Conference materials
UDC 535
DOI: https://doi.org/10.18721/JPM.163.216

Real-time calibration methods for a commercial MDI-QKD system

N.V. Rudavin[3,5]✉, I.S. Gerasin[1,2,3,4], P A. Kupriyanov[1,2,3,4],
A.P. Dvurechenskiy[1,2,3,4], R.A. Shakhovoy[1,2,3,4]

[1]QRate, Moscow, Russia;

[2]Moscow Institute of Physics and Technology, Dolgoprudny, Moscow Region, Russia;

[3]NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia;

[4]Russian Quantum Center, Skolkovo, Moscow, Russia;

[5]HSE University, Moscow, Russia

✉ n.rudavin@goqrate.com

Abstract. Quantum key distribution (QKD) is a well-studied field of science and is becoming a common technology. Commercial systems become more available. Such systems require high level of automatization, so, the set of real-time and prior calibrations is required for them. In this work, we propose calibration algorithms that pre-tune the amplitude of pulses and the laser wavelength and also maintain phase and polarization of weak coherent pulses during generation. Described algorithms were implemented on a prototype of the commercial QKD system and demonstrated high results.

Keywords: quantum key distribution, phase fluctuation, polarization distortion

Funding: The study was commissioned by JSCo RZD.

Citation: Rudavin N.V., Gerasin I.S., Kupriyanov P.A., Dvurechenskiy A.P., Shakhovoy R.A., Features of the construction photonic tensor cores for neural networks, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.2) (2023) 97–102. DOI: https://doi.org/10.18721/JPM.163.216

Материалы конференции
УДК 535
DOI: https://doi.org/10.18721/JPM.163.216

Методы калибровки в реальном времени системы детектор-независимого КРК

Н.В. Рудавин[3,5]✉, И.С. Герасин[1,2,3,4], П.А. Куприянов[1,2,3,4],
А.А. Двуреченский[1,2,3,4], Р.А. Шаховой [1,2,3,4]

[1] КуРэйт, Москва, Россия;

[2] Московский физико-технический институт, Московская область, г. Долгопрудный, Россия;

[3] НТИ Центр квантовых коммуникаций, Национальный исследовательский технологический университет «МИСИС», Москва, Россия;

[4] Российский Квантовый центр, Сколково, Москва, Россия;

[5] Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

✉ n.rudavin@goqrate.com

Аннотация. Квантовое распределение ключей (КРК) является хорошо изученной областью науки и становится распространенной технологией. Коммерческие системы становятся более доступными. Такие системы требуют высокого уровня автоматизации, поэтому для них требуется набор предварительных калибровок, а также калибровок, которые поддерживают рабочее состояние системы в реальном времени. В данной работе мы предлагаем алгоритмы калибровки, которые предварительно настраивают амплитуду импульсов и длину волны лазера, а также поддерживают фазу и поляризацию слабых когерентных импульсов во время генерации. Описанные алгоритмы были реализованы на прототипе коммерческой системы КРК и показали высокие результаты.

Ключевые слова: квантовое распределение ключей, флуктуации фазы, искажения поляризации

Финансирование: Исследование выполнено по заказу ОАО «РЖД».

Ссылка при цитировании: Рудавин Н.В., Герасин И.С., Куприянов П.А., Двуреченский А.А., Шаховой Р.А., Методы калибровки в реальном времени системы детектор-независимого КРК // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.2. С. 97—102. DOI: https://doi.org/10.18721/JPM.163.216

Introduction

The amount of information transmitted via the Internet is rapidly increasing and this information needs to be protected. In contrast to quantum cryptography, classical cryptography has vulnerabilities that allow the eavesdropper to gain (at least, in principle) unauthorized access to sensitive data [1]. When this became clear, it became necessary to develop commercial quantum key distribution (QKD) systems.

