Adapting the Classical Optical Communication Simulation Framework for Continuous-Variable Quantum key Distribution Simulations

Essam Berikaa[(1)*], Fabio Cavaliere[(2)], Jinsong Zhang[(1)], Ramón Gutiérrez-Castrejón[(3)], Luca Giorgi[(2)], Antonio D'Errico[(2)], Stephane Lessard[(4)], David V. Plant[(1)]

[(1)] *Department of Electrical and Computer Engineering, McGill University*, Montréal, Québec H3A 0E9, Canada,
* essam.berikaa@mail.mcgill.ca

[(2)] *Ericsson Research*, Via G. Moruzzi 1, 56124 Pisa, Italy

[(3)] *Institute of Engineering*, Universidad Nacional Autónoma de México UNAM, 04510 Mexico City, Mexico

[(4)] *Ericsson Research*, Saint-Laurent, Montreal, QC H4S 0B6, Canada

***Abstract*—The compatibility of the CV-QKD with the existing telecommunication infrastructure promotes its deployment and integration into existing networks. In this paper, we demonstrate accommodating the classical Optiwave OptiSystem software to CV-QKD simulations, which facilitates the joint simulation of public and quantum channels. The simulation framework is verified through simulating the Gaussian modulated coherent-state (GMCS) CV-QKD protocol with practical parameters followed by the conventional reconciliation and error correction algorithms. We use MatLab to impose the photon statistics of the weak-coherent states and for post-processing. The simulation is concluded by calculating the secure key rate. Simulating CV-QKD systems with OptiSystem examines the practical imperfections of the optical components, and it is anticipated to accelerate and simplify the development of CV-QKD systems.**

I. INTRODUCTION

Quantum key distribution (QKD) is a secure way of exchanging cryptographic keys between two parties based on the laws of quantum mechanics. Its unconditional security comes from the quantum no-cloning theorem and Heisenberg's uncertainty principle, which allow the communicating parties to detect eavesdropping [1]. Several QKD protocols and systems have been proposed and implemented based on discrete variables; though, the continuous variable (CV)-QKD is dominating due to its compatibility with the telecommunication infrastructure, and its higher secure key rates and transmission range [2, 3]. There exist various mathematical models that attempt to model the different noise sources in the CV-QKD system for estimating the secure key rate [4, 5]. However, these models consider simplified experimental setups and ideal components, which highlights the need for developing an accurate simulation platform.

Significant efforts have been devoted to developing QKD simulators. The majority have considered numerical analysis of different QKD protocols, which does not involve any physical constraint on the physical QKD system [6, 7]. Other tools have been developed for high-level simulations of QKD networks that analyze the overall performance of the network including both quantum and public channels [8, 9]. These tools assume a perfect setup and the experimental imperfections are collectively described in the value of the excess noise. In this work, we demonstrate the possibility to adapt the classical optical communication simulator OptiSystem for CV-QKD simulations considering practical imperfections and experimental overheads. To that end, MatLab is used for post-processing and to enforce some of the characteristics of the CV-QKD weak coherent states. As a proof of concept, the Gaussian modulated coherent-state (GMCS) GG02 CV-QKD protocol is simulated and the secret key fraction is calculated [10, 11].

II. GG02 CV-QKD PROTOCOL

The Gaussian modulated coherent-state (GMCS) GG02 CV-QKD protocol is based on weak coherent states as the carrier for the quantum information [10, 11]. These states can be generated by high-quality continuous lasers and are characterized by Poisson photon statistics. At the transmitter side, Alice encodes the electric field quadratures x and p independently with 2 zero-mean random normal distributions; $X \sim N(0, \Sigma_A)$ and $P \sim N(0, \Sigma_A)$. Gaussian modulation implies that both random distributions have the same variance (Σ_A), unlike squeezed states CV-QKD. Heisenberg uncertainty guarantees that both quadratures x and p cannot be measured simultaneously with full accuracy; hence, eavesdropping will leave a signature on the state's quadrates and can be detected. At the receiver, Bob randomly chooses one of the quadratures and measures it with a shot-noise-limited homodyne detector. Consequently, Bob shares with Alice the sequence of measured quadratures, and Alice discards the unused quadrature data. By the end of this step, Alice and Bob possess 2 correlated distributions. Ultimately, reconciliation algorithms are used to distil a secret key out of these correlated distributions.

