ML-Aided SOP Compensation to Increase Key Exchange Rate in QKD Systems

Morteza Ahmadian*, **Marc Ruiz, Jaume Comellas, and Luis Velasco**
Optical Communications Group (GCO), Universitat Politècnica de Catalunya (UPC), Barcelona, Spain
**e-mail: seyed.morteza.ahmadian@upc.edu*

2023 23rd International Conference on Transparent Optical Networks (ICTON) | 979-8-3503-0303-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICTON59386.2023.10207413

ABSTRACT
Secure communications have become a requirement for virtually all kind of applications. Currently, two distant parties can generate shared random secret keys by using public key cryptography. However, quantum computing represents one of the greatest threats for the finite complexity of the mathematics behind public key cryptography. In contrast, Quantum Key Distribution (QKD) relies on properties of quantum mechanics, which enables eavesdropping detection and guarantees the security of the key. Among QKD systems, polarization encoded QKD has been successfully tested in laboratory experiments and recently demonstrated in closed environments. In this paper, we propose a Machine Learning (ML) -based polarization tracking and compensation that is able to keep shared secret key exchange to high rates even under large fiber stressing events. Exhaustive results using both synthetic and experimental data show remarkable performance, which can simplify the design of both quantum transmitter and receiver, as well as enable the use of aerial optical cables, thus reducing total QKD system cost.
Keywords: polarization-encoded quantum key distribution; machine learning.

1. INTRODUCTION

Quantum Key Distribution (QKD) has become mature in closed, controlled scenarios in view of the plenty of works available in the literature reporting related experiments. In polarization encoded QKD systems, a Quantum Transmitter (QTx) sends polarized photons, i.e., quantum bits (qubit), to a Quantum Receiver (QRx), which decodes them and generates a raw key of a defined length. The raw key is then distilled, using a parallel public channel established between transmitter and receiver, to correct possible detection errors due to optical transmission and generate a shared secret key. E.g., the authors in [1] showed a polarization-based QKD system using the BB84 protocol that reaches shared secret Key Exchange Rates (KER) > 1 Mb/s for distances >100 km.

Currently, research efforts are also focused on demonstrating such performance in real (more challenging) scenarios, including aerial cables, where QKD transmission might be severely affected by weather conditions (e.g., high wind) that stresses optical fibers [2]. Such mechanical stress changes fiber birefringence, which introduces fluctuations on the State of Polarization (SOP) of the transmitted qubits and, as a result, Quantum Bit Error Rate (QBER) increases. Note that QBER is causally related to the effective KER, which reduces when QBER increases, e.g., from Mb/s to Kb/s or even b/s as shown in [3]. Since optical eavesdropping generates high QBER, a post processing phase named key distillation enables its detection. However, excessive QBER coming from SOP fluctuations might derive into false eavesdropping detection (threshold is typically set within the range 5%-10%); in such case, safety mechanisms against attacks are activated, thus interrupting (i.e., KER becomes temporarily 0), or even blocking that quantum channel for key exchange.

In this work, we summarize the work in [4] and propose a lightweight ML-based SOP tracking and polarization compensation that uses Deep Neural Network (DNN) models for polarization encoded QKD systems. Such models accurately anticipate SOP fluctuations, so adaptive actions can be taken at the QRx to reverse them before they produce negative impact. The proposed system is specifically designed to maximize performance, i.e., to reduce false eavesdropping detection and increase effective KER, in scenarios exposed to environmental events. The proposed approach will enable cost reduction of QKD systems as: *i*) QTx specifications can be relaxed since SOP imperfections can be corrected by the QRx; and *ii*) the hardware design of the QRx can be simplified and rely on software.

2. ML-BASED FAST QUANTUM KEY DISTRIBUTION

In this section, we first briefly present the main concepts and used notation. Rather than an exhaustive description of QKD systems, we first present the essential concepts regarding transmission, propagation, and photons measurement for raw keys exchange under the BB84 protocol [5]. Next, we identify opportunities and propose solutions to accelerate the distribution of keys over a quantum channel in the presence of SOP fluctuations.

