DARIUS: A Digital Twin to Improve the Performance of Quantum Key Distribution

Morteza Ahmadian, Marc Ruiz, Jaume Comellas, and Luis Velasco

***Abstract*—Polarization encoded Quantum Key Distribution (QKD) is attracting great attention as it generates unlimitedly and unconditionally secure keys for different use cases. Despite its theoretical excellence based on quantum physics, commercial optical devices supporting QKD systems lack precision, which highly limits the final Key Exchange Rate (KER) of the system. Beside optical component imperfections, eavesdropping and unpredicted environmental events occurred in the quantum channel increase quantum Bit Error Rate (qBER), which leads to further KER reduction. In this article, we propose DARIUS, a digital twin for polarization encoded QKD systems that bridges the gap between perfect theoretical QKD systems and real implementations to: *i*) address optical components' non-ideal behavior; *ii*) discern eavesdropping from high qBER; and *iii*) dynamically compensate for environmental events. Taking advantage of DARIUS, even moderate eavesdropping rates can be distinguished from qBER. Moreover, significant improvement in proactive environmental event compensation is achieved, as DARIUS can derive proper optical component tuning.**

***Index Terms*—Machine learning, polarization-encoded quantum key distribution (QKD), quantum digital twin.**

I. Introduction

QUANTUM Key Distribution (QKD) is opening a new era for secure communications since it enables the distribution of unlimited secret keys between two distant parties [1]. Nonetheless, because of the very low power of the optical signal, QKD requires devices with high-precision, which increases their cost and limits the deployment of QKD systems. In polarization-encoded QKD, the BB84 protocol proposed in [2] defines a Quantum Transmitter (QTx) mapping randomly and privately selected pairs <bit, basis> (*qubit*) onto one linear State of Polarization (SOP), namely, Horizontal (H), Vertical (V), Diagonal (D) and Anti-diagonal (A). 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 randomly and privately selects a binary basis and measures the received photon according to this basis. If both QTx and QRx have chosen the same basis, the binary measurement of the photon in the QRx matches the bit sent by the QTx. With this method, both parties can privately share keys with those bits that matched the bases.

Key exchange includes *key distillation*, where modules running beside the QTx and QRx exchange a percentage of bits (10% as defined in [3]), so the module in the receiver can estimate the quantum Bit Error Rate (qBER) of the transmitted key. Keys with qBER higher than a defined threshold are discarded as they are assumed to be tampered by an eavesdropper.

Several eavesdropping attacks to polarization-based QKD systems can be found in the literature. The *intercept and resend* eavesdropping attack [4] is a type of individual attack that entails both measurement of intercepted photons and resending new photons, which requires the attacker to be equipped with the same QTx and QRx that are being utilized for the QKD system. Another individual attack is Photon Number Splitting (PNS) [5], which takes advantage of QTx based on weak-coherent pulse QTx. Finally, in the *collective and coherent* attack [6], the eavesdropper has access to spatial, temporal, and frequencies degrees of freedom physical properties of the photons that allow gaining information about the SOP, and thus, the keys. In this article, we target at detecting the intercept and resend attack performed between QTx and QRx, which requires less complex hardware for the attacker. For such attacks, different scenarios are considered where the eavesdropper has increasing knowledge and capabilities.

Authors in [7], proposed a high accurate method to detect eavesdropping, where resultant qBER of keys tampered by an eavesdropper is compared to that of untapped keys. However, since QTx needs to send photons with predefined bases, key distribution has to be paused whenever the detection is required, which noticeably reduces Key Exchange Rate (KER) of the QKD system. Authors in [8] proposed a slight modification of the polarization-encoded QKD protocol to permit the detection of eavesdropping activities by calculating the randomness of the bit sequence at the QRx after the key sifting procedure, where QTx and QRx discard bits with mismatched bases. The modification entails changing the randomness of the bit and basis selection in the QTx, which would also decrease final KER of the system.

However, many events during photon transmission through the channel can impact the measurements in the QRx, which would result into bases mismatches [9]. Specifically, polarization-encoded QKD can be degraded by SOP distortion

Manuscript received 5 February 2023; revised 21 May 2023; accepted 30 September 2023. Date of publication 3 October 2023; date of current version 4 March 2024. This work was supported in part by the European Commission through the HORIZON ALLEGRO project under Grant 101092766, in part by the AEI IBON under Grant PID2020-114135RB-I00 project, and in part by the ICREA Institution. *(Corresponding author: Luis Velasco.)*

The authors are with the Optical Communication Group, Advanced Broadband Communications Center (CCABA), Universitat Politècnica de Catalunya (UPC), 08034 Barcelona, Spain (e-mail: seyed.morteza.ahmadian@upc.edu; marc.ruiz-ramirez@upc.edu; jaume.comellas@upc.edu; luis.velasco@upc.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2023.3321774.

Digital Object Identifier 10.1109/JLT.2023.3321774

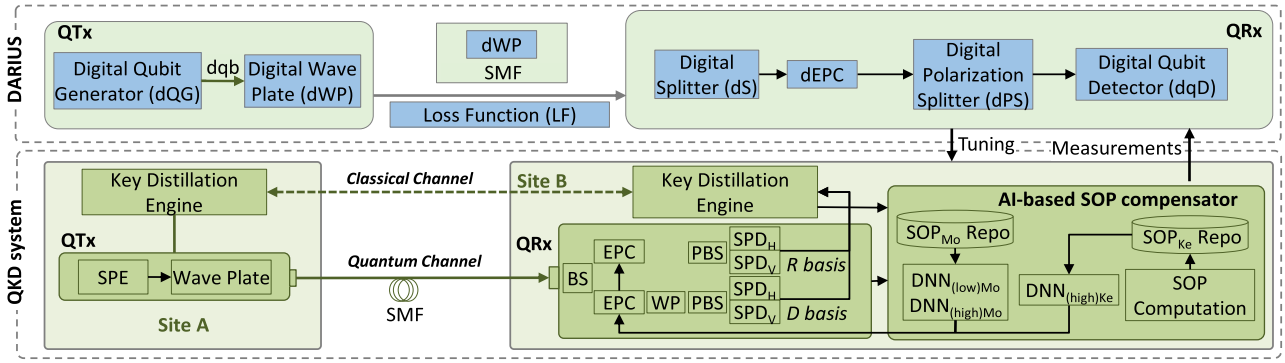

Fig. 1. DARIUS and the QKD system equipped with AI-based SOP compensator.

induced by the long fiber between QTx and QRx, as well as by environmental events occurred in the quantum channel. In continuous-variable QKD systems, methods for SOP compensation include Kalman filters, as proposed by the authors in [10]. In discrete-variable QKD systems, feedback-based methods for SOP compensation can be used, where normal key distribution is interrupted to send photons with known polarization during monitoring (*Mo*) intervals. In this way, Stokes parameters ($<S_0$, S_1, S_2, $S_3>$) representing the SOP of received photons are measured in the QRx, which can be used for SOP compensation. In particular, the authors in [3] send horizontally polarized photons during Mo intervals, which allowed to obtain partial SOP information only. Other authors (see, e.g., [11], [12]) proposed reactive methods to compensate for SOP random drift by performing multiple rotations based on qBER estimation. Authors in [13] added D SOP to be sent during Mo interval to compensate for qBER in both Rectangular (R) and Diagonal (D) bases.

In our previous paper [14], we proposed an improved compensation method based on Deep Neural Networks (DNN) that was able to predict the near future SOP based on the values measured during the last Mo intervals. However, that method assumed ideal conditions with perfectly calibrated optical components and thus, its performance might reduce in real deployments where optical components introduce unexpected photon loss, undesired polarization effects, and other non-ideal behaviors.

Digital twins can be helpful to improve QKD systems performance. In communications systems, digital twins have been proposed for fault management, as they can take advantage of data, models, and algorithms [15], [16]. In [17], we presented a preliminary design of a digital twin for polarization-encoded QKD systems, aiming at improving KER under environmental events. In this article, we go beyond and propose DARIUS, a novel digital twin for polarization-encoded QKD systems. DARIUS concatenates models of the optical components that form the QTx and QRx, as well as the fiber connecting them, to create a digital replica of the quantum channel. DARIUS includes methods to: *i*) discern eavesdropping from fiber stressing events without changing the randomness of <bit, basis> selection nor produce further key exchange interruption. The eavesdropping detection takes advantage of Mo intervals to monitor discrepancies in SOP, qBER, and KER between Mo and key exchange (Ke) intervals; and *ii*) help a DNN-powered compensation method to take counter actions against higher velocity events on the fiber.

