MATHEMATICAL PHYSICS

Conference materials
UDC 535.8
DOI: https://doi.org/10.18721/JPM.163.264

Experimental evaluation of imperfections of quantum states for time-bin encoding

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

✉ i.gerasin@goqrate.com

Abstract. We propose here a simple method to estimate quality of quantum states for quantum key distribution (QKD) protocols with phase-time encoding. The parameters proposed to estimate the quality of states can be easily measured experimentally and will be useful in setting up and debugging the QKD system.

Keywords: quantum key distribution, state preparation, time-bin encoding

Funding: The study was commissioned by JSCo RZD.

Citation: Gerasin I.S., Rudavin N.V., Kupriyanov P.A., Dvurechenskiy A.A., Shakhovoy R.A., Experimental evaluation of imperfections of quantum states for time-bin encoding, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.2) (2023) 366–371. DOI: https://doi.org/10.18721/JPM.163.264

Материалы конференции
УДК 535.8
DOI: https://doi.org/10.18721/JPM.163.264

Экспериментальная оценка неидеальностей квантовых состояний в пространственно-временном кодировании

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

[1] QRate, 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

✉ i.gerasin@goqrate.com

Аннотация. В данной работе предлагается простой метод оценки качества приготовления квантовых состояний, использующихся в системах квантового распределения ключей

(КРК), с фазово-временным кодированием. Параметры для оценки, предложенные в данной работе, могут быть легко измерены экспериментально и будут полезны при настройке и отлаживании систем КРК.

Ключевые слова: квантовое распределение ключей, приготовление состояний, пространственно-временное кодирование

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

Ссылка при цитировании: Герасин И.С., Рудавин Н.В., Куприянов П.А., Двуреченский А.П., Шаховой Р.А. Экспериментальная оценка неидеальностей квантовых состояний в пространственно временном-кодировании // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.2. С. 366–371. DOI: https://doi.org/10.18721/JPM.163.264

Introduction

Nowadays, a lot of efforts are aimed at improving the security of transmitted data. In this regard, quantum key distribution (QKD) is a promising technology towards unconditional security [1]. However, despite the theoretical possibility of achieving unconditional security, real QKD systems are not at all information-theoretic secure. The reason is that practical implementations of QKD systems have imperfections, due to which many of the assumptions used in the theoretical construction of quantum protocols are violated. For instance, instead of ideal single photons, one generally uses weak coherent pulses, which, with some probability, can contain more than one photon. Instead of an ideal quantum channel standard fiber optic communication lines having significant losses are usually employed. Real single photon detectors are characterized by an efficiency different from 100%; moreover, they have a finite dead time and a non-zero probability of dark counts. Finally, phase modulators have a finite bandwidth, intensity modulators have finite extinction, and the high-frequency drivers used to drive them have non-zero jitter and can distort the shape of electrical signals. All these imperfections make the real QKD system vulnerable to various attacks that Eve can implement without being noticed.

In this article, we will focus on the study of imperfections associated with phase and intensity modulators, namely, on the non-ideality of quantum state preparation. This type of imperfection leads to the distinguishability of quantum states in non-orthogonal bases, which can be used by Eve to obtain partial information about the quantum key. Therefore, it is always important to know the accuracy with which quantum states are prepared to properly deal with possible information leakage. The quantum bit error rate (QBER) is usually used to estimate the non-ideality of quantum states; however, QBER is an integral parameter [2] and does not allow separating various effects that lead to imperfections. So, it would be useful to have additional criteria for assessing the quality of quantum states that would allow, e.g., finer tuning of laser drivers, phase modulators, intensity modulators, etc.

In this paper, we introduce simple criteria for estimating the quality of quantum states for QKD protocols with phase-time encoding. These criteria can help assess the leakage of information in the implementation of such protocols. In addition, they will be useful in setting up and debugging the QKD system.

Materials and Methods

There are two widespread approaches to encode quantum states in QKD: polarization and time-bin encoding [3]. The former approach employs light polarization to encode quantum information and is preferred for free-space communication since air environment does not significantly disturb the polarization state of light. In the latter approach, information is encoded in the time of appearance of the optical signal from the source. The times used for encoding can be very short and have an order of magnitude corresponding to the period of oscillation of the electromagnetic field in a pulse. In this case, one usually speaks of optical phase encoding, where

interferometric methods or homodyne detection are used for decoding. If the times are comparable with the pulse width, then one speaks of time-bin coding, where a detector that can distinguish between the arrival times of the pulses is used for decoding. Roughly speaking, with phase encoding, the transmitter shifts in time (using a phase modulator) the carrier wave in the pulse, whereas with time-bin encoding, the transmitter manipulates (using an intensity modulator) the pulse envelope. Since polarization of light is not maintained in optical fiber during propagation, polarization encoding requires additional polarization control system [4]; therefore, time-bin encoding is widely used in fiber-optic systems.

