Optimization of a Polarization-Encoding System for Practical Quantum Key Distribution

Hugo F. Costa[1,2], **Nelson J. Muga**[1], **Nuno A. Silva** [1], **Armando N.Pinto**[1]

[1] Instituto de Telecomunicacões – University of Aveiro, 3810-193, Aveiro, Portugal.

[2]Physics Department – University of Coimbra, R. Larga 2, 3000-370 Coimbra.

huhu.gocosta@gmail.com, muga@ua.pt, nasilva@ua.pt ,anp@ua.pt

Abstract. *We present a method for optimizing the waveplate's voltage range of an electro-optic based electrical polarization controller for qubit encoding in discrete-variable quantum key distribution (QKD). By increasing the number of used waveplates, the maximum voltage range to generate each of the states-of-polarization required by a QKD protocol can be reduced. The proposed machine learning algorithm, particle swarm optimization, was validated through numerical and experimental results. Results show that transitions between six states of polarization used in QKD systems can be generated using a maximum voltage range of 10V in each waveplate.*

1. Introduction

In today's world data security is increasingly an important subject. Our personal, financial, and health data is transmitted over communications networks. With the increase in computational power we have been experiencing over the years and more recently with the development of quantum computers, traditional encryption methods may be at risk. Quantum Key Distribution (QKD) methods have been studied and developed as possible solutions to this security concerns [Pirandola et al. 2020].

QKD is composed by two main steps, quantum communication succeeded by classical post-processing. The security of systems based on it, is not on complex mathematical problems or very secure private channels, but instead on the nature of quantum mechanics. Characteristics such as the described by the non-cloning theorem or Heisenberg's uncertainty principle, are what makes a QKD system unconditionally secure. Non-orthogonal quantum states cannot be cloned and cannot be reliably distinguished. There is no measurement device we can create that can reliably distinguish non-orthogonal states. Different degrees of freedom of the photons can be used to codify the qubits used to employ QKD protocols, those can be polarization, time, frequency, phase and orbital angular momentum [DJORDJEVIC 2020]. There are two main general schemes Discrete variable (DV-QKD) and Continuous variable (CV-QKD).

In (DV)-QKD schemes, a single photon detector (SPD) [Ramos et al. 2022] is applied in Bob's side while in (CV)-QKD the field quadrature of light is measured with support of homodyne/heterodyne detection [DJORDJEVIC 2020] [Pereira et al. 2021] . Methods based in photon polarization, trough DV-QKD are really appellative due to their high versatility (free space and optical fiber) and overall easier use [Muga et al. 2019] [Mantey et al. 2021] [Mantey et al. 2022] [Muga 2020].

To control the state-of-polarization of the photons used in QKD Eletrical Polarization Controller's (EPC) are used. Polarization controllers are optical devices that allow changing an arbitrary input SOP of an optical beam into any desired output SOP. This devices can be based in Electro-optic crystals, Electromagnetic fiber squeezers, Faraday rotators and Fiber-coils.

The device we are looking to optimize is based in Electro-optic crystals. It's working principle is based in Pockels effect, we observe a change in the crystal refractive index linearly proportional to the electric field.

Finding the voltages necessary to change an arbitrary State of Polarization (SOP) at the entrance of the EPC into the desired SOP at the output, while also minimizing the voltage intervals required to achieve all necessary SOP at the output is what it's looked at in this paper.

To achieve this goal a machine learning algorithm, Particle Swarm Optimization is applied. Where we take into account the error of the Stokes vector at the output and the voltage interval needed to change from one SOP to another random one from the usual ortogonal basis used in DV-QKD systems.

2. Electrical Polarization Controller

The EPC we were looking to optimize is based in Electro-optic crystals, this means it can make use of the Pockels effect. Pockels effect is the change in birefringence of an optical medium induced by an electric field.

Only in certain crystals that lack inversion symmetry, such as lithium niobate, can this effect occur. Lithium niobate is the crystal used to make the EPC we are using [van Haasteren et al.]. The EPC's in our possession come with 6 or 8 stages. Each stage is a crystal that will be used as a waveplate to modify the SOP.

