European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Designing a Digital Twin for Quantum Key Distribution

M. Ahmadian[(1)], M. Ruiz[(1)], M. B. On[(2)], S. K. Singh [(2)], J. Comellas[(1)], R. Proietti[(3)], S.J.B. Yoo[(2)], and L. Velasco[(1)]

[(1)] Universitat Politècnica Catalunya (UPC), Barcelona, Spain (*luis.velasco@upc.edu)
[(2)] University of California, Davis, USA. [(3)] Politecnico di Torino, Turin, Italy

Abstract *Classical optical devices lack precision when they operate on single photons. We report a Quantum Digital Twin (QDT) to improve Quantum Key Distribution (QKD) implementations. We show a QDT increasing the Key Exchange Rate under environmental events*. ©2022 The Author(s)

1. Introduction

Quantum Key Distribution (QKD) is opening a new era for secure communications [1] since it enables the distribution of unlimited keys between two distant parties. Nonetheless, QKD requires optical devices with high-precision, which increases its cost and limits its deployment.

In polarization-encoded QKD, a Quantum Transmitter (QTx) randomly and privately selects pairs <bit, basis> (*qubit*) in which one linear State of Polarization (SOP) (Horizontal (H), Vertical (V), Diagonal (D) and Anti-diagonal (A)) is mapped onto. Then, the QTx emits a single photon polarized in the direction of the selected SOP, which is propagated through the fiber channel and received by a Quantum Receiver (QRx). The QRx also randomly and privately selects a binary basis, and measures the received photon based on the basis. If both QTx and QRx have chosen the same basis, the binary measurement of the photon in the QRx matches the selected bit in the QTx. With this method, both parties can privately share a key with those bits that matched the bases. However, many events during photon transmission through the channel can change the measurement, which result in bases mismatches [2]. Specifically, polarization-encoded QKD can be degraded by SOP distortion induced by the long fiber between QTx and QRx. SOP distortions can be compensated using feedback-based compensation methods available in the literature [3]. However, those methods assume ideal conditions with perfectly calibrated optical components and cannot be supported by optical components that introduce unexpected photon loss, undesired polarization effects, and other non-ideal behaviors.

Digital Twins (DT) have been proposed for communications for fault management by taking advantage of data, models, and algorithms [4]. In this paper, we design a Quantum DT (QDT) that models the Quantum Physical Channel (QPC) and shows its application to overcome the above-mentioned imperfections and consequently improve the performance of the QKD system.

2. Quantum Digital Twin and Use cases

The proposed QDT models every component of the QPC. We assume the QPC components presented in Figure 1, with a QTx and QRx connected by a Single Mode Fiber (SMF).

The QTx includes a Single Photon Emitter (SPE) and a polarizer that changes the photons' SOP as a function of the qubit to be transmitted. The SMF connecting QTx to QRx impacts the SOP and introduces photon loss; additionally, variable SOP impact is produced when the fiber is affected by environmental conditions. In the QRx, a balanced Beam Splitter (BS) separates the photons and acts as the random basis selection for the QKD system. Note that the BS can introduce photon loss through its arms [5]. Then, an Electronic Polarization Controller (EPC) changes the SOP with either tunable retardation or tunable orientation of its wave plates [6]. These changes are used to compensate for SOP distortion through the fiber. The internal characteristics of commercially available EPCs are not precisely specified by the manufacturers. A Polarizing Beam Splitter (PBS) separates the photons based on their SOP and acts as bit selector. One arm (*reflection*) passes H polarized photons while the other (*transmission*) passes vertically polarized ones. As the BS, the PBS introduces photon loss through its arms. A module with two Single Photon Detectors (SPD) counts photons. However, the SPDs record more photons than the ones actually hitting them; the additional portion is known as *dark count rate*.

Several use cases can be defined that take advantage of the QDT, e.g., 1) the QDT can optimize the QKD system by adjusting the tunable parameters of the optical components. The tunable parameters in the QPC are related to the polarizer in the QTx, as well as the EPC and SPDs in QRx. Armed with measurements gathered from the QPC, the QDT can provide the needed adjustments of QPC's components for the current QKD system; 2) the QDT can distinguish between eavesdropping and excessive Quantum BER (qBER) in the QPC.