III. SIMULATION MODEL

The developed simulation model of the GG02 CV-QKD protocol is illustrated in Fig. 1. At the transmitter, the first amplitude modulator converts the continuous laser output to a train of intense pulses at a constant repetition rate, which is divided into a strong local oscillator (LO) and a weak signal by a 1:99 directional coupler. OptiSystem assumes that lasers are constant power sources, which is valid for high laser powers. The GG02 CV-QKD protocol is based on weak coherent states that follow a Poisson distribution. Thus, MatLab is used to impose the Poisson photon statistics on the signal path before Gaussian modulation. The IQ modulator modulates the electric field quadratures (x and p) of the weak coherent states, which is followed by an optical attenuator to control the modulation variance and the number of photons per pulse. Then, both the LO and the modulated weak coherent states are transmitted over the same optical fiber through polarization multiplexing. At the receiver, both signals are first demultiplexed and their polarization states are matched with a polarization rotator. MatLab is used to model a voltage-controlled phase shifter that randomly alternates the

978-3-903176-33-1

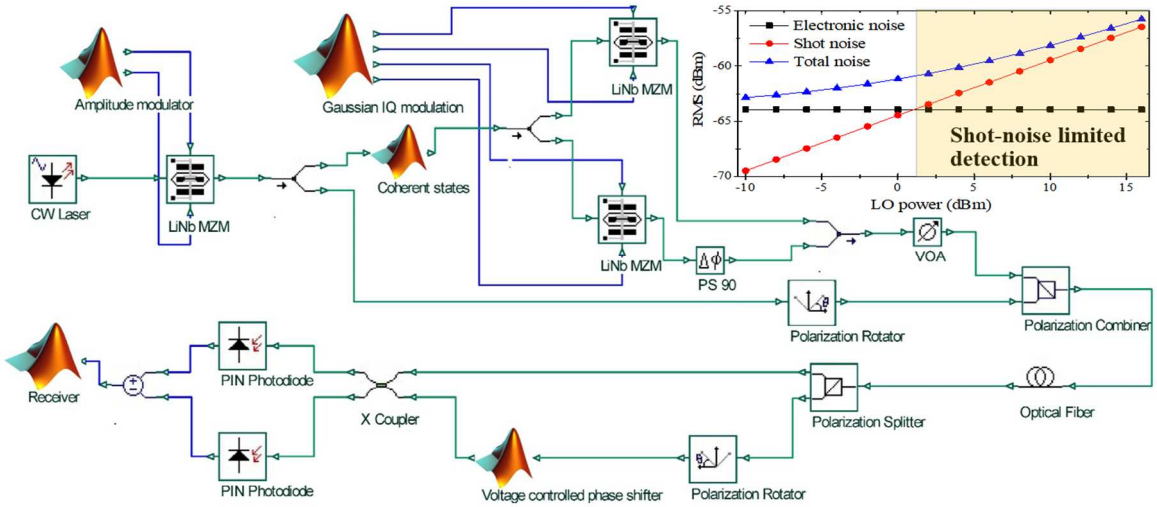

Fig. 1. Schematic of the simulated CV-QKD system. Green lines indicate optical paths, and blue lines indicate electrical signals. The inset shows the total noise of the simulated balanced photodetector at different LO powers.

phase of the LO between 0 and π/2; hence, only one quadrature can be detected. Then, the received weak coherent states and the LO are mixed in a 2x2 coupler followed by 2 balanced photodiodes. The output is proportional to only one of the quadratures according to the phase difference between the signal and the LO. Subsequently, the post-processing is entirely done in MatLab, which includes channel characterization, reconciliation, and privacy amplification. After transmitting N pulses, a portion of these key elements is disclosed for estimating the channel transmission and calculating the probability joint density between transmitter and receiver. The sliced-error correction (SEC) algorithm converts the remaining secret key elements to binary data with an acceptable probability of errors. These errors are corrected with the cascade binary correction protocol. Eventually, a secret key is distilled through multiplying the corrected binary keys with a Toeplitz matrix to erase the disclosed information [12].

Table I shows the parameters used in the simulation. These parameters are adopted from experimental demonstrations of the GG02 CV-QKD protocol [3, 13, 14]. The photodiode noise models are verified to ensure that it is shot-noise limited in the CV-QKD simulations. The contribution of the electronic noise and shot noise at different LO power is depicted in the inset of Fig. 1, which reveals that the detection is limited by the shot noise for LO power higher than 1.5 dBm at the receiver side. OptiSystem has Gaussian and Poisson shot-noise models; the Poisson distribution is used as it is more accurate for weak pulses.

