NANOSYSTEMS:
PHYSICS, CHEMISTRY, MATHEMATICS

Goncharov F.M., et al. *Nanosystems: Phys. Chem. Math.*, 2023, **14** (1), 59–68.
http://nanojournal.ifmo.ru
DOI 10.17586/2220-8054-2023-14-1-59-68

Original article

Increase of signal to reference ratio for phase compensation in continuous-variable quantum key distribution systems

Fedor M. Goncharov, Boris E. Pervushin, Boris A. Nasedkin, Roman K. Goncharov, Daniil A. Yashin, Mikhail E. Gellert, Danil V. Sulimov, Polina A. Morozova, Ilya M. Filipov, Iurii A. Adam, Vladimir V. Chistiakov, Eduard O. Samsonov, Vladimir I. Egorov

ITMO University, St. Petersburg, 197101, Russia

Corresponding author: Fedor M. Goncharov, fedor_goncharov@itmo.ru

PACS 03.67.Dd, 42.30.Rx

ABSTRACT Continuous variables quantum key distribution (CV-QKD) systems are a promising direction for quantum communications. Coherent detection, which is the basis of CV-QKD, requires taking into consideration and compensating phase distortions. Phase compensation algorithms rely on using reference pulses for phase drift estimation and correcting signal quadratures. The ratio of the number of reference pulses to that of the signal ones, affects the accuracy of the phase compensation algorithm. On the other hand, it influences the secure key rate (SKR). The paper considers the effect of the reference to signal ratio on the SKR, and proposes a modification of the phase compensation algorithm, which allows using a smaller number of references at a pulse repetition frequency close to that of the system phase noise, which results in increasing SKR. We also propose a method for estimating the phase noise in the system for selection of the optimal signal to reference ratio.

KEYWORDS continuous-variable quantum key distribution, quantum communications, phase noise, phase compensation, algorithm

ACKNOWLEDGEMENTS The work was completed by the Leading Research Center “National Center for Quantum Internet” of ITMO University by order of JSCo Russian Railways. This research was funded by JSCo Russian Railways.

FOR CITATION Goncharov F.M., Pervushin B.E., Nasedkin B.A., Goncharov R.K., Yashin D.A., Gellert M.E., Sulimov D.V., Morozova P.A., Filipov I.M., Adam I.A., Chistiakov V.V., Samsonov E.O., Egorov V.I. Increase of signal to reference ratio for phase compensation in continuous-variable quantum key distribution systems. *Nanosystems: Phys. Chem. Math.*, 2023, **14** (1), 59–68.

1. Introduction

Since the implementation of the first quantum key distribution (QKD) protocol by Charles Bennett and Gilles Brassard in 1984, quantum communications have been actively developing. QKD is the main constituent of quantum communications, which allows two remote parties (usually referred to as Alice and Bob) to safely distribute the secure key through a quantum channel subject to any actions on the part of the eavesdropper (Eve) obeying the laws of quantum mechanics.

There are two main approaches to QKD implementation, one of them using discrete variables (DV) [1] and the other one using continuous variables (CV) [2]. The first protocols developed for QKD were those for discrete variables. However, this approach has some disadvantages, in particular, the need to use expensive single photon detectors.

Presently, CV-QKD is a promising approach, since it uses standard telecommunication equipment as part of the so-called coherent detection scheme [3] operating with a high detection frequency (of GHz order). Coherent detection approach in its turn is based on the interference of weak signal radiation and on powerful local oscillator (LO), which makes it possible to measure quadrature components of electromagnetic field carrying the encoded information. There are two main approaches to generating LO: on Alice’s side or on Bob’s side. In the former case, the signal and the LO are generated by the same laser in the sender and are jointly transmitted to the receiver using time-division multiplexing and polarization-division multiplexing. Coherent detection makes it possible to measure the quadrature of signal pulses, provided the power of the LO is much higher than the amplitude of the signal, therefore, a combination of multiplexing methods is established to separate the LO and the signal to avoid interference between them in the channel. If the LO is generated on Bob’s side (the so-called “local” LO (LLO)), then there is no need for multiplexing, the system becomes more secure, since there are no loopholes for attacks on LO [4, 5]. However, there is a problem of synchronization of two free-running lasers [6].