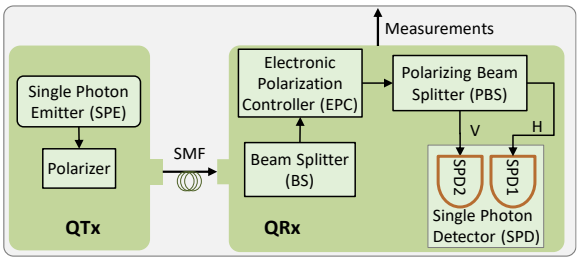

Figure 1. QPC architecture and components.

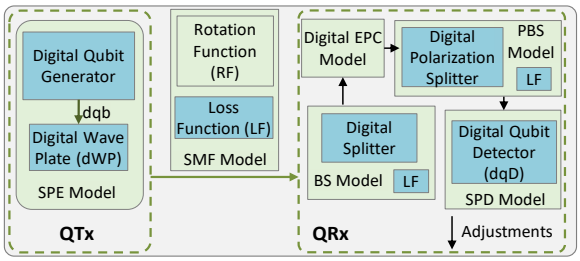

Figure 2. QDT architecture and components.

Table 1: QDT models' and tunable parameters.

Model	Purpose	Tunable Parameters
SPE	Qubit Generation, state initialization	SOP distortion of emitted photons
SMF	Apply fiber impacts (distortion, optical loss) on the state	Fiber length and SOP distortion
BS	Reflect or transmit the qubit (50%, 50%)	photon loss in each arm
PBS	Reflect or transmit the qubit based on the state	photon loss in each arm
EPC	Apply EPC's impact to the state	Wave plates variables
SPD	Store qubit's probability in a repository	Dark count rate

The SOP evolution is traceable when the SMF suffers from external movements caused by human operator works or environmental conditions. In contrast, eavesdropping results into unrecognizable SOP changes [3]; and 3) the QDT can tune parameters used during the key distillation procedure, e.g., qBER threshold for discarding the keys. By distinguishing eavesdropping and excessive qBER, the threshold can be increased, which would increase the Key Exchange Rate (KER).

3. QDT Components and Models

Figure 2 presents the architecture of the proposed QDT, where each block in the QDT models a counterpart optical component in the QPC. The models are presented next.

A generator of digital twins of photons, where their quantum state can be modeled as eq. (1), where α is the phase with respect to orthogonal electric field (x,y) components polarized with orientation angle θ [7]. Here, the quantum state perfectly matches the SOP of emitted photons.

$$|\psi_{DQ}\rangle = \begin{pmatrix} \cos(\theta).\exp(i\alpha_x) \\ \sin(\theta).\exp(i\alpha_y) \end{pmatrix} \quad (1)$$

Next, the digital wave plate (dWP) acts as a quantum gate and it affects the generated digital qubit (*dqb*) in the same way that an optical wave plate changes the SOP of a photon. Eq. (2) is used to model the quantum gate with the orientation angle θ and phase retardation φ of the wave plate [8].

$$dWP_\theta(\varphi) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
$$a = e^{i\varphi/2}cos^2(\theta) + e^{-i\varphi/2}sin^2(\theta)$$
$$b = c = -isin(2\theta)\cdot sin(\varphi/2) \quad (2)$$
$$d = e^{-i\varphi/2}cos^2(\theta) + e^{i\varphi/2}sin^2(\theta)$$

The SMF is modeled by a rotation function (RF), which rotates the SOP. Eq. (3) computes the required quantum gate using the matrix multiplication of three dWPs, where the orientation angles (θ_1,θ_2,θ_3) are derived from the input and output SOP [9]. In addition, a loss function (LF) discards *dqbs* with a probability in line with the photon loss rate of the fiber (eq. (4)). The same function is used in the models of other optical components.

$$RF = dWP_{\theta_1}(\pi/2)\cdot dWP_{\theta_2}(\pi)\cdot dWP_{\theta_3}(\pi/2) \quad (3)$$

$$P(dq\_Tx) = 1 - Loss_{op\_comp} \quad (4)$$

In the QRx, a digital splitter receives *dqbs* and randomly outputs them through the digital reflection (dR) or digital transmission (dT) with equal probability. Similarly, as in the RF, the digital EPC model is a matrix multiplication of dWPs, where the orientation angle and the retardation phase of each component can be set based on physical EPC's specifications. Next, the digital polarization splitter receives *dqbs* and outputs them through the dR or dT based on its quantum state (eq.(5)).

$$P(\mathrm{dR}) = P(H) = cos^2(\theta)$$
$$P(\mathrm{dT}) = P(V) = sin^2(\theta) \quad (5)$$

Finally, a digital qubit detector (dqD) receives P(dR) and P(dT) and adds dark counts based on physical dark count rates.