From a technical point of view, modern QKD systems consisting of a receiver and a transmitter are complex devices that include many components, which are not calibrated by default. Therefore, before starting the key generation process, it is necessary to calibrate all its components. Moreover, it is necessary to develop calibration algorithms most appropriate for the selected QKD protocol and encoding methods and pertinent to the characteristics of the internal components. The calibration system must ensure the correct operation of the QKD setup corresponding to the security requirements of the key distribution. In the measurement-device-independent (MDI) QKD system [2], calibrations are required not only for the receiver and transmitter, but also for the untrusted node. The latter should be configured in such a way that both transmitters could interact with it properly.

Calibration of the QKD system can be divided into 2 stages: initial and real-time. During the initial calibration, one should conFig. the components, whose properties will be constant over time and will not require occasional reconfiguration. In contrast, the purpose of real-time calibrations is a periodic adjustment of the operating parameters of the system to ensure the correctness of the key generation process.

In this work, we describe the most essential calibration techniques needed to ensure maximum visibility of the interference of weak coherent pulses on the beam splitter of our experimental MDI-QKD system.

Materials and Methods

To obtain high interference visibility in the MDI QKD experiment, photons (or rather weak coherent pulses) from both transmitters must be fully indistinguishable. It means that it is necessary to align optical pulses in all their degrees of freedom: frequency, polarization, intensity, and spatiotemporal characteristics.

When using lasers with high thermal stability, their frequencies can be aligned just at the initial calibration. The corresponding calibration procedure we propose is based on measuring the beat frequency observed in the interference pattern of laser beams. To perform the calibration, we input the light from the lasers into a 50:50 beam splitter and acquire the beats with a photodetector. The photodetector output is analyzed with an oscilloscope, where we perform the Fourier transform of the beats to determine the beat frequency. By changing the temperature of one of the lasers, we minimize the beat frequency thereby minimizing detuning between the lasers.

To obtain optical pulses from the continuous laser beam, we use fiber lithium niobate intensity modulators. It is well-known that one should control the bias voltage level of the lithium niobate intensity modulators during operation [3]. Due to the very low bias voltage drift of the modulators that we used in this work, we have decided to use an adjustment algorithm based on a simple proportional controller (P controller) to regulate it:

$$V_n = V_{n-1} - \alpha\left(P_t - P_n\right),$$

where V_n and V_{n-1} are the bias voltages at the current and previous steps respectively, α is the proportional coefficient, P_t is the target value of optical power, P_n is the average value of the optical power at step n of the algorithm. The values P_t and P_n are measured using power meters built into the transmitters. The target value of optical power P_t is determined by maximizing the signal-to-noise ratio measured on single photon detectors (SPD). This P_t choice allows us to achieve the best cutting of optical pulses. Since our setup uses time-bin quantum states encoding, the signal-to-noise ratio for the signal states gives a direct contribution to the quantum bit error rate (QBER) value.

As for the intensity calibration, we introduced the procedure that chooses one of the senders as a master and the second one as a slave and changes the attenuation on the slave to match the master's power. Instead of a power, we measure the total number of clicks on all SPDs for each transmitter separately. It is important for this calibration to make sure that all the SPDs work in linear mode, and that the transmitters send the same pulse sequences. Since the values of losses introduced by tunable optical attenuators on transmitters are constant in time, this calibration is carried out only at the stage of initial setup.

Since the quantum channel is generally a single-mode optical fiber that does not preserve polarization, the polarization of the optical pulse transmitted through such a channel is not correlated with the initial polarization by default. As mentioned earlier, to ensure acceptable visibility of interference, the pulses coming to the beam splitter from two transmitters must be indistinguishable in each degree of freedom including polarization. In the case of time-bin encoding, a polarizing filter coupler (a beam splitter with built-in polarizer) can be used to match the polarization at the receiver inputs. Then a change of polarization in each arm will lead to a change in relative intensities of incoming pulses. It can be shown that an acceptable level of polarization distortions in the case of time-bin encoding is noticeably higher than in the case of polarization encoding. Therefore, the use of time-bin encoding with interference on a polarizing filter coupler makes it possible to significantly reduce the sensitivity of the error level to polarization fluctuations in the channel. In addition, the polarizer guarantees the indistinguishability of independent pulses in the polarization mode, and the error of the polarization distortion compensation algorithm will affect only the intensity of interfering pulses, which does not significantly reduce the quality of interference.