Preliminary concepts

In BB84, the QTx continuously generates raw keys containing sequences of pairs of Boolean values, each pair containing a basis (B) and bit (b). The pair $<B(t), b(t)>$ generated at time t is defined by the quantum state $|q(t)\rangle$, which can be defined as a position on the Bloch sphere. Therefore, $|q(t)\rangle$ can be alternative expressed: i) in Euclidean coordinates $<x(t), y(t), z(t)>$, with one component for axis X, Y, and Z, respectively; or ii) in polar coordinates $<\theta(t), \varphi(t)>$, represented by azimuth and ellipticity angles, respectively. In practice, $|q(t)\rangle$ is encoded

as a single photon, which translates into a single point on the unitary Poincaré sphere; Both Bloch and Poincaré spheres are exchangeable if axes X, Y, and Z of the former match Stokes S_2, S_3, and S_1, respectively, in the latter.

Effects related to fiber propagation and eavesdropping alter $|q(t)\rangle$. Let us denote $|p(t)\rangle = <\theta_{p(t)}, \varphi_{p(t)}>$ as the real polarization of the received photon. We adopt the QRx hardware architecture proposed in [6], where the QRx is equipped with an Electronic Polarization Controller (EPC) followed by a Polarization Beam Splitter (PBS). The photon first reaches the EPC, which is in charge of polarization alignment. Specifically, given a reference polarization state $r(t)$ (hereafter denoted as rotation) defined by the tuple $<\theta_{r(t)}, \varphi_{r(t)}>$, the EPC performs a reversal operation to align the photon detector with the configured polarization state. Hence, it is worth noting that the rotation with configuration $\theta_{r(t)}=\theta_{p(t)}$ and $\varphi_{r(t)}=\varphi_{p(t)}$ is the one perfectly aligned with the state $|p(t)\rangle$ of received photon. Before the photon passes through the PBS, a basis is selected, which entails selecting a specific axis in the sphere to detect the photon and extract its bit [5]. Two main conditions lead to erroneous bit extraction: i) if the sphere is perfectly aligned with $|p(t)\rangle$, the bit is wrongly decoded if QRx selects the wrong basis; and ii) even if QRx selected the correct basis, bit error can be produced if there is misalignment between $r(t)$ and $|p(t)\rangle$.

Besides the quantum channel, a parallel secure public channel is used for key distillation purposes. QRx starts sending a subset of decoded bits and basis to QTx in order to quantify bit errors, i.e., QBER. In case that QBER exceeds a given threshold, e.g., 10%, eavesdropping in the quantum channel is assumed, which triggers a safety mechanism, such as QKD interruption. Otherwise, QKD is assumed to be secure enough. Next, bases need to be verified, since they were randomly selected at the QRx side. To that end, key sifting is performed, where QTx sends to QRx the sequence of used bases through the public channel, so that QRx can check them and discard the wrong ones. After the bases are synchronized, error cascading is conducted to correct the erroneous bits, which results into a corrected sifted key. In the end, a portion of the sifted key is selected as the final shared secret key to amplify privacy. This process results into a maximum achievable KER when QBER is low, and it will be noticeably reduced when QBER increases.

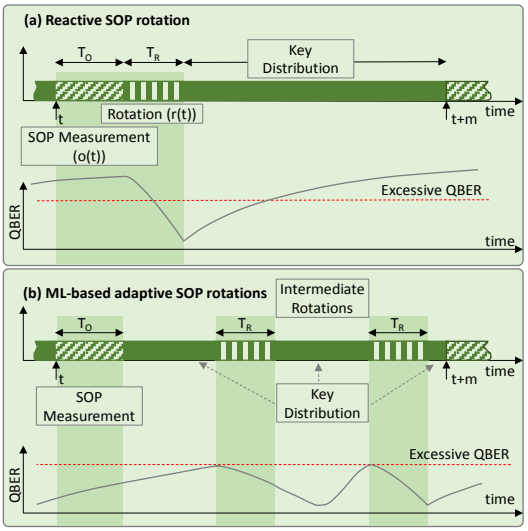

Figure 1. Reactive (a) and ML-based adaptive (b) SOP rotation.

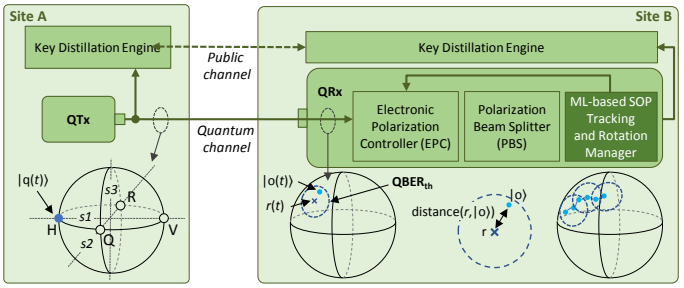

Figure 2. System architecture.