Table 1 summarizes the purpose of the QDT models and their tunable parameters.

4. Results

In this section, we illustrate the imperfections of QPC's components as well as QDT's capability to improve the QKD system. Components' non-ideal behavior are experimentally verified on an experimental testbed set up at UCDavis. Figure 3 shows the testbed and the main components. In the QTx, weak coherent states were used to probabilistically create single-photon pulses. Integration time for photon counts was 0.1 sec. Data generated is openly available in [10].

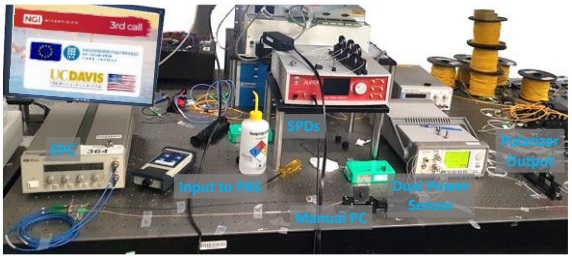

Figure 3. Experimental Testbed.

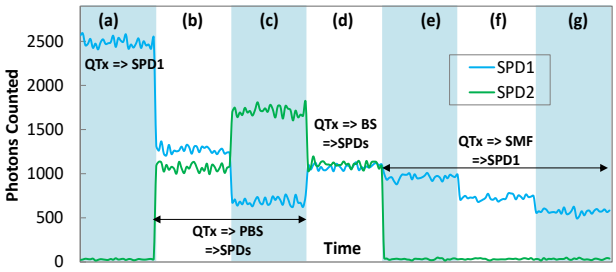

Figure 4. Impact of QPC imperfections.

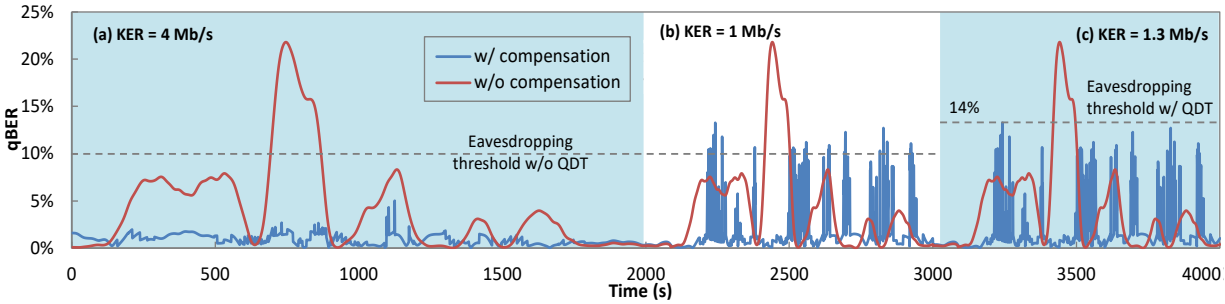

Figure 5. Improvement of the QKD using QDT.

Figure 4 presents the undesired SOP effects in the optical components. The QTx was configured to generate horizontally polarized photons only and to reach a range of 2,500 photons per 0.1 sec: one fixed attenuator and one variable attenuator with 40 and 46 dB, respectively, were placed. Seven testbed configurations are represented in Figure 4: (a) the QTx is directly connected to SPD1; (b) the QTx is connected to a PBS with a bended SMF. The PBS is followed by SPDs; (c) same to (b) but different SMF bending radius; (d) the QTx is connected to a BS and the BS arms are connected to SPD1 and SPD2; (e, f, g) The QTx is connected to a SPD1 through a SMF of 15km, 20km, 25km, respectively. We observe that the SPDs count 2500 photons only when they are directly connected to the QTx in (a). Installing a bended SMF between QTx and QRx changes SOP of the photons, as photons are counted in SPD2 also. Furthermore, different shapes of bended SMF introduce different SOP distortion (b-c). In (d), total counted photons in SPD1 plus in SPD2 is 1050 photons on average, i.e., the BS introduces 200 photon loss through its arms. Finally, the longer the fiber, the more the photons are linearly lost (e-g). Apart of the aforementioned results, the dark count rate in the SPD was 30 photons, when the integration time and quantum efficiency were 0.1 second and 10% respectively.