Similar to BB84 protocol with polarization encoding, one can introduce two non-orthogonal bases with time-bin encoding (let us denote them as *X*- and *Z*-basis). In the *X*-basis, a bit can be encoded by a pair of laser pulses separated in time by ΔT and having a given phase difference. In the *Z*-basis, a single pulse is prepared either in an early (*E*-pulse) or late (*L*-pulse) time slot within the frame corresponding to a given quantum state (Fig. 1). A general quantum state prepared within time-bin encoding can be represented by a tensor product of consecutive weak coherent pulses: $|\psi\rangle = |\alpha\rangle\otimes|\beta\rangle \equiv |\alpha,\beta\rangle$, where α, β are complex amplitudes of coherent states in the neighboring bins (time slots), i.e., in *E*- and *L*-pulses, respectively.

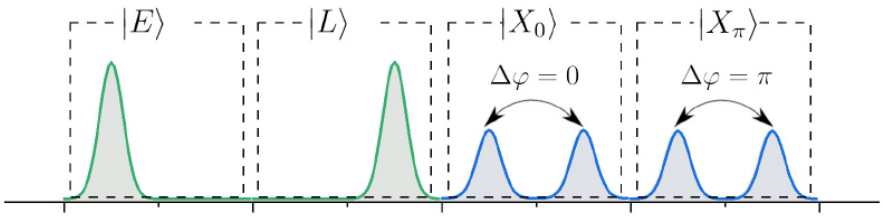

Fig. 1. Schematic of time-bin encoding

Quantum states prepared via real optical modulators inevitably differ from ideal qubits. For instance, intensity modulators employed for cutting pulses from continuous light have finite extinction; therefore, some light remains in the "empty" time slot of the *Z*-basis. In addition, an electrical signal driving the modulator deviates from an ideal rectangular function already due to finite duration of rising and falling edges or even because of the impedance mismatch, which leads to a distortion of the shape of the optical pulse. Non-ideal electrical signals driving the phase modulator may lead, in turn, to inaccuracies in the preparation of the phase difference between pulses.

To characterize the quality of a quantum state, one generally uses *fidelity F*, which is a measure of similarity of quantum states. For pure states $|\psi\rangle$ and $|\phi\rangle$, it is defined via the scalar product as $F = |\langle\psi|\phi\rangle|^2$. Thus, for one of the states in the *Z*-basis, we may define fidelity as

$$F_Z = \left|\left\langle vac, \sqrt{s} \middle| \sqrt{\zeta}, \sqrt{s} \right\rangle\right|^2 = e^{-\zeta}, \tag{1}$$

where $|vac\rangle$ is the signal in the absence of a pulse (vacuum), s is a mean photon number in the 'non-empty' bin, and ζ is the intensity of the signal, which is prepared instead of a vacuum state due to modulator imperfections. Experimentally, it is easier to measure mean photon number per quantum state $S_Z = s + \zeta$, so, introducing the ratio of intensities in the early and late time bins, $r_Z = s/\zeta$, we may write for the residual intensity:

$$\zeta = \frac{S_Z}{r_Z + 1}. \tag{2}$$

It easy to see form (1) that fidelity higher than 0.99 is achieved when the ratio of intensities, r_Z, is greater than 20 dB (in assumption that $S_Z < 1$).

For the states in the *X*-basis, we assume that intensity of laser pulses in the early and late time bins may differ by the value $\delta\gamma$, whereas the phase difference can be prepared with an error $\delta\theta$. In this case, fidelity is written as follows:

$$F_X = \left|\left\langle \sqrt{\gamma}, \sqrt{\gamma} \middle| \sqrt{\gamma}, e^{\delta\theta}\sqrt{\gamma+\delta\gamma} \right\rangle\right|^2 = \\ = e^{-2\zeta-\delta\gamma+2\sqrt{\gamma(\gamma+\delta\gamma)}\cos(\delta\theta)} = e^{-\gamma(1+r_X-2\sqrt{r_X}\cos(\delta\theta))}, \quad (3)$$

where $r_X = (\gamma + \delta\gamma)/\gamma$. Such a fidelity depends on the two parameters, $\delta\gamma$ and $\delta\theta$; therefore, it is convenient to define additional fidelities:

$$F_Z^{\theta} = F_X\,|_{\delta\gamma=0} = e^{-2\gamma(1-\cos(\delta\theta))}, \quad (4)$$

$$F_X^{r} = F_X\,|_{\delta\theta=0} = e^{-\gamma(1+r_X-2\sqrt{r_X})}, \quad (5)$$

which can be easily measured separately. Using numerical calculations, it is easy to show that $F_X^{\theta} > 0.99$ if $\delta\theta < 10°$ and $F_X^{\gamma} > 0.99$ if $r_X < 1.4$.