TABLE I. THE SIMULATION PARAMETERS

Repetition rate	50 Mbps	**Optical fiber:**	
Pulse width	2 nS	Attenuation constant	0.2 dB/km
CW Laser:		Dispersion coefficient	16.7 ps/nm.km
Laser power	12 dBm	Dispersion slope	0.07 ps/nm².km
Line width	100 KHz	**PIN photodetector:**	
$LiNbO_3$ MZM:			
Insertion loss	4 dB	Responsivity	0.8 A/W
Extinction ratio	30 dB	Bandwidth	1 GHz
Vπ	3 V	Dark current	10 nA

IV. RESULTS

The proposed simulation framework has been tested based on the tabulated parameters. Fig. 2A shows the photon statistics of the coherent states before the modulation, which is following the imposed Poisson distribution. This contributes to the uncertainty in the measurements as the prepared states are not measured at the transmitter side. Fig. 2B presents the probability density function for the number of photons per pulse at the receiver side after transmission for different fiber lengths. The inset shows the mean photon number per pulse as a function of the fiber length. It highlights the impact of fiber attenuation on the number of photons reaching the receiver, which can be manipulated further through the variable optical attenuator (VOA) at the transmitter side to optimize the secret key rate. The correlation between the transmitted and received quadratures is quantified and depicted in Figs. 2C-E. The common quadrature is highly correlated and the correlation degrades with the transmission distance due to the reduction of the signal-to-noise (SNR) ratio. The nonlinearity observed in the correlation function is caused by the nonlinear transfer function of the Mach-Zehnder modulators. In contrast, the discarded quadrature is totally uncorrelated with the measured quadrature at the receiver.

For calculating the secure key rate, the transmitter sends a block of 174080 pulses, 20000 symbols are disclosed for channel characterization and the remaining key elements are used in distilling the final secret key. The SNR ranges from 11.5 dB at 0 km to -0.7 dB at 40 km, which ensures operating at the shot-noise detection limit. A secure key is distilled from these correlated values through reverse reconciliation that utilizes the sliced-error correction algorithm. For this proof-of-concept simulation, 5 slices with optimized slicing function are used for error correction and secure key fraction estimation [12]. The asymptotic reconciliation efficiency is 95%; however, the achieved efficiency is 85% only due to the small block size of the transmitted pulses and the finite optical signal-to-noise ratio (OSNR). Fig. 3 shows the calculated secure key fraction and Shannon's theoretical bound as a function of the transmission distance. The calculated secure key rate at 25km is 1.013 Mbps, which

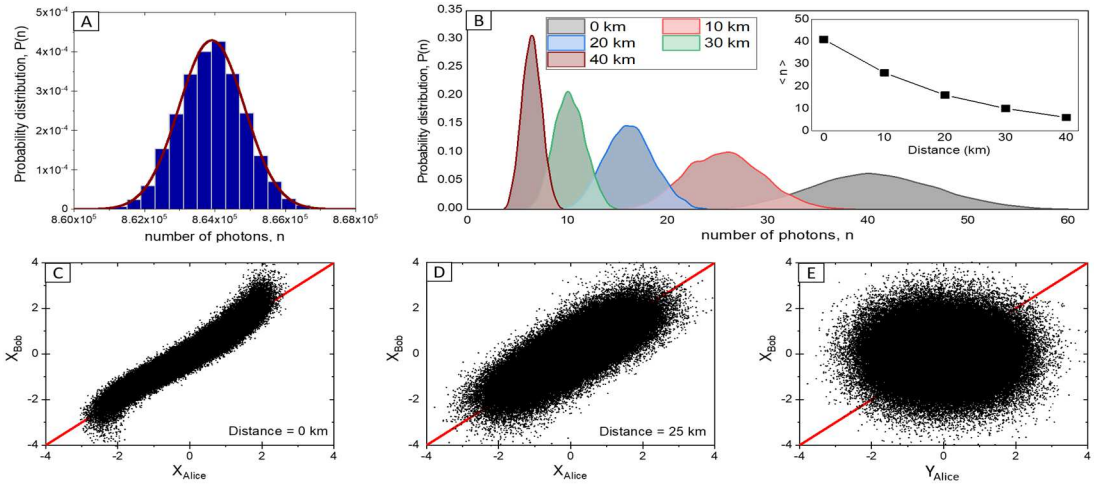

Fig. 2. The probability density function for the number of photons per pulse before modulation (A) and at the receiver side at different transmission distances (B); the inset shows the average number of photons per pulse at different transmission distances. The correlation between the transmitted and measured quadratures at 0 km (C), and 25 km (D). (E) The correlation between the discarded and measured quadratures.

matches the experimentally demonstrated key rate at the same repetition rate [3].