The rest of the article is organized as follows. Section II presents the components in the quantum channel (qCh) and DARIUS use cases. Section III describes DARIUS's components. Then, proposed solutions for eavesdropping detection and higher velocity event compensation based on the information coming from key distillation are detailed. The discussion is supported by the results in Section IV. Finally, Section V draws the main conclusion of the work.

II. QKD and DARIUS's Opportunities

In this section, we first present specifications of qCh components including functionalities and imperfections. Next, opportunities in which DARIUS can take advantage to improve the QKD systems are presented, and three DARIUS's use cases are eventually introduced.

A. QKD System and qCh Components

We assume the qCh components presented in Fig. 1 (bottom), with a QTx and QRx connected through a Single Mode Fiber (SMF). The QTx includes a Single Photon Emitter (SPE) and a Wave Plate that changes photons' SOP as a function of the qubit to be transmitted. The SMF connecting QTx to QRx impacts the SOP and introduces photon loss and 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 between R and D basis for the QKD system.

Note that the BS can introduce photon loss through its arms [18]. Then, two Electronic Polarization Controllers (EPC) for each basis change the SOP with either tunable retardation or tunable orientation of its wave plates (internal characteristics of commercially available EPCs are not precisely specified by the manufacturers) [19]. These changes are used to compensate for SOP distortion through the fiber. 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 V polarized ones. The PBS also introduces photon loss through its arms. A wave plate between

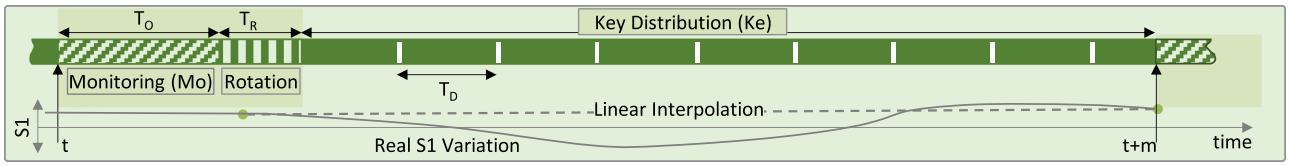

Fig. 2. Proposed interpolation method for high velocity events.

the EPC and PBS in the D basis is used to measure photons with D or A SOP. Next, a module with four Single Photon Detectors (SPD) counts photons. SPDs record more photons than the ones actually hitting them; the additional portion is known as *dark count rate*.

B. Opportunities and Use Cases for DARIUS

The architecture of DARIUS is presented in Fig. 1 (top), where each block models a counterpart optical component in the qCh. Then, the digital twin of the QKD system is defined as a concatenation of the digital qCh component models. DARIUS takes advantage of two repositories in the AI-based SOP compensator storing SOP measurements during Mo and Ke intervals (SOP_{Mo}_Repo and SOP_{Ke}_Repo).

As in [14], Mo intervals are assumed to track SOP fluctuations in case of fiber stressing events. Fig. 2 shows how keys exchange is interrupted and the QTx sends polarized photons during T_O, which the QRx can measure and tune its EPCs during T_R if needed. However, in addition to the proposed H SOP sent during Mo periods, the QTx needs to send D SOP to detect those SOP distortions aligned to the propagation direction of the transmitted photons. Note that any possible SOP evolution can be tracked by sending both H and D polarized photons. SOP trajectories starting from H and D are different but related by the universal rotation matrix [20], where a unique SOP distortion acts as a universal rotation matrix that converts H and D SOPs to SOPs with $S_{1(\mathrm{H})} = 1\text{-}2qBER_R$ and $S_{2(\mathrm{D})} = 1\text{-}2qBER_D$, respectively.

Mo intervals reduce KER of the QKD system and therefore, true Stokes measurements cannot be performed very frequently, which makes QKD systems especially vulnerable against episodes of large SOP variation which leads to large qBER and eavesdropping become indistinguishable. Nonetheless, the distillation process can provide useful information of the Stokes parameters, derived from the qBER estimation of the sifted keys. Particularly, the actual value of $S_{1(H)}$ and $S_{2(D)}$, as well as the absolute value of $S_{2(H)}$, $S_{3(H)}$, $S_{1(D)}$, and $S_{3(D)}$ can be obtained from the qBER estimations during the key distillation process, without the need of real monitoring. In this regard, large keys would produce more precise qBER estimations at the expense of increasing the time to obtain them. Hence, the length of the keys needs to be studied.

Apart from the length of the keys, the distance between QTx and QRx plays a major role in the time of SOP estimation during Ke intervals. For illustrative purposes, Fig. 3 shows the workflow of the key exchange process. At the qCh, QTx (Alice) randomly generates bases and bits to prepare the polarized photons for emission (labeled 1 in Fig. 3), whereas the bases will be used

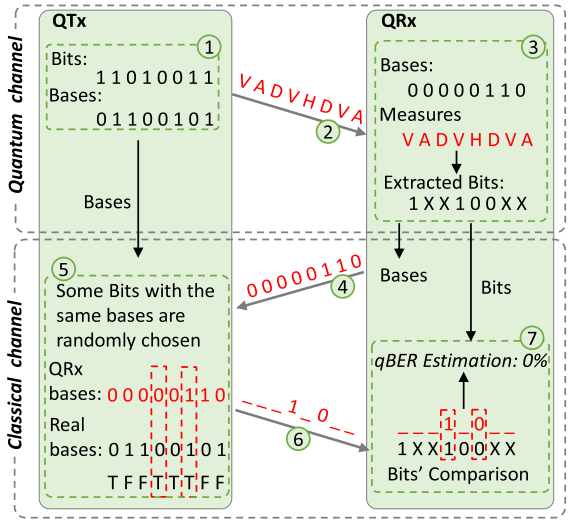

Fig. 3. QBER estimation in the QRx based on the BB84 protocol.

for key distillation. Once photons are received (2) and measured by the QRx (Bob), bits are extracted based on their bases (3). Xs are used for extracted bits with mismatched bases in Fig. 3. Next, Bob sends the bases to Alice for raw key reconciliation (4), so Alice is able to detect bits with matched bases (5). Now, Alice sends some randomly chosen bits with matched bases to Bob (6) for qBER estimation (7). Hence, two-way transmission is needed for qBER estimation and the distance between QTx and QRx should be studied.

Several use cases can be defined that take advantage of DARIUS, e.g.,: 1) DARIUS can optimize the QKD system by adjusting the tunable parameters of the optical components before starting key distribution. The tunable parameters in the qCh are related to the wave plate in the QTx, as well as the EPC and SPDs in QRx. Tunable parameters in the SPDs are delay, dead time, gate width, detection mode and quantum efficiency. Armed with measurements gathered from the qCh, DARIUS can provide the needed adjustments of the optical components to eventually increase KER; 2) DARIUS can distinguish between eavesdropping and excessive qBER, which will allow to continue with the key exchange in case of the latter. The SOP evolution is traceable when events caused by human operator works or environmental conditions affect the optical fiber. In contrast, eavesdropping results into unrecognizable SOP changes [14]. Measurements taken from SOP trajectory repositories both during Mo and Ke intervals help DARIUS to detect eavesdropping; and 3) DARIUS can configure the AI-based SOP compensator in the QRx to take proper countermeasure actions against environmental events.

TABLE I
NOTATION

α_x	Phase difference w.r.t horizontal electric field (rad)
α_y	Phase difference w.r.t vertical electric field (rad)
θ	Orientation angle (rad)
$\|\Psi_{DQ}\rangle$	Quantum state of Digital qubit
φ	Phase retardation (rad)
dq_Tx	Digital qubit transmission
dR	Digital reflection
dT	Digital transmission
$Loss_{op\_comp}$	Optical component loss (%)
$qBER_{(\cdot)}$	qBER in: Mo/Ke interval or R/D bases (%)
m	Time between two consecutive Mo intervals (s)
T_O	Time needed to measure SOP during Mo intervals (s)
T_R	Time needed to perform rotation in QRx (s)
T_D	Time between SOP measurement in Ke intervals (s)
T_{tr}	Transmission time between QTx and QRx (s)
T_{comp}	Computation time for SOP estimation (s)

Environmental events introduce fluctuations on the SOP of transmitted photons with differential velocity as discussed in [14]. In this case, the DNN model under operation in the SOP compensator ($DNN_{Low(Mo)}$) is not able to foresee the SOP of incoming photons. Therefore, another DNN model trained for higher velocity events ($DNN_{High(Mo)}$) is needed. DARIUS can detect the increased SOP velocity and change the model under operation, which would increase KER by SOP distortion compensation in different environmental conditions.

III. DARIUS Specification and Intelligence

In this section, we show how DARIUS improves the performance of the QKD system by discerning eavesdropping from high qBER, as well as taking actions against diverse environmental conditions. We first present the proposed components, which provide a *digital* representation of qCh components. Next, the procedure to detect eavesdropping and differentiate it from high qBER is described. Finally, algorithms to dynamically address high qBER due to SOP fluctuation having different velocity are presented. Table I summarizes the notation that is consistently used along the rest of the article.