Results

Now, we turn to the experimental estimation of the above parameters and corresponding fidelity values. Let us first consider the imperfections associated with the intensity modulator. For this, we will use three states in the X-basis, $|vac\rangle\otimes|vac\rangle$, $|\sqrt{\nu}\rangle\otimes|\sqrt{\nu}\rangle$, $|\sqrt{\mu}\rangle\otimes|\sqrt{\mu}\rangle$ (they can be used as decoy states in a real-world QKD system) and one state in the Z-basis, $|vac\rangle\otimes|\sqrt{s}\rangle$, where $s = 0.6$, $\mu = 0.3$, and $\nu = 0.06$ are corresponding intensities (mean photon numbers) of coherent states.

To prepare the states and measure their fidelities, we used the experimental setup schematically shown in Fig. 2. Note that it can be used for measuring non-idealities in QKD systems with point-to-point connection as well as for QKD with untrusted central note (MDI QKD [5]). The setup consists of two transceivers (TX1 and TX2), each including a CW laser, a phase modulator (PM), and an intensity modulator (IM). To measure IM-related non-idealities, we used the first transceiver (TX1), whose output was connected to both single-photon detector (SPD) and classical photodetector (PD). PM was disabled during these measurements. Light pulses were cut from the beam of the CW laser; pulse repetition rate was 312.5 MHz. The pulses were then split by the 50:50 beam splitter: half of the power were then measured with PD, and the second half was attenuated by variable optical attenuator and then measured with gated SPD. Pulse shapes measured with PD and acquired with an oscilloscope are presented in Fig. 3,*a*. Pulse shapes recovered with SPD by scanning the phase of the gate (with the step 25 ps) are shown in Fig. 3,*b*.

To calculate r_Z, we measured the ratio between areas of the early and late pulses of the state $|Z_0\rangle$ (see Fig. 3,*a* and 3,*b*). Similarly, we calculated the parameter r_X for $|X_\mu\rangle$- and $|X_\nu\rangle$-state. Obtained values are listed in Table 1.