Interference as fundamental element of coherent detection makes it necessary to take account of the phase noise in the system and compensate it. Phase distortions in CV-QKD systems are discussed in multiple articles on quantum communications where algorithms are proposed [7] based on the alternation of signal and reference pulses, which are

© Goncharov F.M., Pervushin B.E., Nasedkin B.A., Goncharov R.K., Yashin D.A., Gellert M.E., Sulimov D.V., Morozova P.A., Filipov I.M., Adam I.A., Chistiakov V.V., Samsonov E.O., Egorov V.I., 2023

used for phase compensation. Most studies [5, 8] describes systems with LLO, where phase noise is particularly strong because of two lasers used. Thus, the limiting ratio of reference pulses to signal pulses (one to one) is chosen as the most reliable option that provides the most accurate phase compensation. Nevertheless, in systems with transmitted LO (and in LLO-based systems with relatively low phase noise), the limiting ratio of reference and signal pulses may be redundant. Increasing the number of signal pulses by one reference increases secure key rate.

The paper consists of four sections: section 1 contains a review of the existing phase compensation method for protocol with Gaussian-modulated coherent states, as well as the essentials of excess phase noise model; section 2 provides a modification for the phase compensation algorithm based on two references instead of one; section 3 analyzes of the effect of the signal to reference ratio on the secure key rate; section 3 presents an experimental comparison of two phase compensation algorithms and estimates the phase noise in the system and the effect of the reference pulses frequency on the accuracy of phase compensation.

2. Phase compensation for CV-QKD protocol based on Gaussian-modulated coherent states

Here we review the CV-QKD protocol based on Gaussian coherent states, discuss the existing phase compensation algorithm and the standard phase compensation model.

2.1. Phase compensation algorithm

In the CV-QKD protocol with Gaussian [9, 10] modulation, Alice prepares numerous coherent states $|\alpha_S\rangle = |Q_{A_S} + iP_{A_S}\rangle$ with quadratures Q_{A_S} and P_{A_S}, each of them independently and identically distributed from two random sets of variables with Gaussian distribution $\mathcal{N}(0, V_A)$ with V_A variance centered at zero [11]. Quantum key is distributed by those quantum states, so we will call them quantum signals. The reference pulses required for phase compensation are the classical coherent states $|\alpha_R\rangle = |Q_{A_R} + iP_{A_R}\rangle$ with the quadratures Q_{A_R} and Q_{A_R}. For convenience, the zero-phase is usually chosen for the reference pulses. A LO is known to be essential to implement coherent detection. For the value at the output of the balanced detector to be proportional to the quadrature components of the field, the intensity of the LO has to be much higher than that of the reference and signal pulses [12]. Besides, the intensity of the reference pulse should also be significantly superior to the signal pulse in order to eliminate the occurrence of interference between the signal and the reference pulse during multiplexing [12]. The intensity of the reference pulses cannot be too low either, since otherwise the phase noise increases [13].

Alice sends Bob a sequence of signal and reference pulses with a certain ratio. Bob performs heterodyne detection, whereby he obtains the values of the signal quadratures (Q_{B_S}, P_{B_S}) and the reference (Q_{B_R}, P_{B_R}). It is important that in the case of homodyne detection, Alice sends a pair of consecutive reference pulses, one of which introduces a delay of $\pi/2$ before measuring. Another option is to use homodyne detection for signal pulses and heterodyne detection for reference ones. If during the time between the two reference pulses, the influence of phase noise is negligible, i.e. $\tau \ll f_{phase}^{-1}$ (where τ is the time interval between the two reference pulses, and f_{phase} is the characteristic frequency of phase noise in the system), the receiver can estimate the phase shift $\widehat{\theta}$ that occurs during the pulse transmission through the channel between the reference pulse and the LO [7]:

$$\widehat{\theta} = \arctan\left(\frac{P_{B_R}}{Q_{B_R}}\right). \tag{1}$$

Since the intensity of the reference pulses is quite low, quantum uncertainty is also to be considered, so there is a phase error of random nature [7]:

$$\widehat{\theta} = \theta + \varphi. \tag{2}$$

It is important that the variables θ and φ have different physical nature, therefore they are independent. Besides the phase drift, the receiver also calculates the effective transmission of the channel T, given by:

$$T = \frac{\|(Q_{B_R}, P_{B_R})\|^2}{\|(Q_{A_R}, P_{A_R})\|^2}. \tag{3}$$

Reverse matching is often used in phase compensation protocols. Bob transmits to the sender the values of the measured quadratures of the reference pulses, using which he calculates the phase drift and the effective transmission according to formulas (1), (3). Otherwise, calculations can be performed on the recipient's side, and it is the values of θ and T that are transmitted. Further, using the values of phase drift and effective transmission received from Bob, Alice corrects the values of her quadratures as follows [7]:

$$\begin{pmatrix} \widehat{Q}_{A_S} \\ \widehat{P}_{A_S} \end{pmatrix} = \sqrt{T} \begin{pmatrix} \cos\hat{\theta} & -\sin\hat{\theta} \\ \sin\hat{\theta} & \cos\hat{\theta} \end{pmatrix} \begin{pmatrix} Q_{A_S} \\ P_{A_S} \end{pmatrix}. \tag{4}$$

2.2. Phase noise model with phase compensation

Studies [7] and [14, 15] guarantee and prove the security of protocols containing reference pulses. The authors claim that under the standard assumption for CV-QKD, Eve can collect complete information about the reference pulses, however, this does not give her any additional information about the signal pulses. During phase compensation, there still appears to be some excess phase noise ξ_{phase}. Generally, the excess noise ξ_{tot} of the CV-QKD system is a key parameter for evaluating its performance. This can be represented by the expression [6]:

$$\xi_{tot} = \xi_{phase} + \xi_{rest}, \tag{5}$$

where ξ_{rest} includes all other sources of excess noise. As follows from [16, 17], phase noise can be represented as:

$$\xi_{phase} = V_A(V_{comp} + V_{ref}) = \xi_{comp} + \xi_{ref}, \tag{6}$$

$$V_{comp} = V_{drift} + V_{channel}. \tag{7}$$

The variance of V_{drift} occurs when using two independent lasers in the protocols with LLO and is given by the expression [16]:

$$V_{drift} = 2\pi(\Delta\nu_A + \Delta\nu_B)|t_R - t_S|, \tag{8}$$

where $\Delta\nu_A$ and $\Delta\nu_B$ are line widths of two free-running lasers, t_R and t_S are the time points of signal and reference pulses emission.

The $V_{channel}$ component evaluates the change in the phase drift between the reference and the signal pulse resulting from the passage of the optical channel. The variance of $V_{channel}$ can be defined as [16]:

$$V_{channel} = \mathrm{var}(\theta_S - \theta_R). \tag{9}$$

Phase compensation is based on the measurement of reference pulses, and quadratures are further corrected with respect to their values. Obviously, phase shift measurement cannot be performed perfectly, thus the measured value of the phase shift $\widehat{\theta}_R$ may differ from the actual θ_R. Therefore, the variance introduced by the inaccuracy of phase shift measurement is given as follows [7]:

$$V_{ref} = \mathrm{var}(\theta_R - \widehat{\theta}_R). \tag{10}$$

In practice, when the ratio of signal and reference pulses is one to one, the main contribution to excess phase noise is through the components ξ_{ref} and ξ_{drift}, whereas ξ_{drift} occurs only when using LLO and is crucial for the analysis of phase noise [16]. In addition, it is important to note that part of the excess phase noise can be considered trusted and irrelevant when evaluating the performance of CV-QKD system. The trusted phase noise model is given in [6].