A. qCh Models

This section presents models to create a digital representation of the qCh components [17]: *i*) the digital Qubit Generator (dQG) and the digital wave plate (dWP) modeling the physical SPE and the wave plate; *ii*) the SMF model; and *iii*) digital components for the QRx, i.e., digital splitter (dS), digital EPC (dEPC), digital polarization splitter (dPS) and digital qubit detector (dqD).

The dQG generates digital qubits (dqb) modeling their quantum states as (1), where α is the phase with respect to orthogonal electric field (x,y) components polarized with orientation angle θ [21]. Here, the quantum state perfectly matches the SOP of emitted photons.

$$|\psi_{dq}\rangle = \begin{pmatrix} \cos(\theta) \times e^{i\alpha_x} \\ \sin(\theta) \times e^{i\alpha_y} \end{pmatrix} \quad (1)$$

The dWP acts as a quantum gate and it affects the generated dqb in the same way that an optical wave plate changes the SOP of a photon. Equation (2) models the quantum gate with orientation angle θ and phase retardation φ of the wave plate [22].

$$dWP_\theta(\varphi) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (2)$$

where,

$$a = e^{i\varphi/2}\cos^2(\theta) + e^{-i\varphi/2}\sin^2(\theta) \quad (3)$$

$$b = c = -i\sin(2\theta) \times \sin(\varphi/2) \quad (4)$$

$$d = e^{-i\varphi/2}\cos^2(\theta) + e^{i\varphi/2}sin^2(\theta) \quad (5)$$

The SMF is modeled by using a dWP, which changes the SOP in the same way that birefringence in the fiber affects the photons. In addition, a loss function (LF) discards dqbs with a probability inversely proportional to the loss rate of optical components (6).

$$P(dq\_Tx) = 1 - Loss_{op\_comp} \quad (6)$$

In the digital QRx, a digital splitter (dS) receives dqbs and randomly outputs them through the digital reflection (dR) or digital transmission (dT) with equal probability.

The dEPC is modeled as three dWPs, where the orientation angles (θ_1, θ_2, θ_3) are derived from the input and output SOP [23]. Equation (7) computes the required quantum gates for a fixed-retardation EPC using the matrix multiplication of the dWPs.

$$dEPC = dWP_{\theta_1}(\pi/2) \cdot dWP_{\theta_2}(\pi) \cdot dWP_{\theta_3}(\pi/2) \quad (7)$$

Next, the digital polarization splitter (dPS) receives dqbs and outputs them through the dR or dT based on its quantum state (8) and (9). Finally, the dqD receives P(dR) and P(dT) and adds dark counts based on physical dark count rates.

$$P(\text{dR}) = P(H) = \cos^2(\theta) \quad (8)$$

$$P(\text{dT}) = P(V) = \sin^2(\theta) \quad (9)$$

Table II summarizes the purpose of the qCh models and their tunable parameters.

B. Eavesdropping Detection and Excessive qBER Compensation

DARIUS collects measurements from the qCh and determines whether it stops the key distribution if eavesdropping is detected or continues the key distribution with fine SOP monitoring. In this article, we assume that the eavesdropper has no control over QTx and QRx qCh components, and explore three scenarios for eavesdropping: *i*) the eavesdropper has no knowledge about Mo intervals or he/she cannot perfectly synchronize with them (*scenario 1*), so any tampering would result in S_0 values noticeably lower than 1; *ii*) the eavesdropper has detected Mo intervals and he/she can insert photons with the right polarization during Mo periods (*scenario 2*). In this case, discrepancies in $qBER_{Mo}$ and $qBER_{Ke}$ values will reveal eavesdropping; and *iii*) the eavesdropper recognizes the strategies for eavesdropping detection and tries to conceal the attack by aligning the discrepancies

TABLE II
DARIUS MODELS AND TUNABLE PARAMETERS

qCh Model	Purpose	Tunable Parameters
dQG	state initialization	θ, α_x, α_y
dWP	state adaptation	SOP distortion of emitted photons
SMF	Apply fiber impacts (distortion, optical loss) on dqb's state	Fiber length and SOP distortion
LF	Apply optical components' loss	$Loss_{op\_comp}$
dS	Reflect or transmit the dqb (50%, 50%)	Photon loss in each arm
dPS	Reflect or transmit the dqb based on the state	Photon loss in each arm
dEPC	Apply EPC's impact to the state	Wave plates variables
dqD	Store qubit's probability in a repository	Dark count rate

in qBER and KER during Mo and Ke intervals, together with emulating a SOP evolution to keep S_0 close to 1 (*scenario 3*). In this case, DARIUS eavesdropping detection is based on the fact that SOP trajectories starting from H and D polarization are related by the universal rotation matrix [20].

Let us first analyze the effect of eavesdropping in scenario 1. In a QKD system, eavesdropping consists in taking photons, measuring them, and injecting new photons in the channel using extracted bits from its measurements. For the sake of simplicity, in this article, we also consider that tampering is performed at a location close to the QTx in site A, which theoretically is the best place for eavesdropping since the remaining optical fiber until the QRx could mask the attack. Because at photon transmission time only the QTx knows the true basis used to polarize a photon, the eavesdropper has to choose its own basis, e.g., randomly. Such decisions impact on the value of S_0, which takes values not that close to 1. Note that during Mo intervals, $S_{1(H)}$ and $S_{2(D)}$ are related to *qBER* in R and D bases when input SOPs are H and D, respectively. S_0 can be computed as (10), which should be equal to one, whereas qBER during Mo period ($qBER_{Mo}$) can be computed as (11) [12].

$$S_0 = \sqrt{S_1^2 + S_2^2 + S_3^2} \tag{10}$$

$$qBER_{\mathrm{Mo}} = \frac{1}{2} \times \left(\frac{1 - S_{1(\mathrm{H})}}{2} + \frac{1 - S_{2(\mathrm{D})}}{2} \right) \tag{11}$$

In scenario 2, differences between $S_{1(H)}$, $S_{2(D)}$, qBER and KER measured and estimated during Mo and Ke periods, allow eavesdropping being distinguishable from high qBER. During the Ke period, $qBER_{Ke}$ can be computed by averaging the partial ones from R and D bases, denoted $qBER_R$ and $qBER_D$ (12), while $qBER_{(\mathrm{R/D})}$ can be obtained from counted photons in the SPDs (13).

$$qBER_{\mathrm{Ke}} = \frac{1}{2} \times (qBER_{\mathrm{R}} + qBER_{\mathrm{D}}) \tag{12}$$

$$qBER_{(\cdot)} = \frac{\#\text{photons SPD}_{\mathrm{V}(\cdot)}}{\#\text{photons SPD}_{\mathrm{V}(\cdot)} + \#\text{photonsSPD}_{\mathrm{H}(\cdot)}} \tag{13}$$

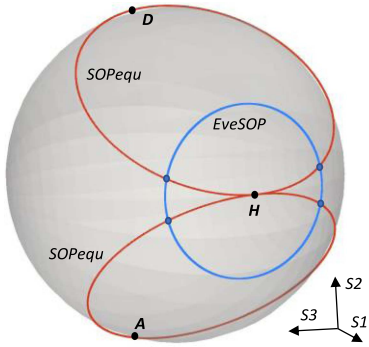

Fig. 4. SOPequ and EveSOP circles on the Poincaré sphere.

In scenario 3, received photons will be equally split in R and D bases, as the eavesdropper intercepts and resends photons in Ke intervals with random bases. This results in similar $S_{1(H)}$ and $S_{2(D)}$ values, coming from measured $qBER_R$ and $qBER_D$.

To cover up the attack, the eavesdropper needs to emulate SOP changes in Mo intervals, so that $S_{1(H)} \approx S_{2(D)}$. However, $qBER_R$ (when H polarized photons are sent) and $qBER_D$ (when D polarized photons are sent) in Mo intervals would be similar only if the emulated SOP changes make SOP_H (SOP_D) to be in one of the two perpendicular circles (*SOPequ*) on the Poincaré sphere that include the reference (i.e., H (D)), as well as A or D (H or V) polarizations (see Fig. 4). However, SOP_H and SOP_D measured in the Mo interval corresponding to a specific eavesdropping rate will be on a circle parallel to S2-S3 and S1-S3 plane (*SOPeve*) on the Poincaré sphere, respectively. DARIUS detects eavesdropping if the eavesdropper makes SOP changes that result in SOP points different than the intersection points between SOP*eve* and SOP*equ* circles. In the case the eavesdropper performs SOP changes that result in one of the four intersection points, DARIUS cannot determine whether there is an attack. However, because the probability to measure equal $qBER_R$ and $qBER_D$ in several consecutive Mo intervals with SOP variations is really low under no attack conditions, DARIUS will stop the key exchange if that event happens.