Let us now analyze the capability of the QDT to improve the QKD system. In this case, the QRx includes all the elements, i.e., EPC, PBS and SPDs. Measurements from the QPC were collected and made available to the QDT, so it could tune the optical components. Experimental data from a fiber shaking event [11] was used to change the SOP of the photons passing through the SMF. The QTx continuously emitted H polarized photons, so qBER was computed with counted photons in SPD2 only. The predictive feedback-based SOP compensation presented in [3] was implemented. The obtained qBER with and without SOP compensation is depicted in Figure 5. Three scenarios for the fiber shaking event were studied: (a) the shaking event at its original speed; (b) twice its original speed; (c) twice its original speed with QDT assistance. In scenarios (a) and (b), the eavesdropping threshold used for key distillation was set to 10%, whereas in scenario (c), the QDT tuned the threshold to adapt it to the current conditions. We observe that in scenario (a) SOP compensation was able to drastically reduce qBER, which otherwise would exceed the eavesdropping threshold. In scenario (b), qBER dramatically rose and the threshold was almost exceeded even with SOP compensation. In this scenario, KER reduced from 4 to 1 Mb/s, although it would be 0 in case of threshold violation. However, with the ability of the QDT to distinguish excessive qBER from eavesdropping, the threshold was increased to 14%, as the SOP evolution could be clearly traced; then, photons were used for the key distribution procedure instead of being discarded. This resulted in a 30% increment in KER in case of extreme environmental events or operators works on patch panels.

Acknowledgements

The research leading to these results has received funding from the EC through the H2020 NGIatlantic.eu 3rd open call (03-275), the MICINN IBON (PID2020-114135RB-I00), the U.S. NSF ICE-T program through the award # 1836921, the U.S. Department of Energy under Award Number DE-SC-0022336, and the ICREA Institution.

References

[1] V. Martin, J. Martinez-Mateo, M. Peev, “Introduction to Quantum Key Distribution,” Wiley Encyclopedia of Electrical and Electronics Engineering, 2017.

[2] S. Pillay, A. Mirza, F. Petruccione, “Towards polarisation-encoded quantum key distribution in optical fibre networks,” South African Journal of Science, vol.111 pp.7-8, 2015, DOI: 10.17159/SAIS.2015/20130380

[3] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, “Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution,” IEEE/OPTICA J. of Lightwave Technology (JLT), Early Access, 2022. DOI: 10.1109/JLT.2022.3157527

[4] D. Wang, Z. Zhang, M. Zhang, M. Fu, J. Li, S. Cai, C, Zhang, X. Chen, “Role of Digital Twin in Optical Communication: Fault Management, Hardware Configuration, and Transmission Simulation,” IEEE Communications Magazine, Vol.59 no.1 pp.133-139, 2021, DOI: 10.48550/arXiv.2011.04877

[5] S. Barnett, J Jeffers, A. Gatti, “Quantum optics of lossy beam splitters,” Physical Review A, vol. 57, 1998, DOI: 10.1364/OE.24.016440

[6] X. Zhang, Y. Zheng, “Classical Areas of Phenomenology: The number of least degrees of freedom required for a polarization controller to transform any state of polarization to any other output covering the entire Poincaré sphere,” Chinese Physics B vol. 17, pp. 2509-2513, DOI: 10.1088/1674-1056/17/7/027

[7] J. Jackson, Classical Electrodynamics, 3nd ed. Hoboken, NJ: John Wiley & Sons, Inc., 1998. ISBN: 978-0-471-30932-1

[8] M. Al-Mahmoud, H. Hristova, V. Coda, A. Rangelov, N. Vitanov, “Non-reciprocal wave retarder based on optical rotators combination,” OSA Continuum, vol. 4, pp.2695-2702, 2021, DOI: 10.1364/OSAC.439325

[9] N. Muga, A. Nolasco, M. Ferreira, J. da Rocha, “Uniform Polarization Scattering With Fiber-Coil-Based Polarization Controllers,” IEEE/OPTICA J. of Lightwave Technology, vol. 24, pp 3932-3943, DOI: 10.1109/JLT.2006.883642

[10] M. Ahmadian, M. Ruiz, S. K. Singh, M. B. On, D. Careglio, J. Comellas, R. Proietti, S.J. Ben Yoo, and L. Velasco, “Replication data for Fast Quantum Key Distribution,” https://dataverse.csuc.cat, 2022.

[11] F. Boitier, V. Lemaire, J. Pesic, L. Chavarria, P. Layec, S. Bigo, E. Dutisseuil, “Proactive fiber damage detection in real-time coherent receiver,” in Proc. ECOC, 2017.