Conference materials
UDC 04.056.55
DOI: https://doi.org/10.18721/JPM.153.212

QKD and phase modulator imperfections

Reutov A. A. [1]✉, Tayduganov A. S. [1,2]

[1] QRate, Skolkovo, Moscow, Russia;

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

✉ aleksey.reutov@phystech.edu

Abstract. Very often in practical schemes of quantum key distribution various realistic device imperfections are usually neglected. In this work we consider the imperfect phase-modulation encoding that might lead to a potential information leakage and study its effect on the secret key generation rate.

Keywords: quantum cryptography, QKD, state preparation

Citation: Reutov A. A., Tayduganov A. S., QKD and phase modulator imperfections, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 15 (3.2) (2022) 65–68. DOI: https://doi.org/10.18721/JPM.153.212

Материалы конференции
УДК 04.056.55
DOI: https://doi.org/10.18721/JPM.153.212

КРК и неидеальности фазового модулятора

А. А. Реутов [1]✉, А. С. Тайдуганов [1,2]

[1] QRate, Сколково, г. Москва, Россия;

[2] НТИ Центр квантовых коммуникаций, Национальный университет науки и технологий МИСиС, г. Москва, Россия

✉ aleksey.reutov@phystech.edu

Аннотация. Очень часто в практических схемах распределения квантового ключа обычно пренебрегают различными реальными несовершенствами устройств. В этой работе мы рассматриваем неидеальности фазово-модуляционного кодирования, которые могут привести к потенциальной утечке информации и изучаем их влияние на скорость генерации секретного ключа.

Ключевые слова: квантовая криптография, КРК, приготовление состояний

Ссылка при цитировании: Реутов А.А., Тайдуганов А.С. КРК и неидеальности фазового модулятора // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2022. Т. 15. № 3.2. С. 65–68. DOI: https://doi.org/10.18721/ JPM.153.212

Introduction

The quantum key distribution (QKD) is based on fundamental laws of quantum physics and theoretically provides security regardless eavesdropper's potential resources. However, the practical QKD implementations suffer from imperfections of realistic devices [1]. One of the sources of potential information leakage in practical BB84 [2] schemes is the imperfect state preparation by a phase modulator (PM) used for the qubit state encoding. This imperfection leads to an asymmetry between the bases, that can provide more efficient strategies for an eavesdropper [3]. In this work we consider the general quantum state description and introduce two possible phase modulation

uncertainties. Using the density matrix formalism, we provide a metrics of distinguishability between the BB84 bases in our model and estimate its effect on the secret key rate.

Theory and Methods

In our setup the linearly polarized light is brought to the Alice's PM at an angle of 45° with respect to the crystal axes of the modulator with an error $\delta\theta$. In general, there is some phase difference φ between the field amplitudes along the ordinary and extraordinary axes. By applying an electric voltage along one of the axes, an additional phase difference φ_{bit}^{basis} (with some uncertainty $\delta\varphi_{bit}^{basis}$) is created, which determines the basis and bit states.

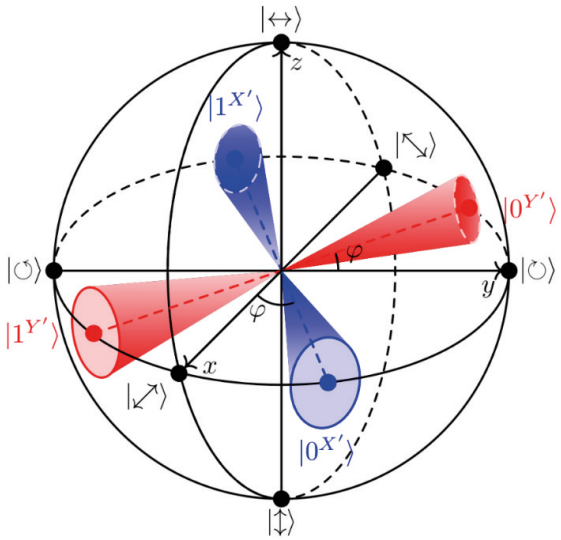

Fig. 1. Physical polarization states on the Bloch sphere; experimental phase uncertainties are schematically depicted as red and blue cones

