Optimization of CV-QKD Systems for Field Deployment

Margarida Almeida[1,2], Armando N. Pinto[1,2], Nuno A. Silva[1,3]

[1]*Instituto de Telecomunicações, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal*

[2]*Department of Electronics, Telecommunications, and Informatics, University of Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal*

[3]*University of Aveiro, Campos Universitário de Santiago, 3810-193 Aveiro, Portugal*

e-mail: mralmeida@ua.pt

ABSTRACT

Continuous-variables quantum key distribution (CV-QKD) allows the secure distribution of symmetric cryptographic keys using off-the-shelf equipment [1-3]. The use of higher-order discrete modulation (DM) in CV-QKD allows a simple implementation [4-5] and can approximate the theoretically optimal performance of Gaussian modulation [6,7,12]. Higher-order DM-CV-QKD has been experimentally demonstrated secure [8-9]. However, due to the computational expense and complexity involved in digital signal processing and post-processing, most experimental demonstrations [8-11] do not account for the reconciliation of the data for key extraction, misleading the achievable key rates [6,8]. We have studied the security bounds of DM-CV-QKD systems considering the true reconciliation efficiency and the frame error rate (FER) of the system, showing that the minimization of the FER does not assure the maximization of the key rate. The maximization of the extraction key rate must consider a proper signal-to-noise ratio (SNR) optimization accounting for the reconciliation step [12,13]. Moreover, the choice of the reconciliation method must also consider the requirements of each reconciliation method in terms of the amount of information transmitted on the classical channel. Since, due to the bandwidth limitations of the optical link, such may limit the achievable key rates, as we analyze in [14].

In systems using optical fiber, the random birefringence of the fiber inevitably disturbs the state of polarization (SOP) of the quantum signal [15], impacting the overall secret key rate. In [16], we analyze the effect of the SOP fluctuations on the estimation of the channel parameters and compare the resulting secret key rate with the theoretical value considering the polarization drift in the channel. Conventionally, the parameter estimation step is provided assuming a perfect channel without polarization drift. By doing so, the estimation of the channel parameters is highly degraded with the increase of the SOP fluctuations. This results in a sub-estimation of the secret key rate, decreasing the performance of the system. As future work, we will study the security of the CV-QKD system considering polarization diversity heterodyne detection, as implemented in the laboratory, to measure both polarization components of the signal. This, aided by digital signal processing methods to combine both polarization components, is expected to improve the estimation of the channel parameters and the overall secret key rate. Experimentally, we are improving the implementation of the DM-CV-QKD system for symmetric keys extraction focusing on characterizing and reducing the noise sources in the system.

Keywords: Quantum Key Distribution; Continuous Variables; Discrete Modulation; Polarization Drift; Polarization Diversity Detection; Experimental Implementation.

REFERENCES

[1] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, Jan. 2002.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, Dec. 2020.

[3] M. Almeida, D. Pereira, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of imperfect homodyne detection on measurements of vacuum states shot noise," *Optical and Quantum Electronics*, vol. 52, no. 11, Nov. 2020.

[4] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, "High-speed gaussian modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," *Optics Express*, vol. 28, no. 22, p. 32 882, Oct. 2020.

[5] E. Kaur, S. Guha, and M. M. Wilde, "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution," *Physical Review A*, vol. 103, no. 1, Jan. 2021.

[6] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, Sep. 2021.

[7] M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, and N. A. Silva, "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution," *Optics Express*, vol. 29, no. 23, p. 38669, Nov. 2021.

[8] F. Roumestan, A. Ghazisaeidi, J. Renaudier, P. Brindel, E. Diamanti, and P. Grangier, “Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution,” *Optical Fiber Communication Conference (OFC) 2021*, 2021.
[9] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, “Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres,” *Optics Letters*, vol. 47, no. 15, p. 3948, July 2022.
[10] W. Liu, Y. Cao, X. Wang, and Y. Li, “Continuous-variable quantum key distribution under strong channel polarization disturbance,” *Physical Review A*, vol. 102, no. 3, Sep. 2020.
[11] S. Kleis, M. Rueckmann, and C. G. Schaeffer, “Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals,” *Optics Letters*, vol. 42, no. 8, p. 1588, Apr. 2017.
[12] 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*, vol. 41, no. 19, p. 6134 - 6141, May 2023.
[13] Margarida Almeida, Armando N. Pinto, and Nuno A. Silva, “Modulation variance optimization in discrete modulated CV-QKD systems,” *Quantum Technologies and Quantum Information Science VI, part of SPIE Security + Defence*, Amsterdam, Netherlands, September 2023.
[14] Margarida Almeida, Daniel Pereira, Armando N. Pinto, and Nuno A. Silva, “Classical Channel Bandwidth Requirements in CV-QKD Systems,” Submitted to the IET Quantum Communications.
[15] W. Liu, Y. Cao, X. Wang, and Y. Li, “Continuous-variable quantum key distribution under strong channel polarization disturbance,” *Physical Review A*, vol. 102, no. 3, Sep. 2020.
[16] Margarida Almeida, Armando N. Pinto, and Nuno A. Silva, “Polarization Drift Impact on the Performance of CV-QKD,” Accepted for poster in Qcrypt 2024, Vigo, Spain.

ACKNOWLEDGEMENTS

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under the PhD Grant UI/BD/153377/2022, projects QuantumPrime (PTDC/EEI-TEL/8017/2020), and co-funded by the Europen Defence Industrial Development Program (EDIP) under the project DISCRETION (S12.858093).