The main advantage of the proposed simulation framework is its compatibility with conventional optical communication simulations; hence, both quantum and public channels can be simulated concurrently. Additionally, the QKD channel performance in wavelength-division multiplexing (WDM) system can be evaluated [3, 15]. OptiSystem has accurate models for the conventional optical communication components, which are the building blocks for all experimentally demonstrated CV-QKD systems. These models include the nonidealities of these components and the user is even able to interfere and input the transfer function measured practically in the lab. Estimating the CV-QKD system performance based on the proposed simulation framework captures the impact of modulator nonlinearity and finite extinction ratio, bandwidth limitation of the different components in the CV-QKD system, and fiber nonlinearities; to name a few experimental imperfections that are hard to be considered by analytical models [4]. It is also suitable for testing and debugging the different digital signal processing algorithms for CV-QKD systems. It is worth noting that the proposed simulation framework aims to study the performance of the CV-QKD system considering the practical behavior of the system components rather than simulating the security attacks or verifying the security proofs.

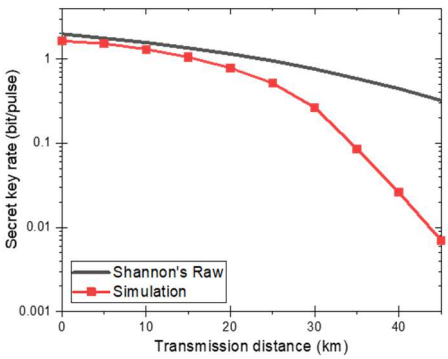

Fig. 3. The calculated secure key fraction (bits/symbol) dependency on transmission distance.

V. Conclusion

To conclude, this work shows how to adapt the classical OptiSystem simulator for simulating the performance of CV-QKD, which aims to speed up and facilitate experimental demonstrations of CV-QKD systems. A proof-of-concept simulation is reported for the GG02 CV-QKD protocol and the secure key fraction is estimated.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography," in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, 1984, pp. 175-179.

[2] Y. Zhang *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.,* vol. 125, no. 1, p. 010502, 2020.

[3] D. Huang *et al.*, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Opt. express,* vol. 23, no. 13, pp. 17511-17519, 2015.

[4] F. Laudenbach *et al.*, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," *Adv. Quantum Technol,* vol. 1, no. 1, p. 1800011, 2018.

[5] E. Samsonov, et al., "Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis," *Sci. Rep,* vol. 10, no. 1, pp. 1-9, 2020.

[6] A. Atashpendar, "QKD Simulator (https://qkdsimulator.com/)," 2014.

[7] M. Kalra and R. C. Poonia, "Simulation of BB84 and proposed protocol for quantum key distribution," *J. Statistics and Management Systems,* vol. 21, no. 4, pp. 661-666, 2018.

[8] M. Mehic, et al., "Implementation of quantum key distribution network simulation module in the network simulator NS-3," *Quantum Inf. Process.,* vol. 16, no. 10, p. 253, 2017.

[9] X. Wu, B. Zhang, and D. Jin, "Parallel Simulation of Quantum Key Distribution Networks," in *Proc. 2020 ACM SIGSIM Conf. on Principles of Advanced Discrete Simulation*, 2020, pp. 187-196.

[10] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.,* vol. 88, no. 5, p. 057902, 2002.

[11] F. Grosshans, et al., "Quantum key distribution using gaussian-modulated coherent states," *Nature,* vol. 421, no. 6920, pp. 238-241, 2003.

[12] G. Van Assche, "Quantum cryptography and secret-key distillation," *Univ., Cambridge Press*, 2006.

[13] G. Zhang *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics,* vol. 13, no. 12, pp. 839-842, 2019.

[14] B. Qi, et al., "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A,* vol. 76, no. 5, p. 052323, 2007.

[15] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *J. Opt. Commun,* vol. 11, no. 6, pp. 285-298, 2019.