Conference materials
UDC 535
DOI: https://doi.org/10.18721/JPM.163.211

Influence of quantum states imperfections on the error rate in measurement-device-independent quantum key distribution

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

[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

✉ kupriianov.pa@phystech.edu

Abstract. Quantum key distribution (QKD) is a modern technology that allows two legitimate users obtaining a shared cryptographic key completely secure. Unfortunately, real implementations of QKD systems contain vulnerabilities, such that an eavesdropper can still get information about the key. Therefore, QKD protocols generally use privacy amplification procedures that reduce the size of the key depending on the level of errors that are generally assumed to be caused by a non-legitimate user. So, the quantum bit error rate (QBER) becomes an important parameter significantly affecting the rate of key distribution. In this work, we investigate the influence of quantum states imperfections on the QBER in the measurement-device-independent QKD protocol with time-bin encoding. We proposed a theoretical model that describes imperfect states, and derived formulas for the dependence of the error level on the degree of imperfection. We also conducted an experiment, the results of which are in good agreement with the predictions of the theory.

Keywords: measurement-device-independent quantum key distribution, imperfect states, time-bin phase-encoding

Funding: The study was commissioned by JSCo RZD.

Citation: Kupriyanov P.A., Rudavin N.V., Gerasin I.S., Dvurechensky A.P., Petrov I.V., Menskoy D.D., Shakhovoy R.A., Influence of quantum states imperfections on the error rate in measurement-device-independent QKD, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.2) (2023) 69–74. DOI: https://doi.org/10.18721/JPM.163.211

Материалы конференции
УДК 535
DOI: https://doi.org/10.18721/JPM.163.211

Влияние неидеальностей приготовления квантовых состояний на уровень ошибок в детектор-независимом квантовом распределении ключей

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

✉ kupriianov.pa@phystech.edu

Аннотация: Квантовое распределение ключей (КРК) – современная технология, позволяющая двум законным пользователям безопасно получить общий криптографический ключ. К сожалению, реальные системы КРК содержат уязвимости, так что у перехватчика появляется потенциальная возможность получить информацию о ключе. Поэтому протоколы КРК обычно используют процедуры усиления секретности, которые уменьшают размер ключа в зависимости от уровня ошибок, которые, как правило, считаются вызванными нелегитимным пользователем. Таким образом, важным параметром, существенно влияющим на скорость распределения ключей, становится квантовый уровень битовых ошибок (QBER). В этой работе мы исследуем влияние несовершенства квантовых состояний на QBER в протоколе детектор-независимого КРК на фазово-временном кодировании. Мы предложили теоретическую модель, которая описывает неидеальные состояния, и вывели формулы зависимости уровня ошибок от степени неидеальности. Также был проведен эксперимент, результаты которого хорошо согласуются с предсказаниями теории.

Ключевые слова: квантовое распределение ключей, неидельность приготовления состояний, фазово-временное кодирование

Финансирование: Исследовательская работа выполнена по заказу ОАО «РЖД».

Ссылка при цитировании: Куприянов П.А., Рудавин Н.В., Герасин И.С., Двуреченский А.А., Петров И.В., Менской Д.Д., Шаховой Р.А., Влияние неидельностей квантовых состояний на уровень ошибок в детектор-независимом КРК // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.2. С. 69–74. DOI: https://doi.org/10.18721/JPM.163.211

Introduction

Measurement-device-independent QKD protocol [1] is resistant to all detector-side attacks. The main feature of this protocol is that two transmitters (Alice and Bob), who want to distribute a secret key, prepare quantum states and send them to an untrusted central node (Charlie). Quantum states are entangled on the beam splitter and then Charlie performs Bell state measurement. Such measurements can give an eavesdropper information only about the mutual correlation of transmitters bits, not about values. This allows the protocol to eliminate all vulnerabilities associated with measurement devices. But there is still a gap between theory and practice that can be used by an eavesdropper to obtain information about the secret key. One of the vulnerabilities is the imperfect preparation of quantum states. In the article [2] QKD on polarization encoding with non-ideal sources was experimentally demonstrated.

Our experimental setup uses time-bin encoding [3], for which the intensity modulator cuts out short pulses from the continuous laser. If Alice prepares "0" in the *X*-basis, then equal pulses are created in both time slots (we refer them to *E*- and *L*-pulses, i.e., early and late). In case of sending "1", it is necessary to additionally apply the phase π between the pulses. For the *X*-basis, there is always a slight intensity difference between the pulses in different time slots as well as deviation of the phase difference from 0 or π. Preparing states in the *Z*-basis, intensity modulator creates a pulse in only one of the two time slots. Here, non-ideality is related to the fact that "empty" time slot still contains some non-zero intensity. These imperfections lead to false clicks of detectors and to an increase in quantum bit error rate (QBER).

