Excess Noise Simulation Analysis in a Discrete Modulation CV-QKD System

Christiano M. S. Nascimento[1,*], Maria H. F. Silva[1], Maron F. Anka[1], Braian P. Silva[1], Alexandre B. Tacla[1], Valéria L. da Silva[1]

***Abstract*— As quantum computing advances, communication systems face increasing cyberattack risks, making secure key distribution essential. Continuous-Variable Quantum Key Distribution (CV-QKD) offers unconditional security and compatibility with current optical networks, yet long-distance deployment is challenged by excess noise and the complexity of Gaussian modulation. Here, we analyze secret key rates as a function of distance and photon number using simulated hardware parameters. Results show that 1024-QAM discrete modulation achieves key rates close to Gaussian modulation, and, counterintuitively, longer distances require higher attenuation and lower photon average numbers, highlighting 1024-QAM's potential to improve CV-QKD practicality for metropolitan-scale quantum communication.**

***Keywords*— quantum key distribution, detection noise, security analysis, discrete modulation.**

I. INTRODUCTION

Fiber optic networks carry large amounts of information and are widely deployed in terrestrial, submarine, metropolitan, and access networks [1]. However, recent advances in sophisticated cyber threats and quantum computing algorithms pose a challenge to the security of classical communication systems [2–4]. While quantum computers promise to change the landscape of data processing and problem-solving, they can also make traditional cryptographic protocols vulnerable, threatening the integrity of current network security systems [5]. Risks include the decryption of secure communications, compromise of data privacy [6], and disruption of financial transactions [7].

One possible solution is using quantum key distribution systems due to their security being based on the principles of quantum mechanics rather than computational complexity [8, 9]. This approach enables secure communication between a transmitter (Alice) and a receiver (Bob) via an untrusted channel vulnerable to an eavesdropper (Eve) [10]. Unlike classical encryption methods, quantum cryptography ensures secure communication by considering that all excess noise and attacks are due to the presence of Eve [11].

Several protocols have been implemented over the years [8]. In particular, continuous-variable quantum key distribution (CV-QKD) gained significant attention due to its compatibility with existing optical communication infrastructure and its ability to generate high secret key rates for metropolitan distances [12, 13]. Despite the advanced security proofs for Gaussian modulated (GM) protocols, practical implementations are restricted due to technical limitations, such as complex post-processing [14–16]. However, high-order discrete modulation (DM) can be employed to facilitate the post-processing stage. Security proof for an arbitrary DM has been recently demonstrated by Denys *et al.* [17].

Long-distance transmission is one requirement for the large-scale use and integration of QKD in existing networks. However, a practical long-distance scenario presents obstacles that severely restrict the safe distance, including limited reconciliation efficiency [15] and excessive noise of the optical system [18]. Increasing excessive noise is also related to a lower Signal-to-noise ratio (SNR), which is a key aspect of long-distance implementations [19].

In this work, we present a study of the excess noise for both Gaussian and discrete modulations. The excess noise can be divided by each noise's individual contribution, such as the detection noise and Raman scattering. By combining the models developed by Laudenbach et al. [20] and Denys et al. [17], it is possible to investigate the optimal way to implement a CV-QKD protocol and its maximum secret key rate.

The remainder of this work is organized as follows: Sec. II outlines the methodology, including the modulation scheme, simulated setup, and hardware parameters. Sec. III presents the main findings, systematically testing different QAM modulation constellations under binomial, uniform, and discrete Gaussian distributions for different total excess noise values. It also examines the relationship between secret key rate and average photon number across different transmission distances. Finally, Sec. IV discusses the practical impact of these results for long-distance CV-QKD implementations.

II. METHODOLOGY

A. Noise model

The performance of a CV-QKD system is affected by total noise, composed of the intrinsic shot noise and excess noise ξ due to experimental imperfections and potentially by the influence of an eavesdropper [20]. The components of ξ originate from: state preparation, detection, intensity fluctuations of the lasers used, or modulation, among others [17, 20]. It is assumed that all these noise sources are independent [20] so that their contributions can be added. Fig. 1 illustrates the percentage contribution of each source to the total excess noise of the system.