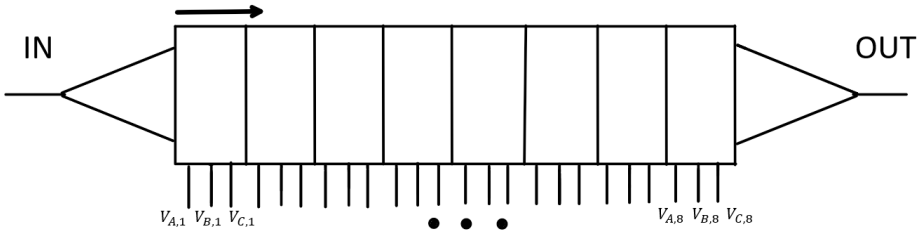


Figure 1. Schematic representation of an EPC comprised by several waveplates.

The number of stages in the EPC will not change it's appearance only the number of usable pins.

2.1. Controlling the EPC

Controlling the birefrigenge of each crystal is a straight forward trough the use of the following equations:

$$V_A = 2_0 \cdot \delta \cdot sin(\alpha) - V_\pi \cdot cos(\alpha) + V_{A,bias} \tag{1}$$

$$V_B = 0 \quad (Ground) \tag{2}$$

$$V_C = 2_0 \cdot \delta \cdot sin(\alpha) + V_\pi \cdot cos(\alpha) + V_{C,bias} \tag{3}$$

V_A, V_B and V_C are the voltages we need to apply to a certain stage to have a wave plate of δ retardation and with $\alpha/2$ the orientation angle of the fast axis.V_{pi},V_0 and $V_{A,bias}$,$V_{B,bias}$ are known constants, found during calibration.

To calculate the output SOP we make use of Mueller calculus, we present the input SOP in the form of a stocks vector. The effect of each stage/wave plate can be defined by the following matrix:

$$M = \begin{bmatrix} cos^2(\alpha) + sin^2(\alpha)cos(\delta) & cos(2\alpha)sin(\alpha)(1 - cos(\delta)) & sin(\alpha)sin(\delta) \\ cos(2\alpha)sin(\alpha)(1 - cos(\delta)) & cos^2(\alpha)cos(\delta) + sin^2(\alpha) & -cos(\alpha)sin(\delta) \\ -sin(\alpha)sin(\delta) & cos(\alpha)sin(\delta) & cos(\delta) \end{bmatrix} \tag{4}$$

So the SOP at the output can be calculated by:

$$\begin{pmatrix} S_1 \\ S_2 \\ S_3 \end{pmatrix}_{OUT} = \prod_{i=0}^{n} M_i^n \cdot \begin{pmatrix} S_1 \\ S_2 \\ S_3 \end{pmatrix}_{IN} \tag{5}$$

Where n is the number of stages we are using in the EPC, and S_0, S_1, S_2 and S_3 are the stocks parameters of the input and output polarization's.

3. Applying machine learning

The goal of this work is to obtain the values of α and δ to achieve the 3 orthogonal basis that are needed to implement an QKD system.There are a lot of possible α and δ for a given input SOP to be converted to a goal SOP.

We intend to find the values of α and δ from those multiple combinations that minimize the jump is voltage values we need to apply in V_A and V_C. The main thing we need to define is the cost function:

$$C = \sum_{i=1}^{3} a \cdot \mid S_i - L_i \mid + \sum_{i=1}^{6} \frac{\mid V_{A,i} - V_{AIN,i} \mid}{b} + \sum_{i=1}^{6} \frac{\mid V_{C,i} - V_{CIN,i} \mid}{c} \tag{6}$$

The first sum represents the difference in the values of the stocks parameters for the current selected combination of $\alpha's$ and $\delta's$ and the desired stocks parameters, a is a weight that can be adjusted. The second and third sum take in account all the differences between the voltages for the current combination of $\alpha's$ and $\delta's$ and the voltages of an SOP from the 3 orthogonal basis. b and c are weights that can be used if needed.