Let us now analyze why the method to compensate for fiber stressing events in [14] is not able to reduce *qBER* under higher velocity events that produce large SOP variations. Fig. 2 illustrates a possible S_1 evolution between two Mo intervals (continuous line in Fig. 2) and the linear interpolation (dotted lines). Using the latter to plan the rotations between the two Mo intervals [t, t+m] would result in that such rotations would not only not improve the *qBER* but also highly reduce *KER* in case of large SOP variations. In contrast, our proposal for *qBER* compensation is based on using information from the key distillation process to estimate the evolution of SOP between two Mo intervals, which will be applied to compute a much more accurate rotation plan.

Assuming the QRx architecture in Fig. 1, the QRx can use the Mo intervals history, as well as the estimation of $\mathrm{SOP_H}$ and $\mathrm{SOP_D}$ computed between Mo intervals in case of high velocity events, i.e., during Ke intervals, to improve the SOP compensation. Note that such estimation can be performed with a shorter

Algorithm I: SOP_{Ke} Estimation.

INPUT: $qBER_R$, $qBER_D$
OUTPUT: SOP_{Ke}
1: $S_{1(H)} \leftarrow 1 - 2\times qBER_R$
2: $S^+{}_{2(H)} \leftarrow \text{sqrt}(2 \times qBER_D \times (1+S_{1(H)}))$
3: $S^+{}_{3(H)} \leftarrow \text{sqrt}(1-(S_{1(H)})^2-(S^+{}_{2(H)})^2)$
4: $S^+{}_{1(D)} \leftarrow \text{sqrt}(2 \times qBER_D \times (1+S_{1(H)}))$
5: $S_{2(D)} \leftarrow 1 - 2\times qBER_D$
6: $S^+{}_{3(D)} \leftarrow \text{sqrt}(1-(S_1{}^+{}_{(D)})^2-(S_{2(D)})^2)$
7: **return** $[<S_{1(H)}, S^+{}_{2(H)}, S^+{}_{3(H)}>, < S^+{}_{1(D)}, S_{2(D)}, S^+{}_{3(D)}>]$

Algorithm II: Eavesdropping Detection and SOP Compensation.

INPUT: $qBERequ$, SOP_{Mo}_Repo, SOP_{Ke}_Repo, $qBER_{Mo}$, avg_$qBER_{Ke}$
OUTPUT: *eaveDetected*, *rotationPlan*
1: $last\_SOP_{Mo} \leftarrow SOP_{Mo}\_Repo.getCurrent()$
2: $S_0 \leftarrow$computeS0($last\_SOP_{Mo}$)
3: $S1(H) \leftarrow 1 - 2\times qBERMo[\text{R}]$
4: $S2(D) \leftarrow 1 - 2\times qBERMo[\text{D}]$
5: **if** $S_0 < 1 - Eve\_S0thr$ OR $qBER_{Mo}$ - avg_$qBER_{Ke} > Eve_qBERthr$ OR ($S1(H) \approx S2(D)$ AND $last\_SOPMo[\text{H}] \notin SOPequ$) **then**
6: **return** <true, ->
7: **if** $S1(H) \approx S2(D)$ AND NOT $SOPMo\_Repo.SOPisConstant()$ **then**
8: $qBERequ$ ++
9: **if** $qBERequ >$ maxEQU **then return** <true, ->
10: **else** $qBERequ \leftarrow 0$
11: **if** avg_$qBER_{Ke} > 0.1$ AND $S_{1(H)}$.velocity > $velocity\_thr$ **then**
12: $interm\_SOPs_{Ke}$ $\leftarrow$DNN$_{(\text{high})\,Ke}$.predict(SOP_{Ke}_Repo)
13: $next\_SOP_{Mo}$ $\leftarrow$DNN$_{(\text{high})\,Mo}$.predict(SOP_{Mo}_Repo)
14: $trajectory \leftarrow$ linearInterpol($last\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, $next\_SOP_{Mo}$)
15: **else**
16: $next_SOP_{Mo} \leftarrow$DNN$_{(\text{low})\,Mo}$.predict(SOP_{Mo}_Repo)
17: $trajectory \leftarrow$ linearInterpol($last\_SOP_{Mo}$, $next\_SOP_{Mo}$)
18: **return** <false, *rotationAndTracking*(*trajectory*)>

period (T_D in Fig. 2). Rotations computed using predictions from either low or high velocity DNN models and from Mo and Ke intervals are applied by the EPCs to compensate for the SOP distortion of the received photons before being counted by the H and V SPDs in the R and D bases.

It is worth mentioning that different EPCs are being used in R and D bases in polarization-encoded QKD systems [24], which entails applying different rotations to compensate for SOP distortion. DARIUS is the responsible for switching between low or high DNN models, in operation in the AI-based SOP compensator, once no eavesdropping evidence is observed. Switching decision is made by measuring the speed of $S_{1(H)}$ and $S_{2(D)}$ once qBER exceeds a threshold.

C. DARIUS Intelligence

Let us now detail the different algorithms that provide intelligence to DARIUS. First, Algorithm I is used to estimate SOP_{Ke}. This algorithm is used by other algorithms, as well as to update the repository every T_D ms. 10% of the last sifted key are used to estimate S_1, abs(S_2), and abs(S_3) for H input SOP and abs(S_1), S_2, and abs(S_3) for D input SOP [13].

DARIUS includes Algorithm II for eavesdropping detection and SOP compensation, which is run every Mo interval. The algorithm takes as input *qBERequ* counter storing the number of consecutive intervals with equal $qBER_R$ and $qBER_D$, a reference to SOP_{Mo}_Repo and SOP_{Ke}_Repo, the value of $qBER_{Mo}$ in the current Mo interval and avg_qBER_{Ke} averaging *qBER* captured every T_D ms in the last Ke interval. SOP in the current Mo interval is retrieved from the Mo repository and used to compute S_0, whereas $S_{1(H)}$ and $S_{2(D)}$ are computed from $qBER_{Mo}$ components (lines 1–4). Next, the eavesdropping scenarios defined in Section III-B are analyzed (lines 5–6). For the first and second eavesdropping scenarios, S_0 amplitude together with $qBER_{Mo}$ and avg_qBER_{Ke} values are checked. For the third eavesdropping scenario, $S_{1(H)}$ and $S_{2(D)}$ are compared and measured SOP_H is checked to be in SOP*equ*. If no eavesdropping is detected, variation of SOP is checked in case of being $S_{1(H)}$ and $S_{2(D)}$ equal and the counter of consecutive Mo intervals is increased; eavesdropping is detected in case the counter exceeds some predefined value (lines 7–10).

If no eavesdropping is detected but avg_qBER_{Ke} is over the threshold, the velocity of $S_{1(H)}$ is measured and compared to the threshold (*velocity_thr*). If both thresholds are exceeded, high velocity DNN models, DNN$_{(\text{high})\text{Mo}}$ and DNN$_{(\text{high})\text{Ke}}$, fed with measured SOP$_{\text{Mo}}$ and last estimated SOP$_{\text{Ke}}$ are used to predict the SOP of the next Mo interval, as well as the evolution of SOP between the current and the next Mo intervals considering SOP_{Ke} values (lines 11–14). Otherwise, low velocity DNN models, DNN$_{(\text{low})\text{Mo}}$, are used to predict the SOP for the next Mo interval and linear interpolation of current and predicted SOPs is computed and used to produce the rotation plan (lines 15–17). Recall that measured SOP during Ke intervals return only the absolute values of $S_{2(H)}$, $S_{3(H)}$, $S_{1(D)}$ and $S_{3(D)}$. Those values are used to feed as inputs of an additional DNN model that predicts absolute values of SOP_{Ke} Stokes parameters for the next Ke period. Also, rotation plans are different in R and D bases. Then, the rotation plan includes the needed reversal rotations to track SOP thus, ensuring that the right trajectory is being followed. Lost photons of reversal rotations and wrong signs' selection must be considered in the results.

The interpolation method used in Algorithm II (Method 1) needs at most four reversal rotations performed by the EPC for each predicted SOP_{Ke} to reveal the sign of the Stokes parameters. After each reversal rotation $qBER_R$ and $qBER_D$ should be checked. As explained before, QRx needs to wait

Algorithm III: Interpolation of the Rotation Plan (Method 2).