Materials and Methods

We first considered the problem of the interference of weak coherent pulses on a beam splitter. Alice and Bob send *L*-pulses with intensities s_a and s_b, respectively, while the time slot corresponding to the *E*-pulse gets noise intensities ζ_a and ζ_b, caused by imperfect operation of the amplitude modulator. The mutual state of Alice and Bob can be thus written as

$$\left|Z_1Z_1\right\rangle_{ab} = \left|\sqrt{\zeta_a}e^{i\varphi_a}\right\rangle_{a_E}\left|\sqrt{s_a}e^{i\varphi_a}\right\rangle_{a_L}\left|\sqrt{\zeta_b}e^{i\varphi_b}\right\rangle_{b_E}\left|\sqrt{s_b}e^{i\varphi_b}\right\rangle_{b_L}. \quad (1)$$

Indices *a* and *b* denote states of Alice and Bob respectively, indices *E* and *L* denote early and late time modes.

As is known, complex amplitudes representing coherent pulses at the input of the beam splitter are added and subtracted at the output ports [3]. Thus, after passing through quantum channels with losses t_a and t_b respectively and after interference at the beam splitter, the states will have the form:

$$\begin{aligned}\left|Z_1Z_1\right\rangle_{cd} = &\left|e^{i\varphi_a}\sqrt{\frac{t_a\zeta_a}{2}}+e^{i\varphi_b}\sqrt{\frac{t_b\zeta_b}{2}}\right\rangle_{c_E}\left|e^{i\varphi_a}\sqrt{\frac{t_as_a}{2}}+e^{i\varphi_b}\sqrt{\frac{t_bs_b}{2}}\right\rangle_{c_L}\otimes\\ \otimes&\left|e^{i\varphi_a}\sqrt{\frac{t_a\zeta_a}{2}}-e^{i\varphi_b}\sqrt{\frac{t_b\zeta_b}{2}}\right\rangle_{d_E}\left|e^{i\varphi_a}\sqrt{\frac{t_as_a}{2}}-e^{i\varphi_b}\sqrt{\frac{t_bs_b}{2}}\right\rangle_{d_L}.\end{aligned} \quad (2)$$

Indices *c* and *d* denote output ports of beam splitter.

We calculated the gain corresponding to the clicking of detectors in orthogonal time modes. When sending the same bits in the *Z*-basis, such events will lead to errors:

$$\begin{aligned}Q^{Z,err}_{s_as_b} = y_{s_a,s_b}y_{\zeta_a,\zeta_b}\Big(&2y_{s_a,s_b}y_{\zeta_a,\zeta_b}-2y_{\zeta_a,\zeta_b}I_0(x_{s_a,s_b})+I_0(x_{s_a,s_b}-x_{\zeta_a,\zeta_b})-\\ &-2y_{s_a,s_b}I_0(x_{\zeta_a,\zeta_b})+I_0(x_{s_a,s_b}+x_{\zeta_a,\zeta_b})\Big),\end{aligned} \quad (3)$$

where $y_{\nu,\mu} = (1-p_{dc})e^{-\eta(t_a\nu+t_b\mu)/4}$, $x_{\nu,\mu} = (\eta/2)\cdot\sqrt{t_at_b\nu\mu}$, and $I_0(x)$ is a modified Bessel function of the first kind. In our model, we assume that probability of dark counts p_{dc} and efficiency η are the same for all detectors.

Similarly, considering the sending of different bits in the *Z*-basis, we calculated the gain for correct events $Q^{Z,corr}_{s_a,s_b}$.

$$\begin{aligned}Q^{Z,corr}_{s_as_b} = y_{\zeta_a,s_b}y_{s_a,\zeta_b}\Big(&2y_{\zeta_a,s_b}y_{s_a,\zeta_b}-2y_{s_a,\zeta_b}I_0(x_{\zeta_a,s_b})+I_0(x_{\zeta_a,s_b}-x_{s_a,\zeta_b})-\\ &-2y_{\zeta_a,s_b}I_0(x_{s_a,\zeta_b})+I_0(x_{\zeta_a,s_b}+x_{s_a,\zeta_b})\Big),\end{aligned} \quad (4)$$

QBER in *Z*-basis can be calculated with the formula:

$$E^Z_{s_a,s_b} = \frac{e_dQ^{Z,corr}_{s_a,s_b}+(1-e_d)Q^{Z,err}_{s_a,s_b}}{Q^{Z,corr}_{s_a,s_b}+Q^{Z,err}_{s_a,s_b}}, \quad (5)$$

where e_d denotes the probability of error in the detection system, which can be caused by distortions in the quantum channel that were not considered in our model.