3.1. Particle Swarm Optimization (PSO)

The algorithm we look to implement is particle swarm optimization, the main advantage of this algorithm is it's high versatility and ease to implement. Comparing it to some

other methods like gradient descent where we would need to solve complex partial differential equations, we will be able to find good enough solutions without having too much computational cost.

PSO is best used to find the maximum or minimum of a function defined on a multidimensional vector space. Since we will have an α and a δ for each stage we could be looking at up to $8 \times 2 = 16$ dimensions for our space.

The method is farly simple and can be described in 3 main principles:

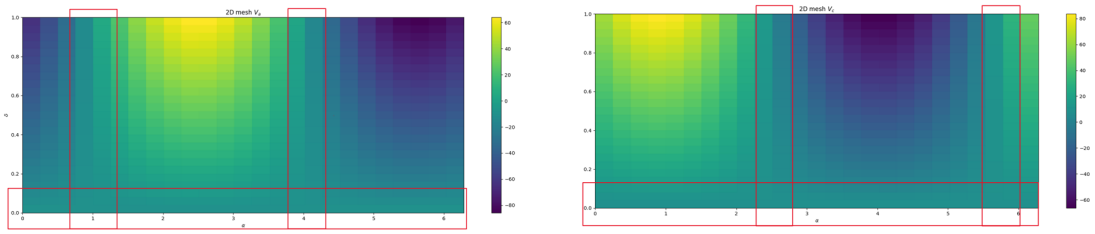
- Particles are created that exist in the variable space
- Each particle is given a score according to the position they are in trough the cost function
- Each particle knows the best score they have achieved and the position they were in, they also know the best score achieved in the group of particles and the position that particle was in

3.2. Particle Space

As discussed previously each particle will exist in a multidimensional vector space, the position of each particle is defined by the values of α and δ that it possesses for each stage.

To generate the positions of each particle we could just randomly assign them values in the space, but that would be highly inefficient and would lead to a larger number of particles or iterations needing to be done.

Instead we will take a look at the distribution of voltage values for both V_A and V_C for each stage.



(a) V_A **distribution.** **(b)** V_C **distribution.**

Figure 2. Voltage distributions for V_A and V_C for stage 1.

The areas inside the rectangles highlighted in red in the Fig.2, the placings in the figure are merely representative and not the exact limitations of the sections used, represent areas where the voltage values are fairly constant. To find the areas where we will generate our particles we calculate the standard deviation of 50 values of α and the same for δ.

We then look for the rows that fall under the 0.15 quantile of standard deviation to get the interval for δ and doing the same for the columns we get the desired interval value for α. The particles are created randomly following a uniform distribution, inside that space.

3.3. Algorithm implementation

In the current implementation of the algorithm and while having 6 available stages we found that the constants in eq.1 that provided the best results in terms of reducing the voltage range and giving exact outputs ($\leq 10^{-4}$) where a=5 and b,c=10.

This parameters could be adapted according to the number of stages we have available, for example for 2 stages we found that **a** with a higher value provided better results.

We use the algorithm to optimize the transitions between the Horizontal SOP and all other 5 SOP's. We don't optimize directly the transitions between each SOP outside of the Horizontal.

We also look for a initial optimal combination of voltages for the Horizontal SOP. The algorithm is used to find a combination of voltages close to the average of values of V_A and V_C in the initial particle space.

Due to the quite random nature of the process we are using we might not always receive the best results even after doing a large number of iterations. Increasing the number of particles to a very high value might be a easy solution but it is very intensive computationally.

In the current implementation we have 80 particles and 150 iterations. After all the iterations are complete the final values are compared to a expected performance, the expected performance is found by analysing initial runs for each of the 5 transitions.

For example we found that while having 6 stages available transitions under 8.8V for both V_A and V_B were easily achievable. If after 150 iterations of the algorithm we don't have values that indicate transitions under 8.8V, and a output SOP error under 10^{-4}, the algorithm is applied from the start with new particles inside the space being generated.