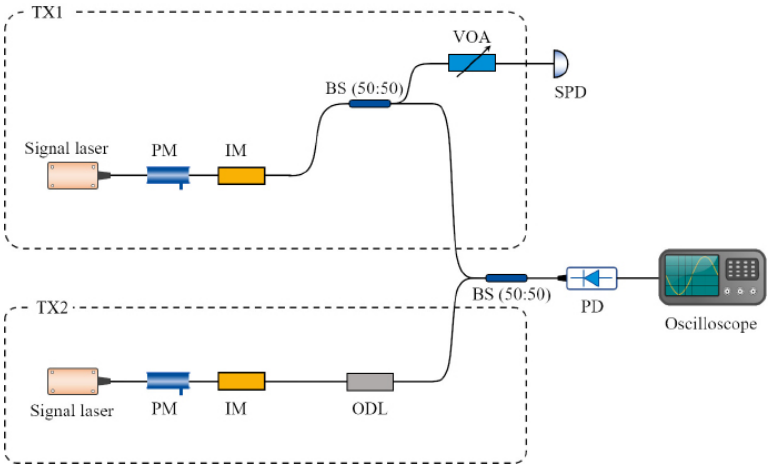

Fig. 2. Experimental setup

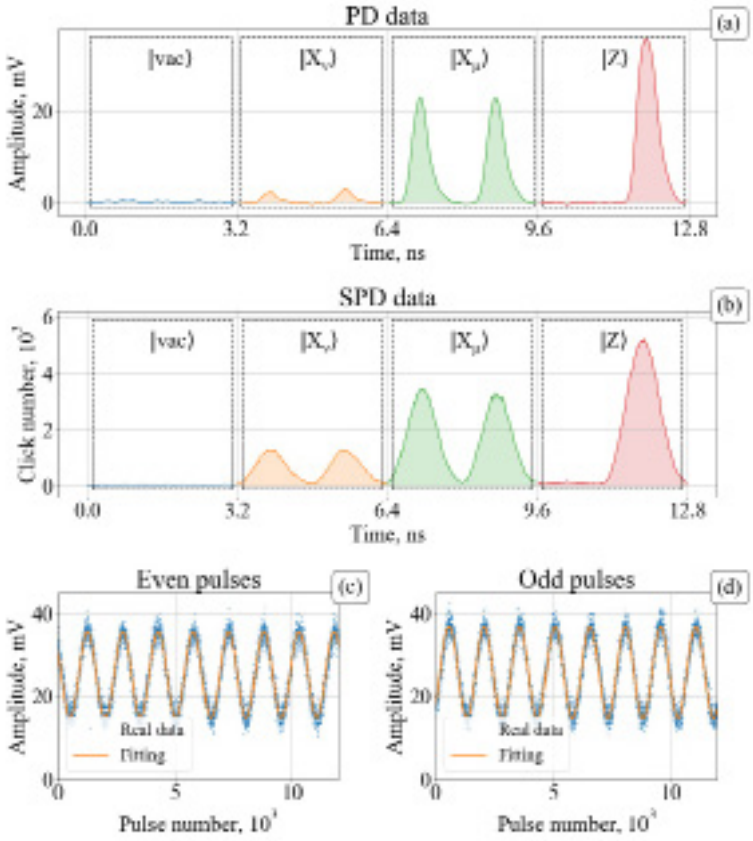

Fig. 3. Experiment results.

Table 1

Experimental and bound values of introduced criteria

Parameter	r_Z	r_X^{μ}	r_X^{ν}	δθ	s/ν
'Classical' value	85±45 dB	1.03±0.01	1.23±0.2	5±1°	11.3±0.2
'Quantum' value	14±1 dB	1.06±0.01	1.01±0.2	–	2.5±0.2

To measure the phase error, δθ, we prepared a continuous sequence of states $|X_\pi\rangle$ with the first transceiver (TX1) and a continuous sequence of states $|X_0\rangle$ with the second transceiver (TX2). The sequences from TX1 and TX2 interfered at the beam splitter (precise overlapping of pulses was achieved with an optical delay line in TX2, whereas alignment of pulse intensities was carried out by varying the bias voltage of the IM in TX1). In this configuration, odd pulses of the sequence from TX1 should interfere constructively with odd pulses of the sequence from TX2, whereas corresponding even pulses should interfere destructively. However, since the lasers in TX1 and TX2 have not been locked to each other, we observed beats: a sinusoidal intensity variation of odd pulses and another sinusoidal variation of even pulses shifted by phase of approximately π. Beats from even and odd pulses were fitted by the function $f(t,a,b,\omega,\theta) = a + b\sin(\omega t + \theta)$ (the data and their fits are presented in Fig. 3,*c* and 3,*d*). The difference between the values of the fitting parameter θ provide the phase error δθ. (The measured value of δθ.)

Discussion

Pulse shapes measured 'classically' (with PD) and 'quantum-mechanically' (with SPD) look similar, although some differences should be noted. First, high non-linearity of SPD and the influence of the dead time led to the fact that relative intensities of the pulses in different bases measured with PD and SPD significantly differ (this is clearly seen from the comparison of $|X_\nu\rangle$

states in Fig. 3 and 4). In fact, when the number of clicks increases, dead time of the SPD plays a more significant role and an effective time of the detection is decreased, such that the measured amplitude of the signal becomes less than the real one. Thus, the ratio s/ν (which nominally should be equal to 10) measured with PD is close to nominal value (see Table 1), whereas in quantum case it is four times smaller due to the non-linearity. This also partially explains the difference in the values of r_Z obtained with PD and SPD. Note that the non-linearity of the SPD can be easily taken into account by pre-calibration, after which both quantum and classical values should be quite close.

As for the measurement of the phase error, the method described here is more suitable for MDI QKD and determines the relative phase error between transmitters. However, it can be easily extended to point-to-point protocols if the phase difference between the pulses in one of the TX is fixed.

Conclusion

We have introduced a simple method to estimate quality of quantum states for QKD protocols with phase-time encoding. Proposed parameters can be easily measured experimentally and can help assess the leakage of information in the implementation of such protocols. In addition, they will be useful when setting up and debugging the QKD system, particularly when tuning intensity and phase modulators.

REFERENCES

1. **Scarani V., et al.**, The security of practical quantum key distribution, Reviews of modern physics 81 (3) (2009) 1301.

2. **Bennett C.H., Gilles B.,** Quantum cryptography: Public key distribution and coin tossing, arXiv preprint arXiv: 2003. (2020) 06557.

3. **Gisin N., et al.,** Quantum cryptography, Reviews of modern physics 74 (1) (2002) 145.

4. **Mekhtiev E.E., et al.,** Polarization control algorithm for QKD systems, Journal of Physics: Conference Series. IOP Publishing, 2086 (1) (2021).

5. **Grosshans F., et al.,** Quantum key distribution using gaussian-modulated coherent states, Nature 421 (6920) (2003) 238–241.

6. **Woodward R.I., et al.**, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Information 7.1 (2021): 58.

7. **Hiskett P.A., et al.**, Long-distance quantum key distribution in optical fibre, New Journal of Physics 8 (9) (2006) 193.

THE AUTHORS

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

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

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

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

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

Received 11.07.2023. Approved after reviewing 12.09.2023. Accepted 12.09.2023.