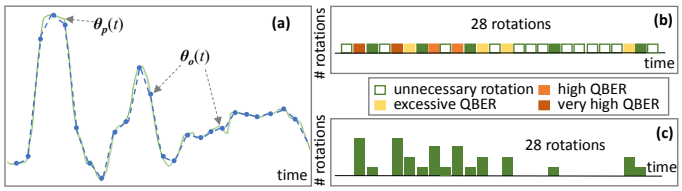

Figure 3: Example of operation (a) performance of the reactive (b) and ML-based adaptive (c) SOP rotation.

Opportunities and proposed solutions

For illustrative purposes, Fig. 1a shows the operation of the quantum channel with time based on the approach proposed in [6]. At regular time intervals of size m, the QTx sends a number of qubits with a predefined polarization that are used to monitor the current SOP, denoted $|o(t)\rangle$, at the QRx. Based on the measured SOP, the QRx computes the needed rotation (denoted $r(t)$) to compensate the polarization drift. Once the rotation is performed, the quantum communication system exchanges polarization-encoded keys. If the value of m is large enough compared to the time for monitoring (T_O) and rotation (T_R), this scheme introduces a small overhead, while allows to react quickly to changes in the SOP. Fig. 1a also includes a possible evolution of the QBER from one rotation to the next. In the presence of SOP fluctuations, it might happen that the rotation performed at the starting of a period does not allow to keep the QBER under a desired threshold (denoted $QBER_{th}$), e.g., 1%, until the next polarization state is measured, and a new rotation is performed.

A possible solution to deal with scenarios with large SOP fluctuations would be to reduce m, which would result in a higher system overhead, especially during the time when fluctuations are small or negligible. For that,

m can be defined dynamically, which would entail a way to synchronize QTx and QRx real-time. In view of this, we propose an approach to track SOP fluctuations and apply ML to predict the next polarization states based on such tracking. Then, rotations can be planned to be performed at any intermediate time from one SOP measurement to the next; the number of rotations would vary from none to several, so the obtained QBER is always under $QBER_{th}$ (Fig. 1b). Because rotations can be planned to be performed at intermediate times, accurate estimation of future states is of paramount importance for the proposed system. Armed with such predictive tool, an optimization problem can be solved to decide not only when to perform the rotations, but also the value of each rotation to minimize the number of total rotations that are performed; this would result into a reduced overhead, while assuring a contained QBER. In the example of QBER evolution in Fig. 1b, no initial rotation is needed, as QBER was initially low, whereas two rotations are performed at intermediate times. In particular, the first rotation is performed to compensate SOP at a future state, as revealed by the evolution of the QBER that progressively reduces until a minimum and increases again reaching a value close to $QBER_{th}$ before the second rotation is performed.

Fig. 2 shows a schematic view of a quantum communication channel established between remote sites A and B. Without assuming any specific polarization based QTx implementation, let us consider that a qubit is generated by randomly selecting one linear polarization (points H, V, R, and Q on the sphere at site A in Fig. 2). Then, the perfectly polarized photon is sent to the QRx. When the photons are received and measured at the QRx side, the SOP position might have drifted. Fig. 2 reproduces the EPC and PBS modules in the QRx based on the architecture proposed in [6]. The obtained QBER will be below $QBER_{th}$ if the state of the received photons is within an area centered in the current reference polarization state with radius d_{th}. When the reference polarization state of the QRx is rotated, the area of tolerable $QBER_{th}$ also moves covering a different region. In the proposed system, a ML-based module is in charge of tracking SOP and deciding the rotations to be performed, as illustrated in Fig. 2.

An illustrative example of the operation is presented in Fig. 3. Fig. 3a shows the evolution polarization angle θ of the real photons state $|p(t)\rangle$ and measured state $|o(t)\rangle$, both at the QRx. In addition, linear (polynomial of degree 1) interpolation connecting two measured polarization states is represented. Note that although linear interpolation is used for the sake of simplicity in the drawing, higher degrees can be used. In Fig. 3b-c, the rotations that are performed under the reactive and adaptive approaches are shown. We assume here the same period *m* for both approaches. In the reactive approach (Fig. 3b), one single rotation is performed once the current state $|o\rangle$ is measured after T_O, which results into 28 rotations for the sample in Fig. 3a. However, as many as 15 of the rotations are unnecessary, because at the time they are performed, the measured polarization state is within the area of low QBER. On the contrary, there are 4 periods with high and very high QBER, due to large SOP fluctuations in those periods. In contrast, the proposed ML-based SOP tracking and rotation planning approach, is able to achieve low QBER even during large SOP fluctuations (Fig. 3c), due to its ability to predict future polarization states and plan the needed rotations. Note that the total number of rotations under the ML-based approach is equivalent (it can be even lower) to the reactive approach, which ensures high efficiency. That fact, combined to the reduced QBER, results in faster KER.