To provide some consistency in the results, once a good seed, for the random number generator, is found it can be stored and used for future runs, this provides further ways to optimize the algorithm.

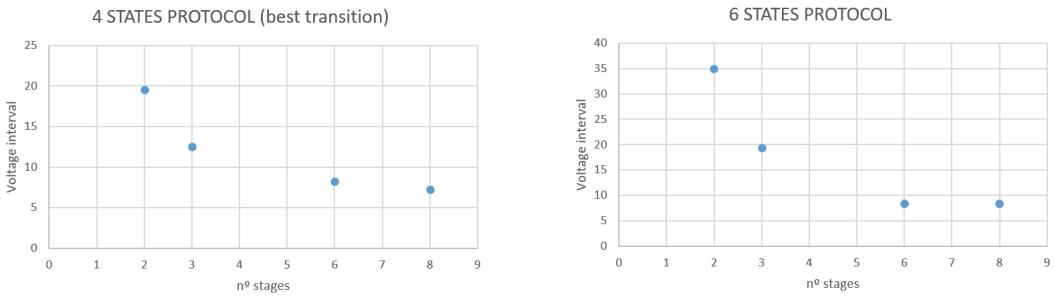
We also noticed some transition that were not optimized directly by the algorithm, like the -45 to left circular SOP, often showed somewhat higher values than all the other transitions, we can take those particular cases into account by comparing the values at the end of the 150 iterations for the transitions between the two states, and repeating the algorithm if they don't fall under a certain value. This proved to be a relatively effective method to improve those specific transitions.

3.4. Numerical algorithm results

We tested the algorithm for 8, 6, 3 and 2 stages. The only result that matters is the highest voltage interval/transition between to SOP's, since the speed of the QKD protocol that we intend to utilize will always be limited by it. We also need to take into account take we might not need all 6 SOP for protocols like BB84, so we will also look for the highest voltage intervals/transitions between the 3 basis a select the two with the lowest values for those cases.

	2 stages	3 stages	6 stages	8 stages
2 basis	19.5	12.53	8.24	7.25
3 basis	34.97	19.42	8.43	8.40

Table 1. Voltage interval values obtained



(a) Two basis QKD protocol.

(b) Three basis QKD protocol.

Figure 3. Voltage intervals from Table 1 presented in graphs with the two possibilities of number of basis to use in QKD.

We observe the expected decrease in voltage intervals with the increasing number of stages. Moreover,we can clearly see that after 6 stages the gains are fairly minimal.

4. Experimental validation

In order to validate the previous results, we have used an experimental setup that comprised an EPC with six waveplates.

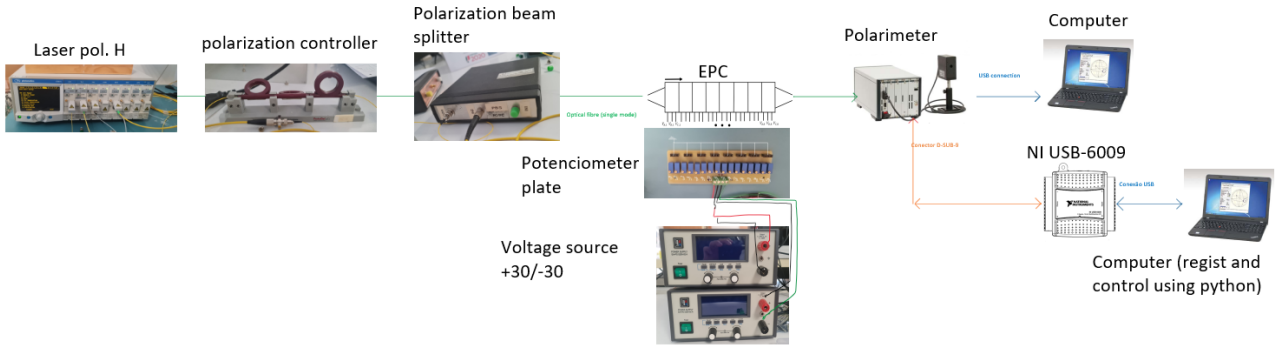


Figure 4. Lab setup used to validate the numerical results.

