QKD optical scheme calibration system

A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin and Y. Kurochkin

1 Russian Quantum Center (RQC), Business Center «Ural», 100, Novaya st., Skolkovo, Moscow reg., 143025, Russian Federation
2 Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russian Federation
3 Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russian Federation

E-mail: a.duplinsky@rqc.ru

Abstract. One-way quantum key distribution (QKD) optical schemes require active stabilization algorithms for continuous operation. To achieve this a mathematical model for a new optical scheme has been developed. The model uses Jones calculus to describe the polarization state evolution within the optical scheme. The developed algorithms have been successfully tested experimentally.

1. Introduction

QKD is currently the most practical part of the quantum information technology. It allows unconditional secrecy of sharing keys between two distant users – the transmitter (Alice) and the receiver (Bob), the security being guaranteed by fundamental laws of quantum physics. In QKD, Alice and Bob generate a secret key by transmitting information encoded in the states of single photons or weak coherent pulses.

One-way polarization encoding optical scheme that is used in the current work requires polarization state stabilization both within the devices of Alice and Bob and the quantum channel between them [1].

2. Modelling of the scheme

For correct operation all parts of the scheme should apply a correct transformation of the polarization state. To formalize the requirements we use Jones matrixes and vectors of polarization. Note that Jones calculus are the same for both classical and quantum states of polarization. The quantum states that are implemented in the current scheme fulfil the BB84 protocol requirements (Fig. 1) [1]:

\[
\begin{align*}
\psi_1 &= \frac{1}{\sqrt{2}} \left( \left| \leftrightarrow \right\rangle + e^{i\varphi_1} \left| \uparrow \downarrow \right\rangle \right) \\
\psi_2 &= \frac{1}{\sqrt{2}} \left( \left| \leftrightarrow \right\rangle + e^{i(\varphi_1 + \pi)} \left| \uparrow \downarrow \right\rangle \right) \\
\chi_1 &= \frac{1}{\sqrt{2}} \left( \left| \leftrightarrow \right\rangle + e^{i(\varphi_1 + \pi/2)} \left| \uparrow \downarrow \right\rangle \right) \\
\chi_2 &= \frac{1}{\sqrt{2}} \left( \left| \leftrightarrow \right\rangle + e^{i(\varphi_1 + 3\pi/2)} \left| \uparrow \downarrow \right\rangle \right)
\end{align*}
\]

(1)
Note that actually $\varphi_1$ does not have to be zero and in general case the states that fit our requirements are two pairs of orthogonal ellipses. This fact significantly simplifies the procedure of guiding the light into the modulator and is exploited within the experimental setup that we present.

Fig. 1 States generated by Alice on the Poincare sphere.

3. Calibration algorithm

As we cannot directly measure the elements of the Jones matrices for every section, we establish a set of observed values to implement the calibration. We use the counts of the single photon detectors for calibration of all the piezo-driven polarization controllers within the scheme.

For every controller a parameter for minimization is chosen. We went through several iterations of the algorithm for minimization before we chose one that fitted our needs best.

The first version of the minimization process was through scanning the whole range of the parameter while changing voltages applied to the polarization controllers. The minimal value was stored in memory as well as its position, and after all the values of voltage had been checked, the algorithm started to search for a value close enough to the found minimum. “Close enough” is an allowed percentage of deviance, chosen empirically to balance precision and search time. The problem with this version was that due to the existence of a random noise component in our parameter, and a non-zero search time during which the polarization could drift, the algorithm could often not find a value close enough to the minimum on its second passing (Fig. 2), which resulted in the repetition of the process, often with the same results.

For the same reasons our second version also didn’t suit us – we tried returning to the position of the minimum in terms of voltage, ignoring its value. But again, after the search time, the minimum would often shift from its old position, enough that the desired precision required to reach a low error rate would not be met.
Finally, we chose the gradient descent approach to find the minimal value. It does not require a second passing over the voltage values, which means that the minimal parameter value is found in real time. But because of the same existing noise components and drift over time, certain problems arose, limiting the stop conditions that we could use to find the minimum effectively.