As shown in Fig. 1, the total simulated excess noise in the system was $\xi_{\text{tot}} = 0.0618$ SNU. Also, the noise sources that

---

[1] QuIIN—Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes, 1845, Salvador, Bahia, 41850-010, Brazil; *christiano.moreira@fbter.org.br (Presenting author)

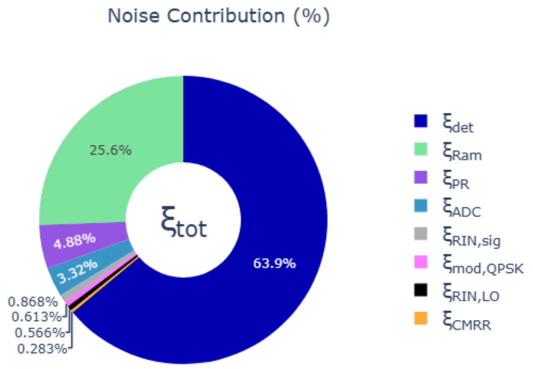

Fig. 1: Decomposition of total excess noise in the simulated CV-QKD system. Each noise component value was calculated using the analytical noise models described in Refs. [17, 20], as well as the respective hardware parameters. The total excess noise measured was $\xi_{tot} = 0.0618$ SNU. ξ_{det}: detection noise, $\xi_{RIN,sig}$: signal laser relative intensity noise (RIN), $\xi_{RIN,LO}$: local oscillator (LO) laser RIN, ξ_{mod}: modulation noise, ξ_{PR}: phase recovery noise, ξ_{Ram}: Raman noise, ξ_{CMRR}: common-mode rejection ratio (CMRR) noise, ξ_{ADC}: analog-to-digital converter (ADC) quantization noise.

contributed more to the total excess noise ξ_{tot} in the simulated CV-QKD system were: detection noise (63.9%), Raman noise (25.6%), phase noise (4.88%), and analog-to-digital converter noise (3.32%). The other noise sources contributed less than 1% each.

In this work, we extend the analysis by simulating multiple scenarios with scaled excess noise values of $\xi_{tot}/2 = 0.0309$ SNU, $\xi_{tot} = 0.0618$ SNU, $2\xi_{tot} = 0.1236$ SNU, and $3\xi_{tot} = 0.1854$ SNU, to evaluate the system performance under increasingly challenging conditions.

B. Modulation

The main approach to GM CV-QKD is based on encoding classical information in the quadrature of coherent states, which follows a Gaussian distribution over the phase space [21]. In this scenario, there are advanced security proofs for several CV-QKD protocols [22].

An alternative is to use DM, based on some discrete alphabet, to create finite-size constellations distributed over the phase space following some probabilistic-shaping distribution [23]. High-order discrete modulation (e.g., 1024-QAM) facilitates practical CV-QKD deployment by streamlining classical post-processing workflows, enhancing practical implementation and efficiency.

Therefore, depending on the probabilistic shaping, QAM modulation may approximate the GM CV-QKD protocol's performance [17]. Among the most commonly used distributions in the literature are the uniform, binomial, and discrete Gaussian distributions. These approximations can directly impact the secret key rate. Fig. 2 illustrates the probability distributions applied to the 1024-QAM modulation states in phase space.

III. RESULTS AND DISCUSSION

A. Modulation Comparison

Based on the analysis shown in Fig. 3, subsequent experiments will consider an average photon number of $\langle n \rangle = 7.5$.

Fig. 4 shows an analysis for excess noise 0.0618 SNU. The longest distance achieved under these conditions is also associated with the 1024-QAM constellation, reaching approximately 81 km for homodyne detection and 71 km for heterodyne detection, with binomial distribution. This measurement is significantly close to the result achieved through Gaussian modulation, corresponding to 82 km.

Next, we present an analysis similar to the above, for excess noise 0.0309 SNU. As shown in Fig. 5, the longest distance achieved under these conditions is also associated with the 1024-QAM constellation, reaching approximately 54 km for homodyne detection and 47 km for heterodyne detection, with binomial distribution. It is notable that this configuration is significantly close to the result achieved through Gaussian modulation, corresponding to 55 km.

Following, we perform the same analysis for excess noise 0.1236 SNU. As shown in Fig. 6, the greatest distance achieved under these conditions is also associated with the 1024-QAM constellation, reaching approximately 27 km for homodyne detection and 28 km for heterodyne detection, with binomial distribution. This setting is significantly close to the result achieved through Gaussian modulation, which is 28 km.