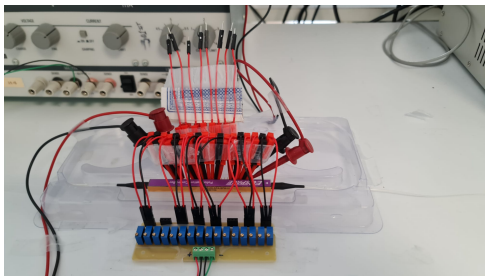


Figure 5. Detail of the EPC connections.

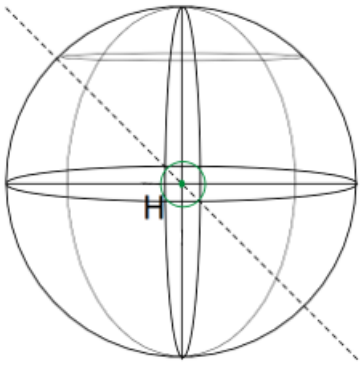


Figure 6. Schematic representation of added error range, green circle related to the exact value at the centre.

In Fig.4 we have the complete lab setup used to validate the numerical results. The output outside the laser has a Horizontal SOP, the beam splitter is used to help maintain a constant SOP at the entrance of the EPC. The voltage applied to the pins in the EPC are changed trough the use of potentiometers, Fig.5, and the values at each pin are monitored with a multimeter. The SOP can visualized trough a direct connection between the polarimeter and a computer, we also make use of a Bus-Powered USB Multifunction I/O Device (NI USB-6009) connected to a different computer to register and process measurements of the SOP at the EPC output. Ideally this setup should actuate automatically back on the EPC pins once the measurements were made, but in this test the actuation's were done by hand.

The input SOP at the entrance of the EPC is measured using the polarimeter, and it was $S_1 = 0.393$, $S_2 = 0.003$ and $S_3 = -0.895$, there are some uncertainties associated with the measurement's due to possible SOP modifications inside the optical fiber while the measurement is being done with the polarimeter, the optical fibre is not the same, they seem do be minimal. Due to the need for mechanical interactions with the EPC to measure the voltage levels at the pins, changes in the output SOP can happen, the exact numerical value for this added error is not yet measured. But a graphical representation of it's effect can be found in Fig.6.

To consider that the results obtained in theory are valid we want to achieve all 6 SOP's in under a 10V range for V_A and V_C independently. The voltage values calculated trough the algorithm are overall not applicable to the EPC mainly due to the fact that we don't know the real values of V_{pi},V_0 and $V_{A,bias}$,$V_{B,bias}$ found in equations 1 and 3, and calibration to find this values has not yet been done. Either way the configuration given by the algorithm for a Vertical SOP, was very close to a Horizontal SOP at the output of the EPC, so we used it as a starting point.

The following SOP's were found using a iterative method. We analysed the effect that each of the voltages $V_{A,1}, V_{A,2}, ..., V_{A,6}$ and $V_{C,1}, V_{C,2}, ..., V_{C,6}$, and used them accordingly. An algorithm like PSO can be applied at this stage as well.

The voltage values found for the 6 SOP are presented in the table bellow:

	H	**V**	**45**	**-45**	**circ R**	**circ L**
VA1	-17,38	-9,887	-12,85	-12,93	-18,3	-9,979
VA2	-15,02	-9,954	-13,94	-19,15	-18,18	-10,038
VA3	-10,199	-8	-12,21	-15,06	-13,36	-6,464
VA4	-2,908	-9,864	-10,824	-1,591	-4,742	-2,139
VA5	-12,22	-6,681	-9,733	-15,7	-7,693	-6,237
VA6	-14,58	-6,277	-10,547	-14,57	-10,587	-5,845
VC1	15,22	7,599	8,069	16,88	8,51	14,48
VC2	9,282	4,538	8,378	13,37	4,617	9,952
VC3	6,112	0,225	1,585	8,496	4,765	4,995
VC4	14,27	7,952	12,38	17,02	8,47	10,617
VC5	19,55	13,55	14,18	22,25	13,91	14,31
VC6	13	9,116	13,22	16,57	8,846	8,835