In gradient descent, the following conditions are used most often to decide when the algorithm should stop: 1) when the change in parameter becomes lower than a certain threshold; 2) when the direction of the search changes repeatedly more than a certain amount of times; 3) a fixed number of steps is applied. Since the change in parameter has a random component, the first and second approaches cannot be applied, since the stop condition might be reached either too early, or it will never trigger even close enough to the minimum. Through experiment we found that option 3 is the most optimal. The algorithm runs a fixed amount of steps on each voltage channel, repeating the process if necessary until the global stop condition (an acceptable QBER) is reached.

4. Requirements for calibration.
Let us briefly summarize the requirements for the SOPs described above:

1) At the input of Alice’s phase modulator, the components along ordinary and extraordinary axes are equal
2) At the input of Bob’s modulator, the components swap
3) Bob’s measurements differentiate BB84 orthogonal states with extinction higher than 98%.

These requirements can be formulated mathematically by defining the Jones matrices for each of the scheme’s sections.

The first section connects the laser source and Alice’s phase modulator. We assume the incident light to be linearly polarized. To fulfil the criterion 1 the transformation of this section has to be:

$$\frac{\sqrt{2}}{2} \begin{bmatrix} e^{i\phi_1} & 1 \\ 1 & e^{-i\phi_1} \end{bmatrix}$$

The second section lies between Alice’s and Bob’s modulators and includes QC. According to the condition 2 the overall transformation of this part should be:
\[ \left\| \begin{array}{cc} 0 & 1 \\ e^{i\varphi_2} & 0 \end{array} \right\| \]  \hspace{1cm} (3) 

Finally, the condition 3 is implemented by section between Bob’s modulator and the PBS:

\[ \frac{\sqrt{2}}{2} \left\| \begin{array}{cc} e^{i\varphi_3} & 1 \\ 1 & e^{-i\varphi_3} \end{array} \right\| \]  \hspace{1cm} (4) 

All three sections may introduce arbitrary relative phase shifts (\(\varphi_1, \varphi_2, \varphi_3\)) between the polarization components, but in order for PBS to distinguish the states correctly their sum should be divisible by 2\(\pi\):

\[ (\varphi_1 + \varphi_2 + \varphi_3) : 2\pi \]  \hspace{1cm} (5) 

This is required as production of the matrices (2), (3) and (4) should be equal to identity matrix. Note that \(\varphi_1\) mentioned in sec. 2 is a result of the transformation (2) that is applied in the first section.

5. Conclusions

We have provided the necessary mathematical conditions and algorithm required for the operation of a single-pass polarization-encoding QKD scheme of our own design. The conditions are based on the Jones matrix formalism used to describe the polarization state of light. The algorithm of choice is the gradient descent method, although not all of its versions can be used in experimental conditions, due to the existence of a random noise component in the parameters for minimization and their drift over time.

The stabilization feedback system based on the calibration algorithm proved itself reliable both for laboratory and urban communication channels. The system has also been used as a link within the quantum network [2]. The calibration procedure was performed automatically and maintained QBER below 5% for hours, applying recalibration if needed. Average time that the system has spent in the data transfer mode is about 80%, while the other 20% has been required for recalibrations.

6. Acknowledgements

The support from Ministry of Education and Science of the Russian Federation in the framework of the Federal Program (Agreement 14.582.21.0009, ID RFMEIF58215X0009) is acknowledged.

7. References

[1] Duplinskiy A, Ustimchik V, Kanapin A and Kurochkin Y 2016 Proc. SPIE 10224 102242W
[2] Kiktenko E, Pozhar N, Duplinskiy A, Kanapin A, Sokolov A, Vorobey S, Miller A, Ustimchik V, Anufriev M, Trushechkin A, Yunusov R, Kurochkin V, Kurochkin Y, Fedorov A, “Demonstration of a quantum key distribution network across urban fiber channels”, \textit{arXiv:1705.07154}