To compensate for polarization distortions, we have designed a polarization control system with two piezo-controlled polarization controllers. Such controllers are driven by an external electrical voltage, are compact enough, and allow for good autonomy and reliability of QKD systems in real conditions. To regularly recover the state of polarization at the receiver by means of the polarization controllers, an active algorithm based on gradient descent was developed [4]. The adjustment is performed periodically in the key generation mode by alternately changing the voltage on the channels of the controllers.

From a mathematical point of view, compensation of polarization distortions is a task of optimizing the objective function. The QBER was used as the objective function in [4], which was estimated in the generation mode according to statistics obtained from the analysis of detected decoy states. In MDI QKD, we generally do not have large enough sifted keys (particularly at high distances); therefore, it is inconvenient to use QBER as the objective function. The task of the polarization control is reduced here to the task of maximizing the total number of clicks, which corresponds to the maximization of the pulse intensity. As usually, this can be done by selecting the optimal set of voltages on the piezo actuators of the polarization controller. Except for using a different objective function, the polarization adjustment algorithm is similar to the one proposed in [4].

SPDs in our setup operate in a gating mode – a sinusoidal voltage is applied to each SPD. When the voltage exceeds the threshold value, the detector switches to the operating mode and can register the pulses coming to it. The detector is in the open state for about 1 ns with a total period of 3.2 ns. The phase of the detector corresponds to the moment of opening the gate. Since we can register a signal pulse only when the detector is “open”, it is necessary to calibrate the optimal phase value within the reference signal period. When calibrating, we change the value of the phase (the time of the gate appearance), scanning the entire period.

Also, to obtain good visibility of the interference pattern, it is necessary that the time of arrival (phase) of laser pulses from both transmitters was the same. To perform this, the phase (spatial) alignment is required [5]. At the first stage of calibration, optical pulses are sent only by the master transmitter, and the phases of all SPDs are adjusted to them. In the second stage, a similar sequence of pulses is sent by the slave transmitter, and the corresponding phase shift is determined. Further, using the difference in phase shifts for the two transmitters, the slave adjusts to the master by changing the values of the delay lines. For rough alignment of optical pulses, a time shift of the intensity modulator with a step of 400 ps is used. The 400 ps is determined by the DAC used to control the modulator. For more precise alignment, a tunable optical delay line (TODL) installed in one of the receiver arms is used. Thus, it is possible to achieve a high degree of alignment of the arrival time of optical pulses from two transmitters. This setting is performed at the initial stage of calibration.

However, temperature variations in the fiber and physical influences on it change the time of arrival of laser pulses, so, the phase calibration must be performed in real-time during the generation mode. Since the number of detector clicks is used as a feedback control parameter, together with the synchronizing sequences, we send short calibration pulse sequences between the signal pulse sequences [6]. Like the primary calibration, the transmitters are tuned alternately, using calibration sequences as feedback. The need for these sequences is due to the use of time-bin encoding, in which the SPDs are configured to register certain quantum states. Note that these sequences are not used to generate a secret key.

As a result of changing the pulse arrival time, it is also possible to change the numbering of packages. Synchronization of package numbering at all nodes of the QKD system is necessary for the subsequent sifting procedure provided for by the MDI-QKD protocol. The sifting procedure refers to the reconciliation of the bases of pulse numbers from the transmitters, which corresponds to a successful event at the receiver.