INPUT: $last\_SOP_{Mo}$, $next\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, m
OUTPUT: *trajectory*
1: $counter = 1$
2: **for each** SOP_{Ke} IN $interm\_SOPs_{Ke}$ **do**
3: **if** $counter \times T_D < m/2$ **then**
4: sign($SOP_{Ke}[S_2]$)←sign($last\_SOP_{Mo}[S_2]$)
5: sign($SOP_{Ke}[S_3]$)←sign($last\_SOP_{Mo}[S_3]$)
6: **else**
7: sign($SOP_{Ke}[S_2]$)←sign($next\_SOP_{Mo}[S_2]$)
8: sign(SOP_{Ke} $[S_3]$)←sign($next\_SOP_{Mo}[S_3]$)
9: $counter \leftarrow counter + 1$
10: **return** linearInterpol($last\_SOP_{Mo}$, $interm\_SOPs_{Ke}$, $next\_SOP_{Mo}$)

Algorithm IV. Interpolation of the Rotation Plan (Method 3).

INPUT: *trajectory*, $next\_SOP_{Ke}$, $qBER_{R,}$, $qBER_{D,}$, *intrpol_thr*
OUTPUT: *newtrajectory*
1: **if** avg($qBER_{R,}$, $qBER_D$) > *intrpol_thr* **then**
2: SOP_{Ke}←estimate_SOP_{Ke}($qBER_R$, $qBER_D$) (Algorithm I)
3: **while** $qBER_{Ke} > 0.5\%$ **do**
4: SOP_{Ke}←sign assumption for SOP_{Ke}
5: perform reversal rotation
6: $qBER_{Ke}$← avg($qBER_{R,}$, $qBER_D$)
7: **return** linearInterpol(SOP_{Ke}, $next\_SOP_{Ke}$)
8: **return** *trajectory*

until all photons of the key are received, as well as the transmission time of Bob's bases (T_{tr}) and Alice's samples (T_{tr}) to estimate $qBER_R$ and $qBER_D$. In consequence, the longer the distance between Alice and Bob, the later the estimated qBER is available for the rotation plan. Moreover, the time for SOP computation from the estimated qBERs in Algorithm I (T_{comp}) needs to be considered. Checking the signs of estimated SOP every T_D would entail losing photons to configure the EPC, as well as when the assumed signs are wrong. In view of this, two alternative interpolation methods to minimize the frequency of checking the signs have been investigated.

Algorithm III details method 2, where the Stokes parameters' sign in $next\_SOPs_{Ke}$ are assigned similar to either measured SOP in the last Mo interval or predicted SOP for the next Mo interval based on the one closer in terms of time (lines 1–9). After sign assignments, linear interpolation is used to predict the evolution of SOP between the current and the next Mo intervals considering SOP_{Ke} values (line 10). Although this method entails no stokes parameters' sign check, its performance can be poor and result in high qBER.

Algorithm IV describes method 3 for interpolation of the rotation plan, which is a tradeoff between checking the signs and high qBER. We use the rotation plan computed in Algorithm III as the default plan. In case the average of $qBER_R$ and $qBER_D$ in the Ke interval is higher than the threshold (*intrpol_thr*), current SOP is estimated using Algorithm I (lines 1–2). Then reversal rotations for checking the signs are performed (lines 3–6). Recall that QRx needs to wait ($3*T_{tr}+ T_{comp}$) after each reversal rotation to compute the $qBER_{Ke}$ (line 6). If the $qBER_{Ke}$ is low enough (under 0.5%), there is no need to check more signs, and the compensational rotations till the next predicted SOP_{Ke} will be linearly planned (line 7).

TABLE III
QCH'S COMPONENTS IMPERFECTIONS (BASED ON [17], [25])

qCh component	Imperfection
BS & BPS	100 photons lost in each arm out of 2,500
SMF	Different bending radius results into different SOP change
SPD	Dark count rate of 3% (integration time and quantum efficiency were 0.1 second and 10% respectively)

IV. RESULTS

In this section, we first present our simulation environment and then, we show DARIUS's capability to detect eavesdropping and improve the QKD system. The non-ideal behavior of qCh components was previously verified on an experimental testbed setup in [17], [25]. In this article, we assume those imperfections, which are summarized in Table III.

A. Simulation Environment

The architecture of DARIUS and the QKD system presented in Fig. 1 have been evaluated on a simulation environment developed in Python, using IBM's Qiskit development tools [26]. In particular, we assume decoy-state based SPE [27] and waveplates to polarize photons in the QTx and the SPD in [28] in the QRx. The simulator implements DARIUS specifications and intelligence as described in Section III, i.e.,: *i*) models that mimic qCh components behavior; *ii*) a light key distillation engine that computes the $qBER_R$ and $qBER_D$ from sifted keys; *iii*) DNN models for SOP predictions; *iv*) the algorithms for eavesdropping detector and high velocity event compensator; and *v*) an optical simulator for the QKD system. Emulated events using the experimental datasets in [29] impact the QKD system assuming a 50 km optical channel.

In line with [27], [28], we assume photon generation and detection rate of 100 Mb/s, regular BB84 with sifted KER of 45%, and privacy amplification rate of 10% [30]. As a result, a nominal KER of 4.5 Mb/s (100∗45%∗10% Mb/s) can be achieved with these specifications, in the absence of SOP perturbations and eavesdropping.

All three DNN models, i.e., $\text{DNN}_{(\text{low})\text{Mo}}$, $\text{DNN}_{(\text{high})\text{Mo}}$ and $\text{DNN}_{(\text{high})\text{Ke}}$, include four hidden layers with 400, 200, 50, and 10 neurons each with the tanh activation function. $\text{DNN}_{(\text{low})\text{Mo}}$,

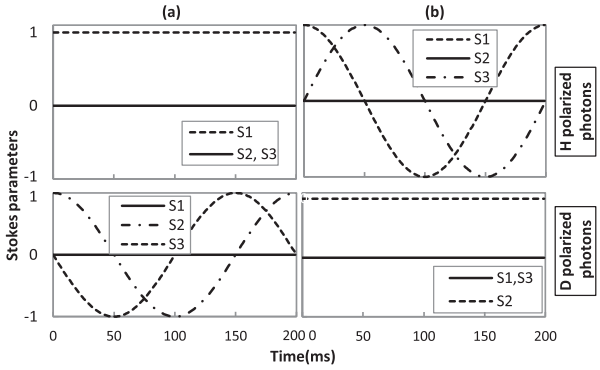

Fig. 5. Measured SOP evolution during S_1 (a) and S_2 axis rotation.

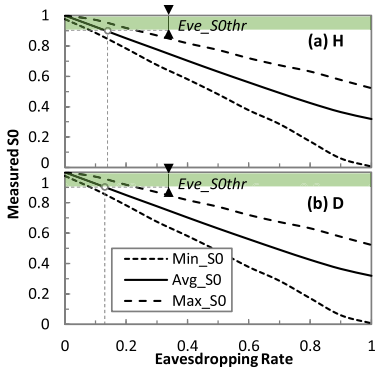

Fig. 7. Eve detection under scenario 1 w.r.t. R (a) and D (b) bases.

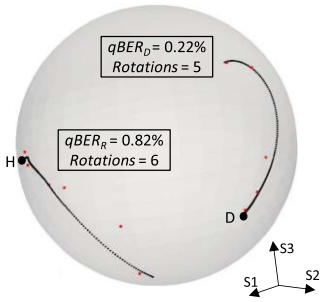

Fig. 6. SOP trajectories and rotation plans w.r.t. R and D bases.

$\text{DNN}_{(\text{high})\text{Mo}}$ models have 80 inputs coming from 10 consecutive Mo intervals, where sine and cosine of the orientation angle and phase retardation from H and D SOPs are collected. The $\text{DNN}_{(\text{high})\text{Ke}}$ model has 400 inputs, coming from 50 consecutive Ke intervals. The output of the $\text{DNN}_{(\text{low})\text{Mo}}$ and $\text{DNN}_{(\text{high})\text{Mo}}$ are the predicted H and D SOPs in the next Mo interval, whereas that of the $\text{DNN}_{(\text{high})\text{Ke}}$ is the predicted H and D SOPs of the next 4 Ke intervals.

DNNs are trained off-line before starting the key distribution with 3×10^6 samples. The SOP_{Mo}*_Repo* includes measured SOP_{Mo} during the last 10 consecutive Mo intervals and the SOP_{Ke}*_Repo* contains all $SOP_{Ke} = [<S_{1(H)}, \text{abs}(S_{2(H)}), \text{abs}(S_{3(H)})>, <\text{abs}(S_{1(D)}), S_{2(D)}, \text{abs}(S_{3(D)})>]$ estimated every T_D during the last 10 Mo intervals.