3. Linear phase compensation algorithm

An important assumption of the phase compensation method discussed in the previous section was that the phase shift between the reference pulse and the following signal pulse it undergoes almost no change. This assumption has also be met with a theoretical increase in the number of signal pulses by one reference pulse: the phase drift for all signal pulses has to be almost the same. Based on this assumption, in the [6, 7] the component $\xi_{channel}$ in the expression (6) was considered negligible. However, with an increase in the number of signal pulses between the reference ones, this assumption may not be met. In this paper we propose to modify the phase compensation algorithm so that the phase shift can be considered as linearly changing rather than constant between the reference pulses. The resulting phase compensation algorithm will be referred to as linear.

3.1. Linear phase compensation algorithm

A sequence consisting of a reference pulse (a pair of reference pulses for homodyne detection) and subsequent signal pulses up to the next reference pulse will be called a cycle (Fig. 1). The idea of using two reference pulses for phase compensation of one signal between them using the average value of the reference phase drift was proposed in [14] for a system with a “local” LO, since in such implementation phase noise can have high impact even on the interval between the neighboring pulses. Here we extend this approach to multiple signals in a cycle. Thus, linear phase compensation combines the ideas of using two reference pulses to compensate for the phase of one signal pulse, and using several signal pulses in a cycle, which allows increasing secure key rate (see section 3). The difference between the algorithms is shown in the Fig. 1.

Based on the assumption of the linear nature of the phase shift changes in the time interval between the reference pulses, the phase compensation is performed for each signal pulse in the cycle. The values of phase drift and transmission for the first and second reference pulses are calculated according to the following formulas, respectively:

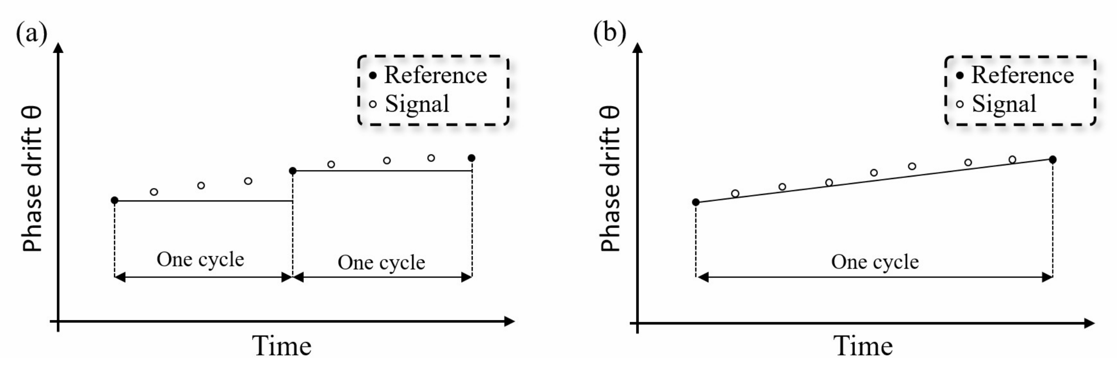


FIG. 1. Single reference pulse method (a) and linear method (b) of phase compensation

$$\widehat{\theta}^{1st} = \arctan\left(\frac{P^{1st}_{B_R}}{Q^{1st}_{B_R}}\right), \quad T^{1st} = \frac{\left\|\left(Q^{1st}_{B_R}, P^{1st}_{B_R}\right)\right\|^2}{\left\|\left(Q_{A_R}, P_{A_R}\right)\right\|^2}; \tag{11}$$

$$\widehat{\theta}^{2nd} = \arctan\left(\frac{P^{2nd}_{B_R}}{Q^{2nd}_{B_R}}\right), \quad T^{2nd} = \frac{\left\|\left(Q^{2nd}_{B_R}, P^{2nd}_{B_R}\right)\right\|^2}{\left\|\left(Q_{A_R}, P_{A_R}\right)\right\|^2}, \tag{12}$$

where $Q^{1st}_{B_R}, P^{1st}_{B_R}$ and $Q^{2nd}_{B_R}, P^{2nd}_{B_R}$ are the measured quadrature values of the first and the second reference pulses, correspondingly.