In the X-basis, the imperfect phase between the E- and L-pulses leads to additional errors. If we do not accurately select the voltage supplied to the phase modulator, an erroneous phase difference $\delta\Theta_{ab}$ appears. In a similar way, we calculated QBER for the X-basis:

$$Q^{X,err}_{\gamma_a,\gamma_b} = 2y_{\gamma_a,\gamma_b}y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}\left(y_{\gamma_a,\gamma_b}y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b} - y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}I_0(x_{\gamma_a,\gamma_b}) - \right.$$
$$\left. - y_{\gamma_a,\gamma_b}I_0(x_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}) + I_0\left(\sqrt{x^2_{\gamma_a,\gamma_b} + x^2_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b} - 2x_{\gamma_a,\gamma_b}x_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}\cos\delta\Theta_{ab}}\right)\right), \quad (6)$$

$$Q^{X,corr}_{\gamma_a,\gamma_b} = 2y_{\gamma_a,\gamma_b}y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}\left(y_{\gamma_a,\gamma_b}y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b} - y_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}I_0(x_{\gamma_a,\gamma_b}) - \right.$$
$$\left. - y_{\gamma_a,\gamma_b}I_0(x_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}) + I_0\left(\sqrt{x^2_{\gamma_a,\gamma_b} + x^2_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b} + 2x_{\gamma_a,\gamma_b}x_{\gamma_a+\delta\gamma_a,\gamma_b+\delta\gamma_b}\cos\delta\Theta_{ab}}\right)\right), \quad (7)$$

$$E^X_{\gamma_a,\gamma_b} = \frac{e_d Q^{X,corr}_{\gamma_a,\gamma_b} + (1-e_d)Q^{X,err}_{\gamma_a,\gamma_b}}{Q^{X,corr}_{\gamma_a,\gamma_b} + Q^{X,err}_{\gamma_a,\gamma_b}}. \quad (8)$$

Here γ denotes intensity in the Early time slot in X-basis, $\delta\gamma$ denotes the difference between intensities in Late and Early time slots.

In order to verify our model, we set up an experiment in which we measured QBER depending on the level of noise. Since the formula (3) includes detector parameters such as efficiency and probability of dark count, it was necessary to conduct auxiliary experiment, in which the dependence of the number of detector clicks N_d on the power of weak coherent pulses was investigated. This dependence is described by the formula:

$$N_d = \frac{(1-(1-p_{dc})e^{-\eta\mu})N_t}{1+(1-(1-p_{dc})e^{-\eta\mu})f\tau}, \quad (9)$$

where f is the pulse repetition frequency, N_t is the number of pulses, that were sent during the time t. Fitting the experimental data we found parameters of detectors: probability of dark count and efficiency (Fig. 1).

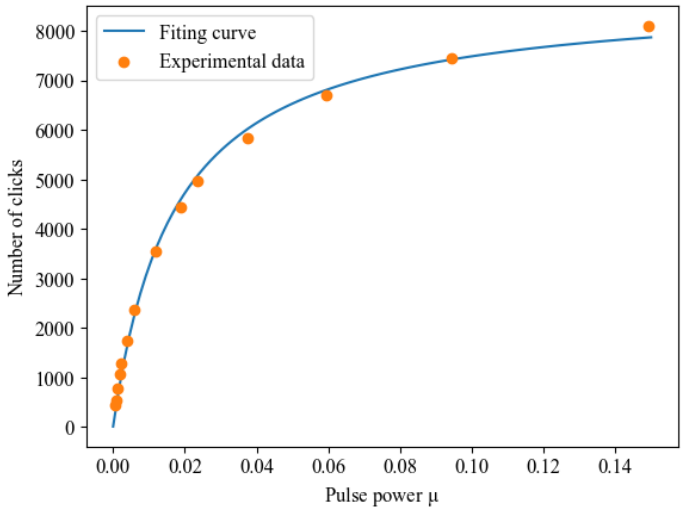

Fig. 1. Dependence of clicks on the power of pulse

The transmission function of the intensity modulator from the voltage is the cosine shifted up along the ordinate axis [5]. By changing the modulator bias, we can displace the operating point and vary the ratio of noise power to signal pulse power. For each bias value, we sent to Charlie pattern of the same *E*-pulses, scanned the detector phase (Fig. 2) by changing the position of the detector strobe relative to the arrival time of the pulses. From the graph, we obtained values N_s and N, i.e., the number of clicks corresponding to the signal pulses and the number of noise clicks, respectively. N_s is equal to the maximum number of clicks. N is equal to the average number of clicks that are shifted by half a period from the maximum, since the orthogonal detectors are shifted relative to each other by half a period. Then, using the calibration graph of the detector, we found the power values s and ζ that correspond to these numbers. Selecting shifts and attenuation in such a way that the signal pulse power and the noise power are equal for both transmitters, we have measured averaged QBER in key generation mode.