B. Reference SOPs in Mo Intervals

Fig. 5 illustrates why only H or D reference SOPs sent by the QTx would not enable the QRx to detect aligned distortion to the propagation axis of transmitted photons. Fig. 5(a) shows the evolution of the Stokes parameters when the QTx sends H and D SOPs, while Poincaré sphere rotates along S_1 axis. SOP evolution is not distorted when the QTx sends H polarized photons, but it is clearly distorted in the case of D polarized ones. The opposite effect on the SOP is observed in Fig. 5(b), when Poincaré sphere rotates along S_2 axis; here H polarized photons enable the QRx to detect the distortion.

Fig. 6 illustrates 0.1s of a low velocity fiber stressing event applied to the qCh considering both R and D bases in the QRx. We observe that SOP trajectories (lines) in R and D bases are clearly different. As the velocity of the event is low, using $\text{DNN}_{(\text{low})\text{Mo}}$ and linear interpolation for the rotation plan (as proposed in [14]) results in good performance since the QRx can predict both trajectories and plan and apply corresponding reversal rotations. Note that rotations (dots) are being applied at different times by the EPCs installed in R and D bases, and the resulting qBER and number of rotations is also different, as shown in Fig. 6.

C. Eavesdropping Detection and Excessive qBER

Let us now evaluate eavesdropping detection and high velocity events compensation methods for the scenarios discussed in III.B. For the sake of generality, let us consider different *eavesdropping rate* computed as ratio of the transmitted photons that are actually tampered by the eavesdropper.

Under scenario 1, Fig. 7 shows how different eavesdropping rates impact on the value of S_0 measured in Mo intervals. For each rate, all possible SOP distortions of the transmitted photons before eavesdropping are evaluated. Photons with less linear SOP are slightly less helpful for revealing the eavesdropper and vice versa, so, average, minimum and maximum S_0 values are plotted. Even extremely distorted photons reaching the eavesdropper disclose tampering in the channel after being measured by the QRx. Assuming *Eve_S0thr* = 0.1 (which is actually a very large threshold), even eavesdropping rates as moderate as 14% can be detected. Because, the QTx sends H and D polarized photons in Mo intervals to enable QRx to track all sorts of distortions in the qCh, measured S_0 of the received photons in Mo intervals with either polarization is similarly decreased due to the eavesdropping actions.

Fig. 8 shows eavesdropping detection under scenario 2. $S_{1(H)}$ and $S_{2(D)}$ are measured in both Mo and Ke intervals. In the considered set-up (50 km), T_{Tr} would be about 250 μs and $T_{SOP\cdot Est} = 500$ μs (round-trip time). We also consider $T_{comp} = 50$ μs. Then, total time for SOP estimation is about 550 μs, which is short enough to allow the QRx to estimate $S_{1(H)}$ and $S_{2(D)}$ every 10ms. We observe that the values of $S_{1(H)}$ in Fig. 8(a) and $S_{2(D)}$ in Fig. 8(b) clearly drop when the eavesdropper tampers the qCh, which enables eavesdropping detection. Such behavior can be analyzed together with the difference between

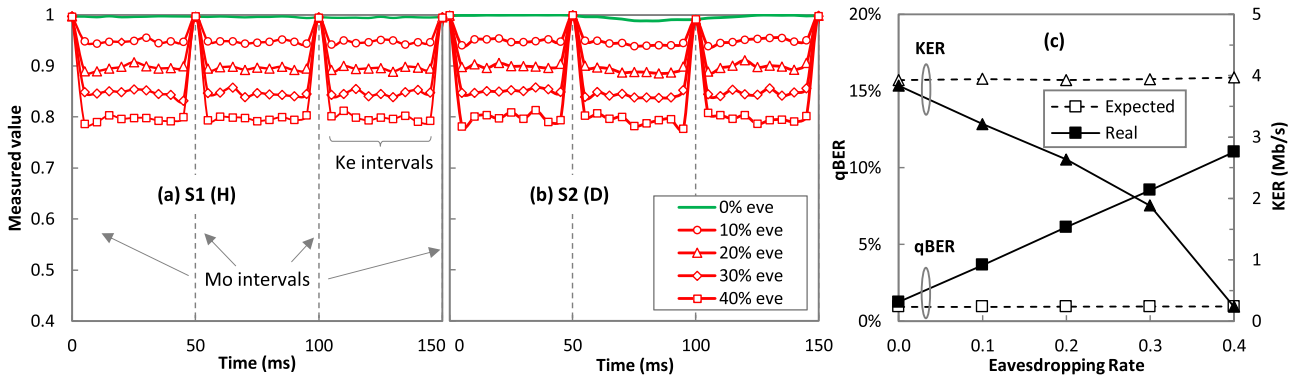

Fig. 8. Eve detection under scenario 2 w.r.t. R (a) and D (b) bases. qBER and KER evolution vs. eavesdropping rate (c).

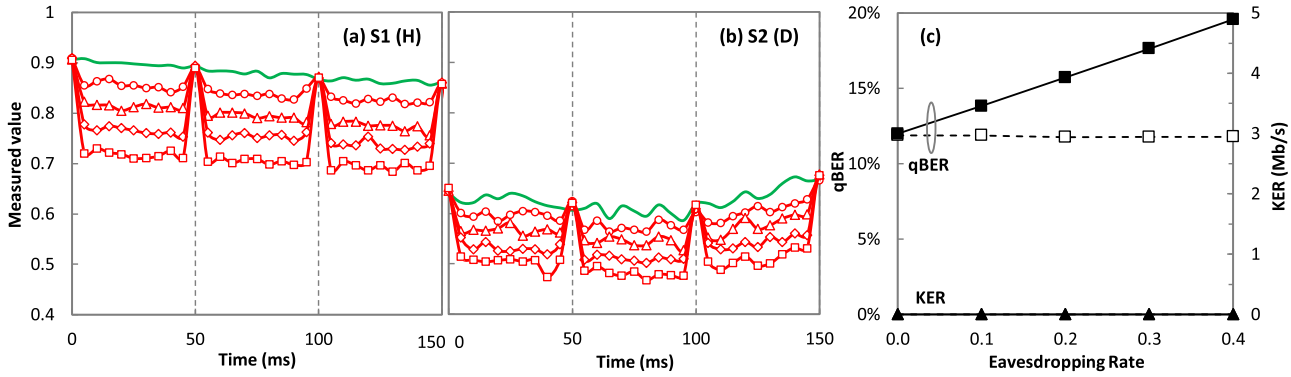

Fig. 9. Eve detection together with an environmental event under scenario 2 w.r.t. R (a) and D (b) bases. qBER and KER evolution vs. eavesdropping rate (c).

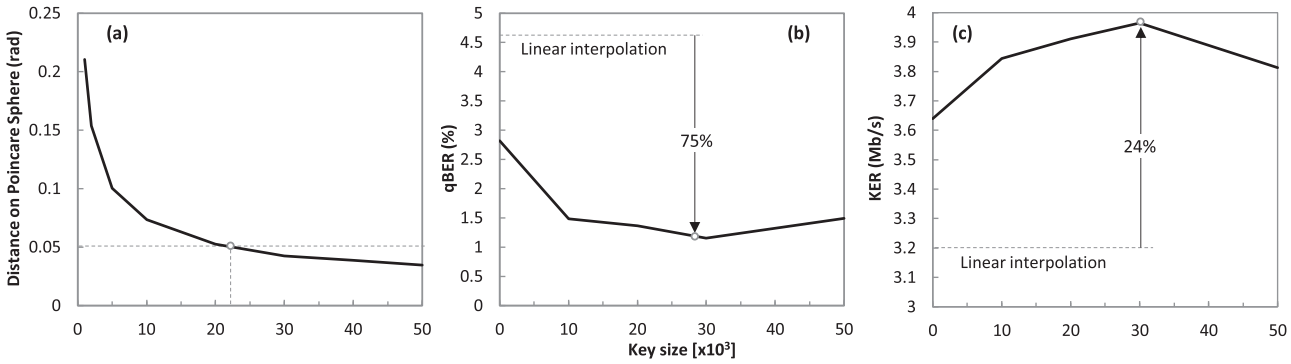

Fig. 10. Precision of SOP_{Ke} estimation (a), compensation performance w.r.t. qBER (b), and KER (c) in a B2B scenario.

expected $qBER_{Mo}$ and $qBER_{Ke}$ versus the real ones (Fig. 8(c)). Considering $Eve\_qBERthr = 2\%$, the analysis clearly reveals eavesdropping even with only 10% eavesdropping rate. Note also that KER significantly reduces when the eavesdropping rate increases following qBER increment, which could lead to false diagnosis if SOP measurements in Ke intervals are not analyzed.