Lastly, we perform the same analysis for excess noise 0.1854 SNU. As shown in Fig. 7, the greatest distance achieved under these conditions is also associated with the 1024-QAM constellation, reaching approximately 13.5 km for homodyne detection and 12 km for heterodyne detection, with binomial distribution. This setting is significantly close to the result achieved through Gaussian modulation, which is 14 km.

In general, the results show that Gaussian modulation offers the highest secret key rates in terms of distance, reflecting its widespread use in the literature. On the other hand, it was evident that the results achieved by 1024-QAM modulation with binomial distribution were significantly close to those exhibited by Gaussian modulation. In this context, discrete modulations represent a viable alternative to implementations due to the methodical way in which their constellations structure the data.

The average number of photons related to the highest secret key rates was 7.5 for both Gaussian modulation and QAM modulation, which facilitates their experimental implementation. Overall, the results obtained using homodyne detection were better than those using heterodyne detection.

B. Average Photon Number Analysis

Considering that the best results obtained in the previous analysis were for the 1024-QAM binomial constellation, we next present a performance comparison between this modulation format and the Gaussian constellation for different transmission distances. The objective is to evaluate the behavior of the average photon number and determine the optimal average photon number required for each case.

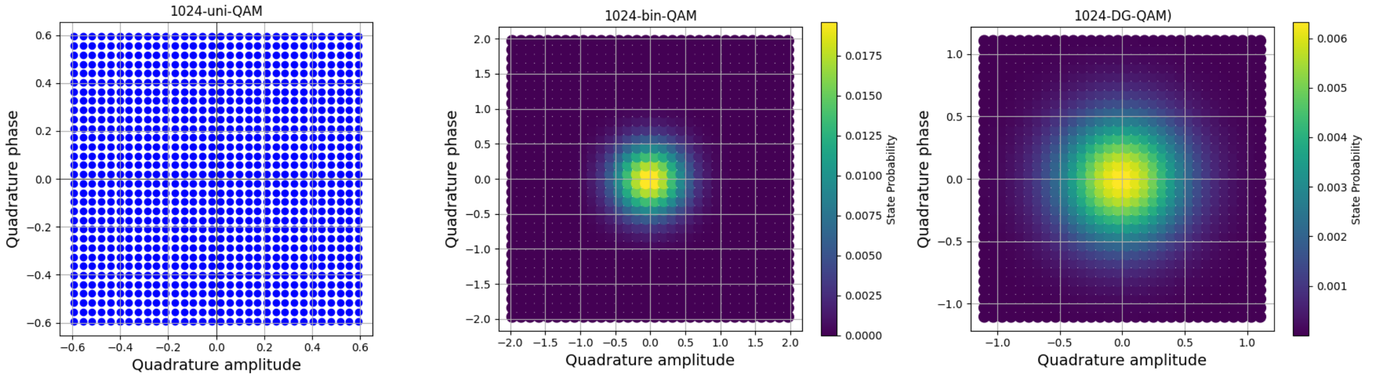

Fig. 2: Probability distributions for 1024-QAM modulation states in phase space: (a) uniform, (b) binomial, and (c) discrete Gaussian. Each plot shows the probability associated with every constellation point, highlighting differences in state weighting across the three models.

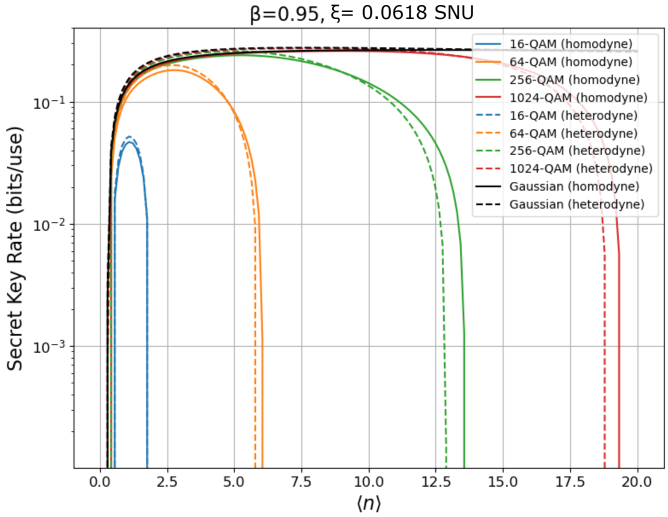

Fig. 3: Analysis of the secret key rate (SKR) versus the average photon number, comparing QAM and Gaussian modulation performance for homodyne and heterodyne schemes, plotted for a fixed transmission distance of 12 km under excess noise $\xi_{tot}/2$.