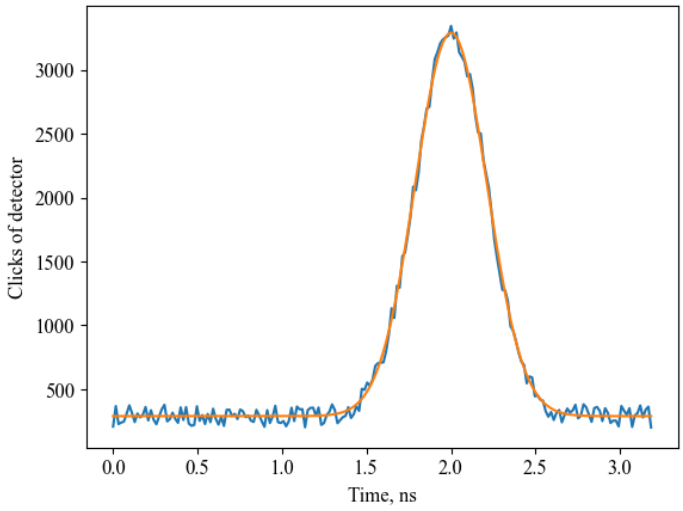

Fig. 2. Dependence of clicks on the arrival time of pulse
Orange line denotes moving average

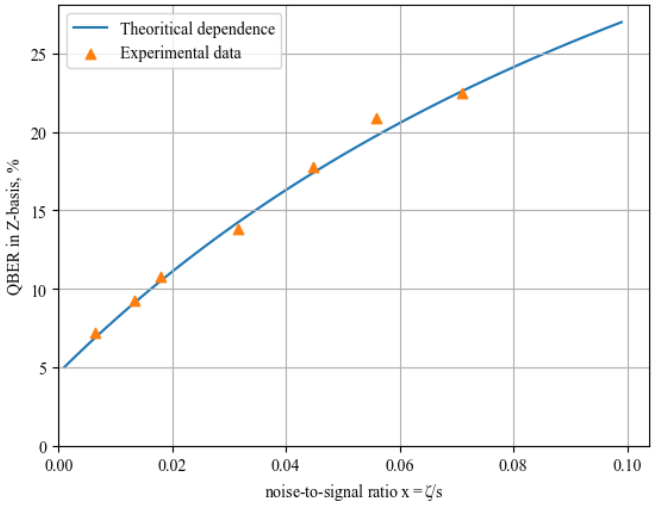

Fig. 3. Dependence of $E^Z_{s_a,s_b}$ on the noise-to-signal ratio $e_d = 4.2 \pm 0.2\%$

Results and Discussion

Considering the interference of weak coherent pulses, we obtained dependences of the error rates on the imperfections of the preparation of states. The plot of this dependence for the *Z*-basis and experimental data are presented in Fig. 3.

The parameter e_d for the theoretical curve was chosen to minimize the deviation from the experimental data. We can say that e_d limits the value of QBER that we can achieve under the condition of perfect preparation of states. The factors affecting the parameter e_d include distortion in the optical fiber, intersymbol interference [6], errors in the polarization adjustment system.

Conclusion

In this work, we derived formulas that allow estimating the error rate in the MDI-QKD protocol. These formulas can be used to solve the inverse problem: to find the characteristics of experimental equipment that allow us not to exceed a certain QBER value. We also proposed an experimental way to evaluate the effects of error parameter e_d and non-ideal states on QBER.

REFERENCES

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

2. **Tang Z., Wei K., Bedroya O., Qian L., Lo H. K.,** Experimental measurement-device-independent quantum key distribution with imperfect sources. Physical Review A, 93.4 (2016) 042308.

3. **Chen H., An X. B., Wu J., Yin Z. Q., Wang S., Chen W., Han Z. F.**, Hong–Ou–Mandel interference with two independent weak coherent states. Chinese Physics B 25.2 (2016) 020305.

4. **Tang G.Z., Sun S.H., Chen H., Li C.Y., Liang L.M.**, Time-bin phase-encoding measurement-device-independent quantum key distribution with four single-photon detectors. Chinese Physics Letters 33.12 (2016) 120301.

5. **Thomaschewski M., Bozhevolnyi S.I.**, Pockels modulation in integrated nanophotonics. Applied Physics Reviews, 9.2 (2022) 021311.

6. **Yoshino K.I., Fujiwara M., Nakata K., Sumiya T., Sasaki T., Takeoka M., Tomita A.**, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. npj Quantum Information 4.1 (2018) 8.

THE AUTHORS

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

PETROV Ivan V.
i.petrov@goqrate.com
ORCID: 0000-0002-5422-2886

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

MENSKOY Daniil D.
d.meskoy@goqrate.com

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

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

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

Received 06.07.2023. Approved after reviewing 11.09.2023. Accepted 11.09.2023.