Fig. 9 complements the previous study in the presence of an environmental event affecting the qCh. Even in this case, $S_{1(H)}$ (Fig. 9(a)) and $S_{2(D)}$ (Fig. 9(b)) values can still disclose the eavesdropping actions in the channel. In this case, qBER is higher than the qBER threshold (10%) and keys are discarded. However, qBER estimation during key distillation can show that $qBER_{Mo}$ and $qBER_{Ke}$ (expected and real $qBER$) are clearly different (Fig. 9(c)). Therefore, considering Eve_qBERthr = 2%, as in the case where no environmental events affected the qCh, eavesdropping rates as low as 10% can be detected.

Let us now analyze the case of high qBER coming from high velocity events. For this analysis, we assume a back-to-back (B2B) set up. Let us first analyze the influence of the size of the keys on the precision of the SOP estimation during Ke periods (Fig. 10(a)). We observe that keys longer than 22k photons result in very precise SOP estimation using key distillation information. Fig. 10(b) and (c) show the performance of the method of interpolation described in Algorithm II. In Fig. 10(b)

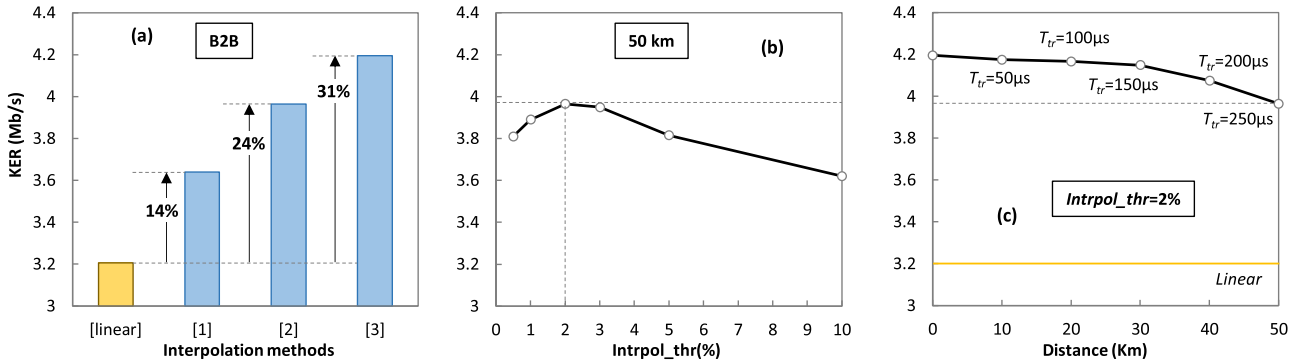

Fig. 11. Comparison of compensation methods (a) and the performance of compensation method 3 w.r.t the threshold (b) and distance (c).

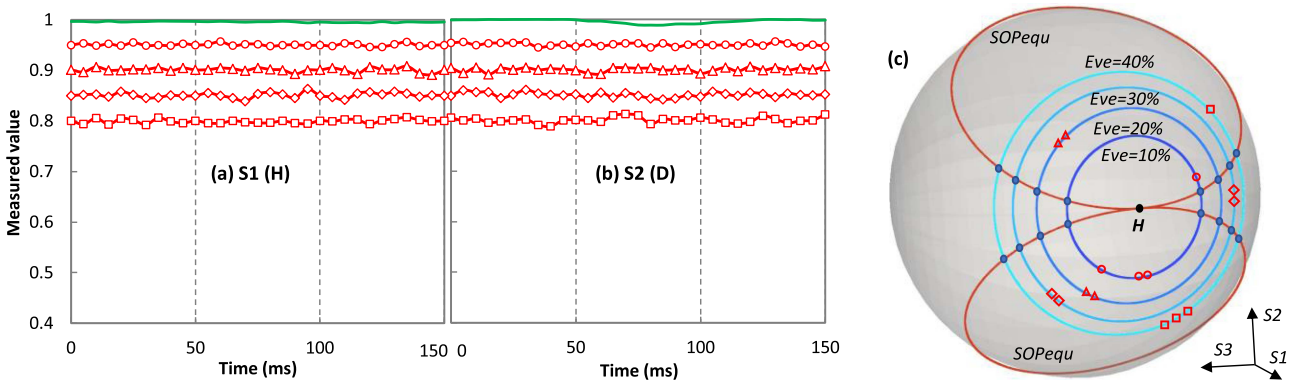

Fig. 12. SOP changes emulation w.r.t. R (a) and D (b) bases under scenario 3. Measured $\mathrm{SOP_H}$ in Mo intervals for different Eve rates.

we observe that keys with 30k photons decrease qBER by 75%. We found that the average reversal rotation applied by EPC is 1.12, which entails that the first rotation for checking the signs, which assumes the signs similar to the last SOP measurement, almost compensates for the high qBER. In Fig. 10(c), we observe that 30k photons improve KER by 24% Therefore, keys of 30k photons length maximize the precision of SOP estimation and the final KER.

Next, we focus on comparing the different methods for interpolation of the rotation plan (Section III-C) for the B2B scenario. Fig. 11(a) illustrates how linear interpolation can be improved by the three proposed interpolation methods taking advantage of the predicted SOP_{Ke}. Method 1 can improve KER by 14% by just using predicted $\mathrm{SOP_{Ke}}$ without any reversal rotations for checking stokes' sign. Method 2 improve the linear interpolation by 24% by always checking the signs every 10ms. Finally, the third interpolation method (threshold-based) can improve the QKD system by 31% as it needs less reversal rotations. Note that distance would impact the performance of methods 2 and 3 because of the round-trip-time needed for sign checking.

In view of these results, we focus on compensation method 3 and study the impact of the value of *intrpol_thr* and the distance between the QTx and the QRx. Fig. 11(b) compares the performance of method 3 as a function of different thresholds assuming 50 km between QTx and QRx. We observe that *intrpol_thr* $=$ 2% is the best candidate to take the countermeasure action against deficient interpolation. Lower values would waste photons for reversal rotations applied by the EPC and consequently decreases KER, whereas higher values would delay rotation decision making, which would also reduce KER. Finally, Fig. 11(c) studies the impact of distance between QTx and QRx assuming *intrpol_thr* $= 2\%$. We observe that although KER reduces with distance, KER is always better than that of linear interpolation for the studied distances.

Finally, in eavesdropping scenario 3, the attacker emulates SOP changes during Mo intervals as shown in Fig. 12(a) and (b), respectively. Selected SOP_H in Mo intervals are measured for different eavesdropping rates (Fig. 12(c)) and checked w.r.t. SOP*equ* circles for H polarization. Eavesdropping is detected in case of mismatch.

A complete example is eventually showcased to illustrate how DARIUS can help the QKD system to address the high qBER in case of higher velocity events is presented. Fig. 13 reproduces such example, where the evolution of $S_{1(H)}$ (as a SOP representative) and qBER are plotted. Initially, the $\mathrm{DNN_{(low)Mo}}$ model is in operation in the AI-based SOP compensator, which uses linear interpolation to compensate for low speed events, and qBER is well under the eavesdropping threshold (10%). At time 300ms, an event of speed 2 rad/s affects the qCh. We observe that the rotation points follow the SOP trajectory with good precision, so qBER remain under the eavesdropping threshold. From 550 ms on, the velocity of the events increases and violates the *velocity_thr* (3 rad/s), so DARIUS stops compensation until learning the new conditions. As a result, qBER exceeds the threshold

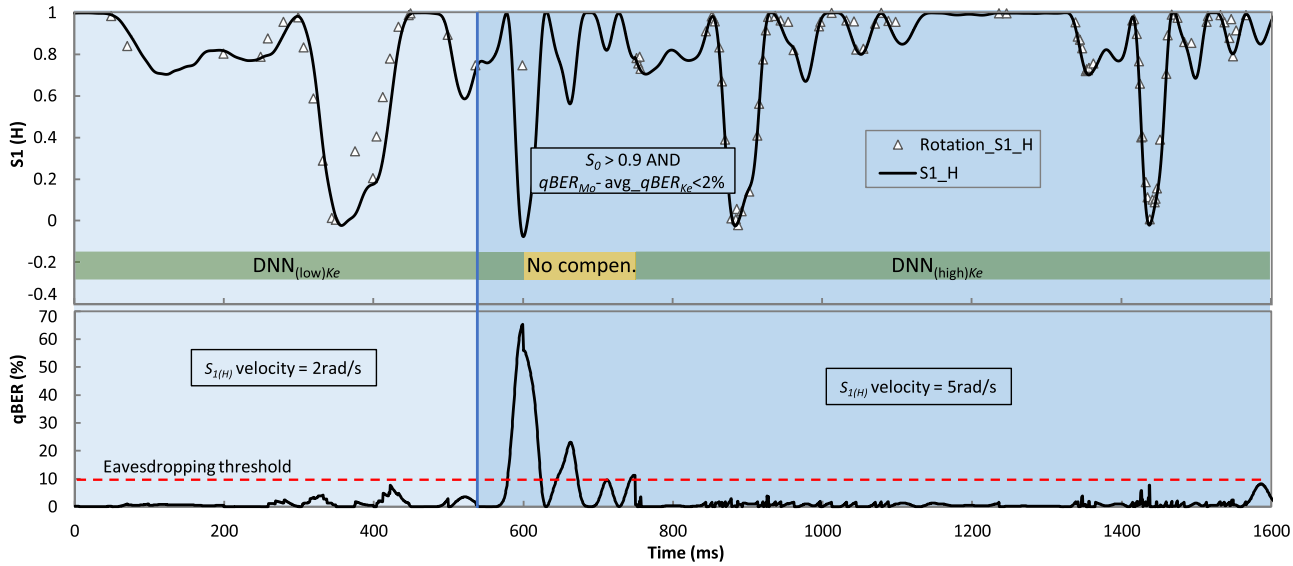

Fig. 13. Illustrative example of DARIUS operation.