Table 2. Obtained voltage combinations

	2 Basis			3 Basis
	LB->DB	LB->CB	DB->CB	
Max ΔV	9,281	8,735	9,463	9,463

Table 3. Voltage transition study, Linear Basis is LB, Diagonal Basis is DB and Circular Basis is CB

We have confirmed that all 6 SOP can be achieved in under 10V. It's important to keep in account that since the EPC is a very sensible device that requires daily calibration to function correctly it's possible that by applying this voltage values to the pins,at any given day, might give an SOP that fall's a little bit outside the error band presented in Fig.6, small corrections might be necessary.

5. Conclusion

A method for optimizing the waveplate's drive voltage range of an electro-optic based EPC for qubit encoding in discrete-variable quantum key distribution (QKD) was proposed. By using a machine learning algorithm, the particle swarm optimization, we were able to reduce the required voltages to apply at each of the different waveplates that comprise the EPC. The numerical results were successfully validated through experimental data. Moreover, when comparing with the standard full range of the drive voltages, which in the employed EPC equals 140 V, our results show that such ranges can be reduced up to a maximum of 10 V. This reduction in the required range voltages for each waveplate represents a positive realization towards practical and efficient implementation of QKD protocols employing polarization encoding, as it will allow using simpler electronic drivers to control the polarization encoding subsystems.

Acknowledgment

This work is supported by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), under the project QuantumPrime reference: PTDC/EEI-TEL/8017/2020, and by FCT/MCTES through national funds and when applicable co-funded EU funds under the projects UIDB/50008/2020 and UIDP/50008/2020 (actions QuRUNNER, QUESTS, and DigCORE).

References

[DJORDJEVIC 2020] DJORDJEVIC, I. B. (2020). *Physical-layer security and quantum key distribution*. SPRINGER NATURE.

[Mantey et al. 2021] Mantey, S. T., Ramos, M. F., Silva, N. A., Pinto, A. N., and Muga, N. J. (2021). Algorithm for state-of-polarization generation in polarization-encoding quantum key distribution. In *2021 Telecoms Conference (ConfTELE)*, pages 1–6.

[Mantey et al. 2022] Mantey, S. T., Ramos, M. F., Silva, N. A., Pinto, A. N., and Muga, N. J. (2022). Demonstration of an algorithm for quantum state generation in polarization-encoding QKD systems. In *2022 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3.

[Muga 2020] Muga, N. J. (2020). Fpga-assisted state-of-polarisation generation for polarisation-encoded optical communications. *IET Optoelectronics*, 14:350–355(5).

[Muga et al. 2019] Muga, N. J., Ramos, M. F., Mantey, S., Silva, N. A., and Pinto, A. N. (2019). Deterministic state-of-polarization generation for polarization-encoded optical communications. In *2019 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)*, pages 1–3.

[Pereira et al. 2021] Pereira, D., Silva, N. A., and Pinto, A. N. (2021). A polarization diversity CV-QKD detection scheme for channels with strong polarization drift. In *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 469–470.

[Pirandola et al. 2020] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., and Wallden, P. (2020). Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236.

[Ramos et al. 2022] Ramos, M. F., Silva, N. A., Muga, N. J., and Pinto, A. N. (2022). Full polarization random drift compensation method for quantum communication. *Opt. Express*, 30(5):6907–6920.

[van Haasteren et al.] van Haasteren, A., van der Tol, J., van Deventer, M., and Frankena, H. Modeling and characterization of an electrooptic polarization controller on $LiNbO_3$, year=1993, volume=11, number=7, pages=1151-1157, doi=10.1109/50.238075. *Journal of Lightwave Technology*.