As shown in Fig. 8, longer transmission distances require lower average photon numbers — a counterintuitive result, since one might expect larger distances to demand more photons. This behavior arises from the fact that longer transmission distances reduce channel transmittance, thereby lowering the signal-to-noise ratio (SNR) and consequently limiting the average photon number.

The average photon number was the same for both Gaussian and 1024-QAM binomial constellations, varying only with distance: 7.5 for 5 and 10 km, 5 for 20 km, and 2 for 80 km. The secret key rate (SKR) was slightly higher for the Gaussian constellation in all scenarios, as expected for a continuous rather than a discrete distribution. Nevertheless, the 1024-QAM binomial scheme successfully maintains SKR under increased attenuation across metropolitan-scale distances.

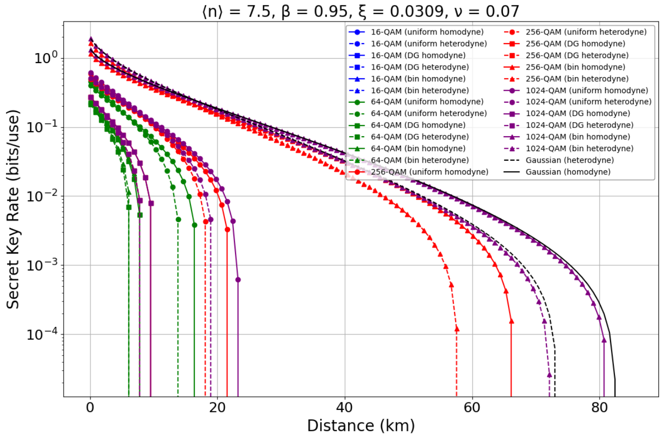

Fig. 4: Analysis of the secret key rate (SKR) versus distance for excess noise $\xi_{tot}/2$, comparing QAM and Gaussian modulation performance for homodyne and heterodyne schemes.

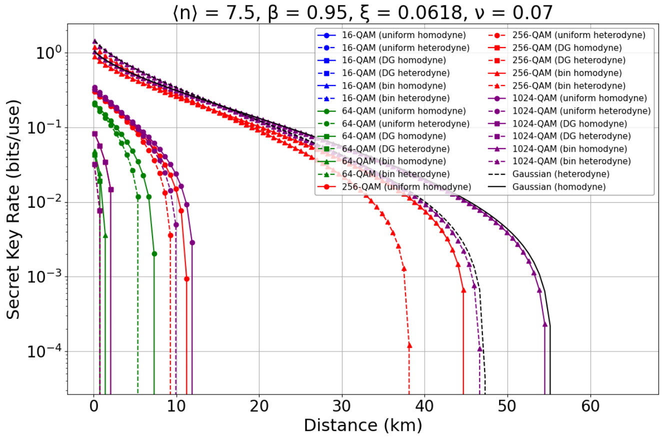

Fig. 5: Analysis of the secret key rate (SKR) versus distance for excess noise ξ_{tot}, comparing QAM and Gaussian modulation performance for homodyne and heterodyne schemes.

IV. CONCLUSION

In this work, we presented a comprehensive analysis of continuous-variable quantum key distribution protocols em-

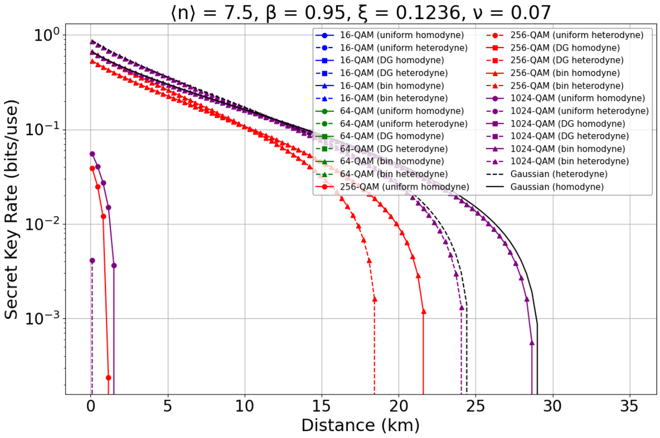

Fig. 6: Analysis of the secret key rate (SKR) versus distance for excess noise $2\xi_{tot}$, comparing QAM and Gaussian modulation performance for homodyne and heterodyne schemes.