Initially, the numbering of packages is set up at the initial stage of calibration, two mechanisms have been developed for it to set the general numbering of parcels. The first uses a change in the delay time of the generation of the first laser pulse in the signal sequence on the transmitter, thereby changing the numbering of the parcels. As mentioned earlier, pulse generation is performed by the intensity modulator, so in this case, the moment when the high-frequency signal is applied to the modulator changes. The second mechanism allows to adjust of the delay in the SPD electrical channels, i.e., allows to shift of the numbering of packages on the receiver.

The electrical channels connecting the SPDs to the FPGA control board have different lengths, which is why pulses registered at the same time on different SPDs can reach the FPGA at times corresponding to different periods of the clock signal on the control board. To solve this problem, we use additional individual delays in the channel of each SPD with a maximum delay equal to 7 reference signal periods.

Calibration is performed alternately for each transmitter. It is important to note that to calibrate the package numbering, the transmitter should send a pseudo-random, not a periodic sequence of laser pulses. At the same time, the receiver needs to know in advance which sequences the transmitter will send to detect a correlation between the received and expected sequence by going through the period numbers. To do this, a pseudo-random calibration sequence of pulses is used, which is known to all nodes in the QKD system. The transmitter performs calibration by iterating over the period numbers using a 128-period delay line. Accordingly, the shift of the package numbering on the calibrated transmitter modulator should not exceed 128 periods. Then the found delays are applied to the intensity modulators of the transmitters. Delays for phase modulators are also determined based on the delays of intensity modulators.

The described package numbering calibrations are applied in the generation mode if the QBER level, estimated by decoy states statistics, becomes equal to 50%, which may indicate that there is no synchronization of numbers. Accordingly, for this calibration, the generation mode is interrupted, and the system switches to calibration mode. If, after numbers synchronization recalibration, the QBER level remains above the threshold value, the algorithm for the primary calibration of the QKD system is started.

Results and Discussion

With the described methods, we run the key generation procedure on the prototype of the MDI-QKD system and measured second order correlation function, click count and QBER. During the experiment, both Alice and Bob were connected to Charlie by 75 kilometers of standard single-mode telecommunication optical fiber SMF-28e. Alice and Bob's fiber was in the same room under the same conditions. As signal lasers with high-temperature stability we used Koheras BASIK from NKT Photonics. As power meters for bias control were used Thorlabs PM101A, as photodetector and oscilloscope for lasers frequency calibration were used Thorlabs RXM40AF and Lecroy Waverunner 8404MR respectively. We can see that the number of clicks on each SPD is kept at the level from 5500 to 5900 clicks throughout the experiment (see Fig. 1).

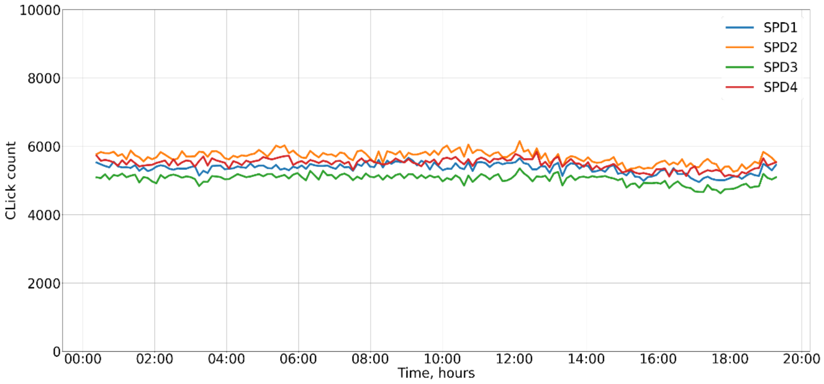

Fig. 1. Number of clicks on SPDs with total 150 km of fiber for 19 hours

Since we used weak coherent states with random phase, the minimum achievable value of second order correlation function was 50%, we obtained 52%. Fig. 2 shows the dependence of QBER estimated by signal states. The general level of error is about 6%, and an outlier of the error level of up to 8% was also recorded about 15 hours of the experiment. We believe that this outlier is due to the imperfection of the bios control algorithm used, which caused a temporary change of the signal-to-noise ratio for the signal states. Since the obtained values are appropriate for key generation, the experiment confirmed that the proposed calibration algorithms can be used in MDI-QKD experimental system.