and keys are discarded. DARIUS checks for eavesdropping and both scenarios are checked and results detailed in Fig. 13 confirm no attack. During that period, DARIUS also collects adequate Mo and Ke intervals' SOP measurements to feed $\text{DNN}_{(\text{high})\text{Mo}}$ and $\text{DNN}_{(\text{high})\text{Ke}}$ models, in case no eavesdropping is detected. Then, DARIUS checks the velocity of $S_{1(H)}$ before and after the increased qBER and determines that velocity has increased from 2 rad/s to 5 rad/s. In consequence, the AI model in operation is changed to $\text{DNN}_{(\text{high})\text{Mo}}$, and threshold-based interpolation using $\text{DNN}_{(\text{high})\text{Ke}}$ model is applied. Now, the AI-based SOP compensation method can take advantage of good predictions in the Mo and Ke intervals, and it can perfectly compensate for the higher velocity events and keep the qBER under the threshold.

V. Concluding Remarks

A Digital Twin, named DARIUS, has been proposed to improve the performance of polarization-encoded QKD systems. Precise quantum measurement of received photons enable DARIUS to achieve its three main objectives: *i*) consider optical components' non-ideal behaviors in the QKD system to help the QRx discern polarization distortions in the qCh from optical components loss; *ii*) help distillation engines to distinguish between eavesdropping and high qBER in the channel; and *iii*) assist QRx with fine proactive compensation of distortion due to environmental events having different velocity. Including D polarized photons along with H ones for reference SOPs in Mo intervals, enable the QRx to detect a larger sort of SOP distortions in the qCh. Taking advantage of the Mo intervals, DARIUS might not only recognize SOP distortions but also distinguish them from eavesdropping, as both rise the qBER.

DARIUS exhibited extraordinary accuracy in detecting eavesdropping by analyzing its effects on SOP. Even moderate eavesdropping rate of 14% could decrease S_0 by 10% when attacks are performed without knowledge of Mo intervals, whereas eavesdropping rates as low as 10% were detected when they are performed during Ke intervals only, as SOP during those intervals is changed, as compared to that measured during Mo ones.

DARIUS assists the QRx with proper actions against different velocity of fiber stressing events in the qCh. Results showed that DARIUS is able to measure the velocity and choose the best solution to compensate for the effects of the events. DARIUS compensation method improved KER by 31% w.r.t. linear interpolation.

References

[1] V. Martin, J. Martinez-Mateo, and M. Peev, *Introduction to Quantum Key Distribution*. Hoboken, NJ, USA: Wiley, 2017.
[2] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, 1984, pp. 175–179.
[3] Y. Ding et al., "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," *Opt. Lett.*, vol. 42, pp. 1023–1026, 2017.
[4] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, pp. 3–28, 1992.
[5] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, and G. B. Baumgartner, "Using modeling and simulation to study photon number splitting attacks," *IEEE Access*, vol. 4, pp. 2188–2197, 2016.
[6] D. Babukhin, D. Kronberg, and D. Sych, "Explicit attacks on the Bennett-Brassard 1984 protocol with partially distinguishable photons," *Phys. Rev. A*, vol. 106, 2022, Art. no. 042403.
[7] C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in BB84 quantum key distribution protocols," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 2689–1701, Sep. 2022.
[8] G. S. Castro and R. V. Ramos, "Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness," *Quantum Inf. Process.*, vol. 21, p. 79, 2022, doi: 10.1007/s11128-022-03422-y.
[9] S. Pillay, A. Mirza, and F. Petruccione, "Towards polarisation-encoded quantum key distribution in optical fibre networks," *South Afr. J. Sci.*, vol. 111, pp. 1–6, 2015.
[10] T. Wang, P. Huang, S. Wang, and G. Zeng, "Polarization-state tracking based on Kalman filter in continuous-variable quantum key distribution," *Opt. Exp.*, vol. 27, pp. 26689–26700, 2019.
[11] A. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. André, and A. N. Pinto, "Continuous control of random polarization rotations for quantum communications," *J. Lightw. Technol.*, vol. 34, no. 16, pp. 3914–3922, Aug. 2016.

[12] M. Ramos, N. Silva, N. Muga, and A. Pinto, "Reversal operator to compensate polarization random drifts in quantum communications," *Opt. Exp.*, vol. 28, pp. 5035–5049, 2020.
[13] M. Ramos, N. Silva, N. Muga, and A. Pinto, "Full polarization random drift compensation method for quantum communication," *Opt. Exp.*, vol. 30, pp. 6907–6920, 2022.
[14] M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "Cost-effective ML-powered polarization-encoded quantum key distribution," *J. Lightw. Technol.*, vol. 40, no. 13, pp. 4119–4128, Jul. 2022.
[15] D. Wang et al., "Role of digital twin in optical communication: Fault management, hardware configuration, and transmission simulation," *IEEE Commun. Mag.*, vol. 59, no. 1, pp. 133–139, Jan. 2021.
[16] D. Sequeira, M. Ruiz, N. Costa, A. Napoli, J. Pedro, and L. Velasco, "OCATA: A deep-learning-based digital twin for the optical time domain," *J. Opt. Commun. Netw.*, vol. 15, pp. 87–97, 2023.
[17] M. Ahmadian et al., "Designing a digital twin for quantum key distribution," in *Proc. Eur. Conf. Opt. Commun.*, 2022, pp. 1–4.
[18] S. Barnett, J. Jeffers, A. Gatti, and R. Loudon, "Quantum optics of lossy beam splitters," *Phys. Rev. A*, vol. 57, 1998, Art. no. 2134.
[19] X. Zhang and 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," *Chin. Phys. B*, vol. 17, pp. 2509–2513, 2018.
[20] A. Sit, L. Giner, E. Karimi, and J. Lundeen, "General lossless spatial polarization transformations," *J. Opt.*, vol. 19, 2017, Art. no. 094003.
[21] J. Jackson, *Classical Electrodynamics*, 3rd ed. Hoboken, NJ, USA: Wiley, 1998.
[22] M. Al-Mahmoud, H. Hristova, V. Coda, A. Rangelov, and N. Vitanov, "Non-reciprocal wave retarder based on optical rotators combination," *Opt. Soc. Amer. Continuum*, vol. 4, pp. 2695–2702, 2021.
[23] N. J. Muga, A. N. Pinto, M. F. S. Ferreira, and J. R. F. da Rocha, "Uniform polarization scattering with fiber-coil-based polarization controllers," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 3932–3943, Nov. 2006.
[24] X. Tang, L. Ma, A. Mink, and A. Nakassis, "High speed fiber-based quantum key distribution using polarization encoding," *Proc. SPIE*, vol. 5893, pp. 326–334, 2005.
[25] S. M. Ahmadian et al., "Replication data for fast quantum key distribution," 2022, doi: 10.34810/data190.
[26] H. Norlen, *Quantum Computing in Practice With Qiskit and IBM Quantum Experience: Practical Recipes for Quantum Computer Coding at the Gate and Algorithm Level With Python*. Birmingham, U.K.: Packt Publishing, 2020.
[27] IDQuantique Clavis XG QKD System, 2023. [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/
[28] L. Comandar et al., "GHz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," *J. Appl. Phys.*, vol. 117, 2015, Art. no. 083109.
[29] F. Boitier et al., "Proactive fiber damage detection in real-time coherent receiver," in *Proc. Eur. Conf. Opt. Commun.*, 2017, pp. 1–3.
[30] Y. Tang et al., "High-speed and large-scale privacy amplification scheme for quantum key distribution," *Sci. Rep.*, vol. 9, 2019, Art. no. 15733.