Without uncertainty $\delta\varphi_{bit}^{basis}$ and error $\delta\theta$, the polarization state, prepared by Alice in X' and Y' bases, can be described on the Bloch sphere (Fig. 1) in the following form,

$$\begin{aligned}
\left|0^{X'}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\leftrightarrow\right\rangle + e^{i\varphi}\left|\updownarrow\right\rangle\right),\\
\left|1^{X'}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\leftrightarrow\right\rangle + e^{i(\varphi+\pi)}\left|\updownarrow\right\rangle\right),\\
\left|0^{Y'}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\leftrightarrow\right\rangle + e^{i(\varphi+\pi)/2}\left|\updownarrow\right\rangle\right),\\
\left|1^{Y'}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\leftrightarrow\right\rangle + e^{i(\varphi-\pi)/2}\left|\updownarrow\right\rangle\right),
\end{aligned} \tag{1}$$

where $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ are the standard horizontal and vertical polarization states. The general polarization state with PM imperfection corrections is given by

$$\begin{aligned}
\left|\psi_0^{X'}\right\rangle &= \cos\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\leftrightarrow\right\rangle + e^{i(\varphi+\delta\varphi_1)}\sin\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\updownarrow\right\rangle,\\
\left|\psi_1^{X'}\right\rangle &= \cos\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\leftrightarrow\right\rangle + e^{i(\varphi+\pi+\delta\varphi_2)}\sin\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\updownarrow\right\rangle,\\
\left|\psi_0^{Y'}\right\rangle &= \cos\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\leftrightarrow\right\rangle + e^{i(\varphi+\pi/2+\delta\varphi_3)}\sin\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\updownarrow\right\rangle,\\
\left|\psi_1^{Y'}\right\rangle &= \cos\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\leftrightarrow\right\rangle + e^{i(\varphi-\pi/2+\delta\varphi_4)}\sin\left(\frac{\pi}{4}-\frac{\delta\theta}{2}\right)\left|\updownarrow\right\rangle,
\end{aligned} \tag{2}$$

where $\delta\theta$ represents in Fig. 1 the deviation from the xy – plane on the Bloch sphere caused by e.g. the 45° fiber input error.

To describe the distinguishability between the states in two bases, the metric Δ called the *imbalance of "quantum coin"* [4] is used. It can be expressed in terms of *fidelity* F [5]:

$$\Delta \equiv \frac{1-\sqrt{F\left(\rho^{X'},\rho^{Y'}\right)}}{2}, \tag{3}$$

and fidelity F is given by

$$F\left(\rho^{X'},\rho^{Y'}\right) \equiv \left(\mathrm{Tr}\sqrt{\sqrt{\rho^{Y'}}\,\rho^{X'}\sqrt{\rho^{Y'}}}\right)^2, \tag{4}$$

where the density matrices $\rho^{X'}$ and $\rho^{Y'}$ are given by $\rho^{basis} = \left(\left|\psi_0^{basis}\right\rangle\left\langle\psi_0^{basis}\right| + \left|\psi_1^{basis}\right\rangle\left\langle\psi_1^{basis}\right|\right)/2$ and can be written (with help (2)) as:

$$\rho^{X'} = \frac{1}{2}\begin{pmatrix} 1+\sin\delta\theta & \frac{1}{2}e^{-i\varphi}\left(e^{-i\delta\varphi_1} - e^{-i\delta\varphi_2}\right)\cos\delta\theta \\ \frac{1}{2}e^{i\varphi}\left(e^{i\delta\varphi_1} - e^{i\delta\varphi_2}\right)\cos\delta\theta & 1-\sin\delta\theta \end{pmatrix},$$
$$\rho^{Y'} = \frac{1}{2}\begin{pmatrix} 1+\sin\delta\theta & -\frac{i}{2}e^{-i\varphi}\left(e^{-i\delta\varphi_3} - e^{-i\delta\varphi_4}\right)\cos\delta\theta \\ \frac{i}{2}e^{i\varphi}\left(e^{i\delta\varphi_3} - e^{i\delta\varphi_4}\right)\cos\delta\theta & 1-\sin\delta\theta \end{pmatrix}. \quad (5)$$

It's leads us to the following result for fidelity:

$$F\left(\rho^{X'}, \rho^{Y'}\right) = \frac{1+\sin^2\delta\theta}{2} + \frac{\cos^2\delta\theta}{2}\cos\frac{\delta\varphi_{12}}{2}\cos\frac{\delta\varphi_{34}}{2} + \frac{\cos^2\delta\theta}{8}\sum_{\substack{i=1,2\\ j=3,4}}\left(-1\right)^{i+j}\sin\delta\varphi_{ij}, \quad (6)$$

where designation $\delta\varphi_{ij} = \delta\varphi_i - \delta\varphi_j$ is used. The minimum of (6) is achieved at $\delta\theta = 0$ and $\delta\varphi_{1(3)} = -\delta\varphi_{2(4)} = \pm\delta\varphi_{\max}$,

$$F_{\min} = \frac{1+\cos^2\delta\varphi_{\max}}{2}. \quad (7)$$

Results and Discussion

Using explicit state parametrization (2), we provide the analytical computation of fidelity (6) and estimate the single-photon phase error rate correction according to [4]:

$$E_1^{phase} = E_1^{bit} + 4\Delta'\left(1-\Delta'\right)\left(1-2E_1^{bit}\right) + 4\left(1-2\Delta'\right)\sqrt{\Delta'\left(1-\Delta'\right)E_1^{bit}\left(1-E_1^{bit}\right)},$$

where the single-photon yield Y_1 and bit error rate E_1^{bit} are determined via decoy-state technique taking into account the finite-key-size effects [6]. Here we consider the worst case, when only a part of the pulses reached to Bob due to losses, but all the different (in the sense of a quantum coin) and useful for eavesdropper pulses were not lost during transmission over the channel. That's way we use Δ' instead of Δ:

$$\Delta' = \frac{\Delta}{Y_1'},$$

E_1^{phase} is used for the secret key rate calculation [7],

$$r_{\sec}^{l} = \frac{Q_1}{Q_\mu}\left[1 - h_2\left(E_1^{phase}\right)\right] - f_{ec}h_2\left(E_\mu\right), \quad (8)$$

where Q_1 is single-photon gain, Q_μ is signal gain and E_μ is measured quantum bit error. Then we study the effects of $\delta\theta$ and $\delta\varphi_{bit}^{basis}$ uncertainties on $r_{\sec}^{l}$.

Our main result is presented in Fig. 2. One can see that for the 100 km–long optical line the critical (i.e. when $r_{\sec}^{l} \le 0$ no secret key can be distributed) value of a phase disturbance is about 1.5°. For the length of 50 km our result is more promising – the key rate vanishes only for the phase error is about 5°.

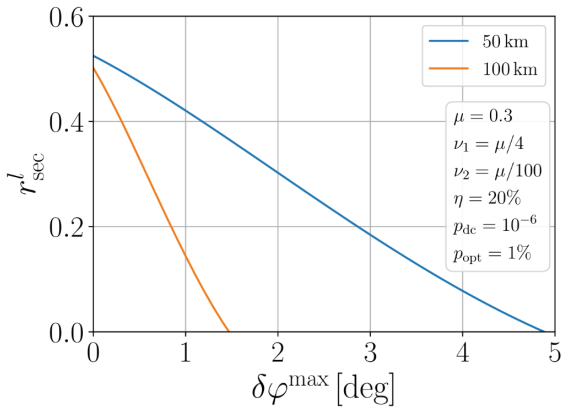

Fig. 2. Minimized secret key rate (7) (per bit) lower bound as function of maximum phase modulation error $\delta\theta_{max}$. The parameters μ, ν_1, ν_2, η, p_{dc}, p_{opt} are signal, week decoy and vacuum decoy intensities, quantum efficiency, dark count rate probability and probability of the optical error respectively. The simulation is run for the 50 km (orange line) and 100 km (blue line) optical fiber distances.

Conclusion

From our research we conclude that rather precise (~ 1° for short distances and ~ 0.1° for large distances) fine tuning of PM is required in order to have a reasonable secret key generation rate.

Acknowledgments

The authors would like to acknowledge Arina Gavrilovich for thoughtful and productive discussions.

REFERENCES

1. **Bennett, C. H., Brassard G.,** Quantum Cryptography: Public-Key Distribution and Coin Tossing, In: Proc. Of the IEEE Int. Conf. On Comp. Sys. And Sign. Process. (IEEE, 1984), 175–79.
2. **Gottesman D., Lo H.-K., Lüttkenhaus N., Preskill J.,** Security of Quantum Key Distribution with Imperfect Devices, *Quant. Inf. Comput.* 4 (2004) 325–60.
3. **Jozsa R.,** Fidelity for Mixed Quantum States, Journal of Modern Optics 41 (12) (1994) 2315–23.
4. **Lo H.-K., Ma X., Chen K.,** Decoy State Quantum Key Distribution, Phys. Rev. Lett. 94 (2005) 230504.
5. **Lo H.-K., Preskill, J.,** Security of Quantum Key Distribution Using Weak Coherent States with Nonrandom Phases, Quantum Info. Comput., 7 (5) (2007) 431–58.
6. **Trushechkin A. S., Kiktenko E. O., Fedorov A. K.,** Practical Issues in Decoy-State Quantum Key Distribution Based on the Central Limit Theorem, Phys. Rev. A 96 (2017) 022316.
7. **Xu F., Ma X., Zhang Q., Lo H.-K., Pan J.-W.,** Secure Quantum Key Distribution with Realistic Devices, Rev. Mod. Phys. 92 (May) (2020) 025002.

THE AUTHORS

REUTOV Aleksei A.
aleksey.reutov@phystech.edu
ORCID: 0000-0001-5838-4770

TAYDUGANOV Andrey S.
a.tayduganov@goqrate.com

Received 15.08.2022. Approved after reviewing 16.08.2022. Accepted 08.09.2022.