3. ML-BASED SOP TRACKING AND ROTATION MANAGER

In this section, we first present the procedure used to measure and predict the evolution of photons' polarization state based on the combination of the quantum state tomography theory and DNN models. Next, the procedure to plan the sequence of Poincaré sphere rotations that needs to be carried out to achieve accurate polarization alignment based on the SOP prediction is described.

SOP monitoring and prediction

As introduced in the previous section, SOP can be affected by perturbations on the fiber, during the monitoring period starting at time t, the QTx sends a number of photons with a known polarization and the QRx measures them in different axes to accurately estimate the current state $|o(t)\rangle$, defined by the tuple $\langle\theta_{o(t)}, \varphi_{o(t)}\rangle$. Specifically, the QTx generates n photons with H polarization (i.e., $\langle B,b\rangle = \langle 0,0\rangle$), which are propagated through the quantum channel. At the QRx side, the received photons are separated in three different chunks of $n/3$ photons, one for each of the three axes X, Y, and Z measurements. The decoded bits can contain some 1's due to the combination of the selected axes for measurement, the fluctuations of the SOP during propagation, and the current rotation configuration in the EPC. Then, we define the QBER of a chunk as the sum of the extracted bits (number of erroneous bits) over the length of the chunk ($n/3$). After transmitting and decoding all *n* photons, measurement results are available for each axis, i.e., QBER(t) = {*X*, *Y*, *Z*}. The measurement along the Z axis is enough to compute $\theta(t)$, whereas $\varphi(t)$ requires from measurements along X and Y axes to estimate sine and cosine of $\varphi(t)$, respectively.

Once the current polarization state $|o(t)\rangle$ is estimated, it is used to predict the SOP evolution until the next monitoring period. Currently estimated state $|o(t)\rangle$ and the set of past polarization state estimations along with the DNN model f used for SOP prediction. The objective is to generate sequence *O* containing the current estimated state $|o(t)\rangle$ and the prediction of the next *k* consecutive and evenly distributed polarization states

connecting $|o(t)\rangle$ and the expected one for the next monitoring period, i.e., $|o(t+m)\rangle$. Sequence O is determined by using DNN-based forecasting and polynomial fitting sequentially. The DNN is used to accurately forecast a discrete time-dependent event ahead in time, whereas polynomial is used to interpolate unknown polarization states between known states. The procedure is as follows; the last estimated polarization state is stored in the SOP database and the last estimated polarization states within the previous time window w are retrieved that are used to feed a DNN model that predicts $|o(t+m)\rangle$. The DNN has $2\cdot \lfloor w/m \rfloor$ inputs (for angles θ and φ of those last SOP values), several hidden layers using the tanh activation function, and two outputs for angles θ and φ of predicted state $|o(t+m)\rangle$. Next, the last w estimated polarization states together with the predicted $|o(t+m)\rangle$ are used to interpolate a polynomial-based model g. To increase the accuracy of the interpolation procedure, g is a compound model with four l-degree polynomials used to estimate $\sin(\theta)$, $\cos(\theta)$, $\sin(\varphi)$, and $\cos(\varphi)$ as a function of time in the range $[t, t+m]$. Finally, g is used to obtain k predictions between $|o(t)\rangle$ and $|o(t+m)\rangle$.

Rotation plan computation based on SOP prediction

After the SOP prediction phase, the problem of finding which rotations need to be applied within the time interval [t, t+m] is solved. This problem can be modeled as an optimization problem and stated as follows:

Given:

- The sequence O of predicted states, each for a relative time $i\in[0, m]$ and defined as $O(i) = <\theta_o(i), \varphi_o(i)>$.
- The set of candidate rotations R, where every rotation r is defined by $<\theta_r, \varphi_r>$. R includes the rotation r_0 currently configured in the EPC.
- A circular area of radius d_{max} [rad] defined for a target QBER and thus, determining the need of rotations. A candidate rotation $r\in R$ that becomes active at relative time j is valid for state predictions $|o\rangle\in O \mid i\geq j$ if and only if distance$(r, |o\rangle) \leq d_{max}$.