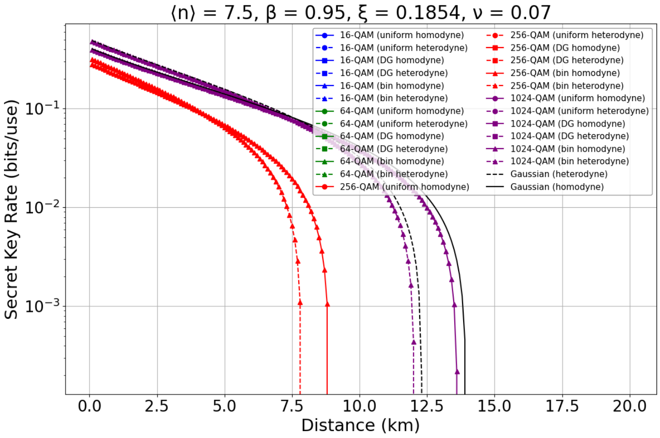

Fig. 7: Analysis of the secret key rate (SKR) versus distance for excess noise $3\xi_{tot}$, comparing QAM and Gaussian modulation performance for homodyne and heterodyne schemes.

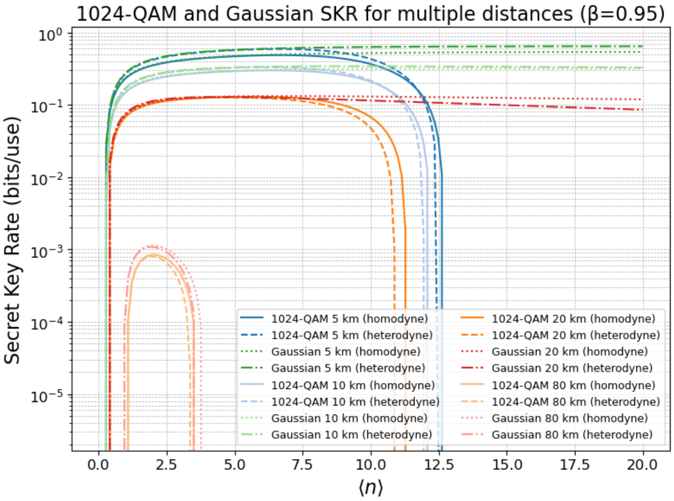

Fig. 8: SKR versus average photon number for 1024-QAM binomial and Gaussian constellations over metropolitan distances of 5, 10, 20, and 80 km.

ploying discrete modulation, focusing on 1024-QAM constellations, and compared their performance against standard Gaussian modulation. By simulating realistic hardware parameters and accounting for various sources of excess noise, we evaluated the secret key rate (SKR) as a function of transmission distance and average photon number, for both homodyne and heterodyne detection schemes.

Results show that high-order discrete modulation, particularly 1024-QAM with binomial or discrete Gaussian distributions, can closely approach the performance of Gaussian modulation while significantly reducing implementation complexity. A future avenue of research is to optimize the parameter ν of the discrete Gaussian distribution in order to assess whether there is a significant improvement in performance.

Homodyne detection consistently outperformed heterodyne detection in terms of maximum achievable distance and key rate, demonstrating its suitability for practical CV-QKD deployment. Interestingly, achieving longer transmission distances required a lower average photon number — a counterintuitive behavior that further highlights the flexibility of 1024-QAM in metropolitan-scale networks.

These findings highlight discrete modulation as a viable and practical alternative to Gaussian modulation, providing guidance for designing robust CV-QKD systems under realistic conditions. A natural way for future research is to validate these results experimentally in the laboratory, investigating the impact of each noise source, testing other high-order or hybrid modulation formats, and optimizing reconciliation strategies to advance scalable, high-performance, and long-distance quantum-secure communication networks.

