 3b) do QRNG, enquanto que a modulação gaussiana demanda mais de 34 bits por símbolo complexo. A modulação PCS 16-QAM apresenta alcance de 176 km, demonstrando resultado superior à modulação uniforme 256-QAM que alcança 155 km. Os resultados mostram que PCS-QAM com CCDM em blocos de $N \approx 10^4$ permite obter SKR próxima à modulação gaussiana com redução de até $85{,}6\%$ na demanda por bits do QRNG.



Modulação	**Demanda (bits/símbolo)**
Gaussiana ($L = 17$)	34
16-QAM uniforme	6
64-QAM uniforme	8
256-QAM uniforme	10
PCS 16-QAM	3.31
PCS 64-QAM	4.91
PCS 256-QAM	7.62

Figura 3. a) Análise assintótica de CV-QKD com detecção heteródina ($\xi = 0{,}02$, $\beta = 0{,}95$). b) Tabela com a demanda por bits aleatórios do QRNG por esquema de modulação.

5. Conclusão

Este trabalho analisou o impacto da modulação na demanda por bits aleatórios do QRNG e no desempenho de SKR em CV-QKD com detecção heteródina. Para a modulação gaussiana, a transformada de Box–Muller requer precisão mínima de $L \approx 17$ bits por quadratura para atingir o regime gaussiano, implicando uma demanda por 34 bits/símbolo. Para a modulação discreta com PCS, o CCDM com blocos de $N \approx 10^4$ é suficiente para aproximar a distribuição de Maxwell–Boltzmann.

A PCS 64-QAM apresentou melhor desempenho, com SKR próxima à referência gaussiana, alcance superior a 300 km e consumo de aproximadamente $4{,}91$ bits/símbolo, correspondendo a uma redução de $85{,}6\%$. A PCS 16-QAM supera a PCS 256-QAM em alcance, mostrando que maior cardinalidade não implica ganho de desempenho. Como trabalhos futuros, pretende-se investigar *distribution matching* de menor complexidade, como o Hi-DM, bem como efeitos de tamanho finito e integração com os blocos de processamento em sistemas CV-QKD práticos.

Agradecimentos

Este trabalho foi totalmente financiado pelos projetos: *Análise e Desenvolvimento de algoritmos para Casamento de Distribuição para CV-QKD* e *HW DSP: Desenvolvimento e Prototipagem de SoC Multicore com Aceleradores Dedicados e DSP RISC-V* suportados pelo QuIIN - Quantum Industrial Innovation, Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas, com recursos financeiros oriundos do PPI IoT/Manufatura 4.0 do MCTI, através do Termo de Cooperação 053/2023, firmado com a EMBRAPII.

Referências

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York.

Civelli, S. and Secondini, M. (2020). Hierarchical distribution matching for probabilistic amplitude shaping. *Entropy*, 22(9).

Denys, A., Brown, P., and Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540.

Huang, M., Chen, Z., Zhang, Y., and Guo, H. (2020). A gaussian-distributed quantum random number generator using vacuum shot noise. *Entropy*, 22(6).

Kaur, E., Guha, S., and Wilde, M. M. (2021). Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, 103(1).

Leverrier, A. (2017). Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Phys. Rev. Lett.*, 118:200501.

Leverrier, A. and Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102:180504.

Pi, Y., Wang, H., Pan, Y., Shao, Y., Li, Y., Yang, J., Zhang, Y., Huang, W., and Xu, B. (2023). Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber. *Opt. Lett.*, 48(7):1766–1769.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236.

Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Leverrier, A., Diamanti, E., and Grangier, P. (2024). Shaped constellation continuous variable quantum key distribution: Concepts, methods and experimental validation. *Journal of Lightwave Technology*, 42(15):5182–5189.

Schulte, P. and Böcherer, G. (2016). Constant composition distribution matching. *IEEE Transactions on Information Theory*, 62(1):430–434.

Tian, Y., Zhang, Y., Liu, S., Wang, P., Lu, Z., Wang, X., and Li, Y. (2023). High-performance long-distance discrete-modulation continuous-variable quantum key distribution. *Opt. Lett.*, 48(11):2953–2956.

Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., and Lloyd, S. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621. [Fonte 29].

Zhang, Y., Bian, Y., Li, Z., Yu, S., and Guo, H. (2024). Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1):011318.