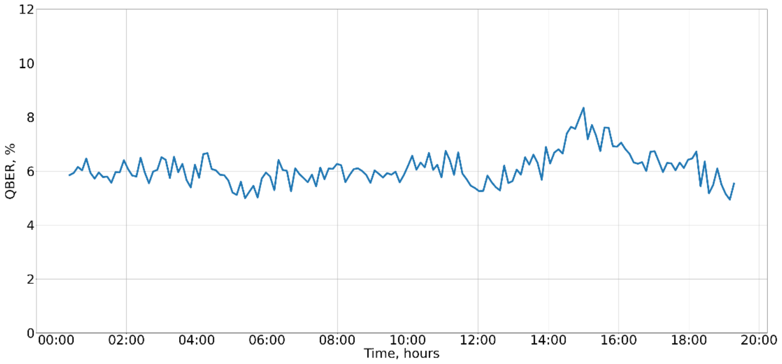

Fig. 2. QBER with total 150 km of fiber for 19 hours

Conclusion

In this work, we demonstrated the most essential calibration techniques needed to ensure maximum visibility of the interference of weak coherent pulses on the beam splitter of our experimental MDI-QKD system. Using the described initial and real-time calibrations, we obtained stable QBER and number of clicks on SPDs, which allowed us to start key generation. Importantly, described algorithms allows us not to interrupt the key generation process with any change in the optical path length, which increases the speed of the secret key.

REFERENCES

1. **Gisin N., Ribordy G., Tittel W., Zbinden H.,** Quantum cryptography, Reviews of modern physics 74.1 (2002) 145.

2. **Lo H.K., Curty M., Qi, B.,** Measurement-device-independent quantum key distribution, Physical review letters 108.13 (2012) 130503.

3. **Wooten E.L., Kissa K.M., Yi-Yan A., Murphy E.J., Lafaw D.A., Hallemeier P.F., et al.,** A review of lithium niobate modulators for fiber-optic communications systems, IEEE Journal of selected topics in Quantum Electronics 6.1 (2000) 69–82.

4. **Mekhtiev E.E., Gerasin I.S., Rudavin N.V., Duplinsky A.V., Kurochkin Y.V.,** Polarization control algorithm for QKD systems, Journal of Physics: Conference Series. Vol. 2086. No. 1. IOP Publishing, 2021.

5. **Hiskett P.A., Rosenberg D., Peterson C.G., Hughes R.J., Nam S., Lita A. E., et al.,** Long-distance quantum key distribution in optical fiber, New Journal of Physics 8.9 (2006) 193.

6. **Rudavin N.V., Gerasin I.S., Mekhtiev E.E., Duplinsky A.V.,** Synchronization protocol for MDI-QKD systems, St. Petersburg State Polytechnical University Journal: Physics and Mathematics. 15.S3. 2 (2022) 56–60.

THE AUTHORS

RUDAVIN Nikita V.
n.rudavin@goqrate.com
ORCID: 0000-0003-0264-5710

GERASIN Ilya S.
i.gerasin@goqrate.com
ORCID: 0000-0001-5084-7056

KUPRIYANOV Pavel A.
p.kupriyanov@goqrate.com
ORCID: 0009-0006-1663-6806

DVURECHENSKIY Alexander P.
a. dvurechenskiy@goqrate.com
ORCID: 0009-0008-7391-0079

SHAKHOVOY Roman A.
r.shakhovoy@goqrate.com
ORCID: 0000-0003-2750-0518

Received 13.07.2023. Approved after reviewing 15.09.2023. Accepted 15.09.2023.