ACKNOWLEDGMENTS

This work was fully funded by the "Impact of Laser Linewidth Variations in CV-QKD Systems: analysis and comparison" project supported by QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Industry 4.0 program of the MCTI, through Cooperation Agreement No. 053/2023, established with EMBRAPII.

REFERENCES

[1] Purva Sharma, Anuj Agrawal, Vimal Bhatia, Shashi Prakash, and Amit Kumar Mishra. Quantum key distribution secured optical networks: A survey. IEEE Open Journal of the Communications Society, 2:2049–2083, 2021.

[2] Mandeep Kumar and Bhaskar Mondal. A brief review on quantum key distribution protocols. Multimedia Tools and Applications, pages 1–40, 2025.

[3] Victor Lovic. Quantum key distribution: Advantages, challenges and policy. 2020.

[4] Guobin Xu, Jianzhou Mao, Eric Sakk, and Shuangbao Paul Wang. An overview of quantum-safe approaches: quantum key distribution and post-quantum cryptography. In 2023 57th Annual Conference on Information Sciences and Systems (CISS), pages 1–6. IEEE, 2023.

[5] Philip Chidozie Nwaga and Stephen Nwagwughiagwu. Exploring the significance of quantum cryptography in future network security protocols. World J Adv Res Reviews, 24(3):817–833, 2024.

[6] Sadik Khan, P Krishnamoorthy, Mrinal Goswami, Fayzieva Makhbuba Rakhimjonovna, Salman Arafath Mohammed, and D Menaga. Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses. Nanotechnology Perceptions, 20:S13, 2024.

[7] Mario Coccia, Saeed Roshani, and Melika Mosleh. Evolution of quantum computing: Theoretical and innovation management implications for emerging quantum industry. IEEE Transactions on Engineering Management, 71: 2270–2280, 2022.

[8] 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), 2024.

[9] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. Advances in optics and photonics, 12(4):1012–1236, 2020.

[10] Petar Radanliev. Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15(1):4, 2024.

[11] Sanjaikanth E Vadakkethil Somanathan Pillai and Kiran Polimetla. Analyzing the impact of quantum cryptography on network security. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), pages 1–6. IEEE, 2024.

[12] Valéria Loureiro da Silva, Micael Andrade Dias, Nelson Alves Ferreira Neto, and Alexandre B Tacla. From coherent communications to quantum security: Modern techniques in cv-qkd. In 2024 SBFoton International Optics and Photonics Conference (SBFoton IOPC), pages 1–5. IEEE, 2024.

[13] Yuehan Xu, Tao Wang, Lang Li, Huanxi Zhao, Peng Huang, and Guihua Zeng. Simultaneous continuous-variable quantum key distribution and classical optical communication over a shared infrastructure. Applied Physics Letters, 123(15), 2023.

[14] Matthieu Bloch, Andrew Thangaraj, Steven W McLaughlin, and J-M Merolla. Ldpc-based gaussian key reconciliation. In 2006 IEEE Information Theory Workshop-ITW'06 Punta del Este, pages 116–120. IEEE, 2006.

[15] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. Physical Review A—Atomic, Molecular, and Optical Physics, 77(4):042325, 2008.

[16] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum key distribution protocols with a discrete modulation. arXiv preprint arXiv:1002.4083, 2010.

[17] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum, 5:540, 2021.

[18] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. Physical Review A—Atomic, Molecular, and Optical Physics, 72(5):050303, 2005.

[19] 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, 2016.

[20] 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.

[21] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. Reviews of Modern Physics, 84(2):621–669, 2012.

[22] Rui Zhang, Wen-Jr Jiang, Konstantin Kuzmin, Yi Weng, Wenlong Mou, Gee-Kung Chang, and Winston I Way. The impact of local oscillator frequency jitter and laser linewidth to ultra high baud rate coherent systems. Journal of Lightwave Technology, 38(6):1138–1147, 2020.

[23] Margarida Almeida, Daniel Pereira, Margarida Facão, Armando N Pinto, and Nuno A Silva. Reconciliation efficiency impact on discrete modulated cv-qkd systems key rates. Journal of Lightwave Technology, 41(19): 6134–6141, 2023.