Output: The rotations plan $P = [<r, i>]$, where every element defines the relative time $i\in[0, m]$ when candidate rotation $r\in R$ needs to be configured in the EPC.

Objective: minimize the number of rotations to be performed.

To reduce the complexity of the rotation plan problem, we consider that set R includes the current rotation r_0 and all predicted polarization states in O. Therefore, a trivial feasible solution would consist in performing k rotations, one for each predicted state. To efficiently solve the rotation plan optimization problem, we designed the fast deterministic greedy algorithm (Algorithm I). A pre-computation phase is run to find the subset of predicted polarization states that can be served from each candidate rotation. Then, an iterative procedure is executed to build the plan (sequence) of rotations until all polarization states are assigned to, at least, one of the selected rotations. At every iteration, the greedy cost of every rotation is computed. Such cost is defined as a weighted sum of three components, with weights $\beta_1 >> \beta_2 >> 1$. The three components account: *i*) whether the rotation covers reference polarization state $|o_{ref}\rangle$, which is initialized with the measured polarization state and updated with the last state covered by the rotation when a new rotation is performed. This component tries to foster selecting new rotations that overlap with the previous one, which forces building the plan as a sequence that tracks the evolution of O; *ii*) whether the rotation is the currently active one or not, so as to reduce the number of rotations; and *iii*) the number of polarization states covered by the candidate rotation. The candidate rotation with the highest greedy cost is selected and added to the incumbent solution. Then, the relative time to perform the next rotation is computed and the set of covered polarization states O_{in} and reference state $|o_{ref}\rangle$ are updated. Finally, the rotation plan is returned.

Algorithm I. Heuristic for the rotation plan problem.

INPUT: O, R, d_{max}
OUTPUT: P

$P \leftarrow \{\}$; $i \leftarrow 0$; $O_{in} \leftarrow \{\}$; $|o_{ref}\rangle \leftarrow O[0]$
for $r \in R$ **do**
  for $|o\rangle \in O$ **do**
    if *distance*$(r, |o\rangle) > d_{max}$ **then continue**
    r.O.append($|o\rangle$)
while $O_{in} <> O$ **do**
  for each $r \in R$ **do**
    if $|o_{ref}\rangle \in r$.O **then** $x_1 \leftarrow 1$ **else** $x_1 \leftarrow 0$
    if r=r_0 **then** $x_2 \leftarrow 1$ **else** $x_2 \leftarrow 0$
    $x_3 \leftarrow |r.O|$
    r.cost $\leftarrow \beta_1 \cdot x_1 + \beta_2 \cdot x_2 + x_3$
  $r' \leftarrow$ argmax(r.cost $\forall r\in R$)
  $P \leftarrow P \cup <r', i>$
  $O_{in} \leftarrow O_{in} \cup r'$.O
  $|o_{ref}\rangle \leftarrow r'$.O[-1]
  $i \leftarrow |o_{ref}\rangle$.i
return P

4. CONCLUSION

A ML-based SOP tracking and polarization compensator has been presented that might significantly reduce the cost of polarization encoded QKD systems by simplifying the specifications of quantum transmitter and receiver and enabling the use of aerial optical fiber cables. The proposed system is based on three main components: i) a SOP monitoring procedure able to precisely estimate the current polarization state while minimizing overhead; ii) a lightweight ML-based SOP prediction that is able to accurately forecast future SOP evolution with fine granularity; iii) a Poincaré sphere rotation planner, which decides when rotations need to be performed and the magnitude of such rotations to compensate polarization drift and keep QBER under a given threshold.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Commission HORIZON ALLEGRO (G.A. 101092766) and the AEI IBON (PID2020-114135RB-I00) projects and from the ICREA institution.

REFERENCES

[1] M. Khan *et a*l., "Analysis of achievable distances of BB84 and KMB09 QKD protocols," *Quantum Info*, vol. 18, 2020.
[2] R. Liu *et al.,* "Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design," *OFT*, 2019.
[3] B. Fröhlich *et al.,* "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, 2017.
[4] M. Ahmadian *et al*., "Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution," *JLT*, 2022.
[5] P. Shor *et al.,* "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Let*, vol. 85, 2000.
[6] M. Ramo**s** *et al*., "Reversal operator to compensate polarization random drifts in quantum communications," *OSA*, 2020.