Next, using the values for each signal pulse in the cycle obtained from formulas (11), (12), phase drift correction and transmission are calculated:

$$\widehat{\theta}_m = \frac{m\left(\widehat{\theta}^{2nd} - \widehat{\theta}^{1st}\right)}{n_S + 1} + \widehat{\theta}^{1st}, \tag{13}$$

$$T_m = \frac{m\left(T^{2nd} - T^{1st}\right)}{n_S + 1} + T^{1st}, \tag{14}$$

where n_S is the number of signal pulses in the cycle. Then, similarly to the expression (4), the receiver corrects the value of each signal pulse in the cycle by using the formula:

$$\begin{pmatrix} \hat{Q}^m_{A_S} \\ \hat{P}^m_{A_S} \end{pmatrix} = \sqrt{T_m}\begin{pmatrix} \cos\hat{\theta}_m & -\sin\hat{\theta}_m \\ \sin\hat{\theta}_m & \cos\hat{\theta}_m \end{pmatrix}\begin{pmatrix} Q^m_{A_S} \\ P^m_{A_S} \end{pmatrix}. \tag{15}$$

This method provides an opportunity to increase the time interval of one cycle, thereby increasing the number of signal pulses by one reference. The experimental difference in the operation of phase compensation algorithms is presented in Section 4.1.

3.2. Effect of the ratio of reference and signal pulses on the accuracy of the phase compensation algorithms

The use of a linear phase compensation algorithm is aimed at increasing the number of signal pulses in the cycle. However, it is necessary to consider how an increase in the number of signal pulses affects the accuracy of the phase compensation operation, in other words, how the excess phase noise of CV-QKD system will change.

Let us return to expression (6). The accuracy of measuring the reference pulses does not appear to depend on the number of signal pulses, so ξ_{ref} will not be considered. However, the number of pulses in the cycle affects the second part of the equation (6), namely ξ_{comp}. For further discussion, it is more convenient to switch from the value of the number of signal pulses in the cycle to the frequency of sending reference pulses f_{ref}:

$$f_{ref} = \frac{f_{rep}}{n_S + n_R}, \tag{16}$$

where f_{rep} is the frequency of sending pulses (corresponds to the frequency of signals), $n_R = 1$ for heterodyne detection of reference pulses, $n_R = 2$ for homodyne detection.

In systems with transmitted LO, a theoretical analysis of the effect of the frequency of reference pulses on the phase noise component ξ_{comp} seems to be challenging, since in real-world operating conditions of CV-QKD systems, phase noise depends on many factors, such as temperature [18], vibrations and others. Thus, it is more reliable to determine the phase noise of a particular system experimentally before running the CV-QKD protocol. Therefore, it is possible to analyze resulting phase noise regardless of the reasons it appears. The method of determining the phase noise of the system and the assessment of the effect of reference pulses frequency on V_{comp} is discussed in the experimental part of this paper (section 4.2).

On the other hand, in a system with LLO, it is possible to analytically evaluate the component ξ_{drift}. The value V_{drift} defining ξ_{drift} is given by formula (8). Let us estimate the maximum possible value of V_{drift}, which is achieved by a signal pulse in a cycle that is as far as possible from the reference ones in the time domain. This signal pulse is the central signal in the cycle. Denote $\Delta t = |t_R - t_S|$. Then for the central signal in the cycle Δt can be obtained as follows:

$$\Delta t = \frac{n_S + 1}{2} \frac{1}{f_{rep}}. \tag{17}$$

Therefore, V_{drift} takes the following form:

$$V_{drift} = 2\pi(\Delta\nu_A + \Delta\nu_B)\frac{n_S + 1}{2f_{rep}}. \tag{18}$$

Specifically, for the case of heterodyne detection $n_R = 1$, (18) can be represented in terms of the frequency of reference pulses using (16):

$$V_{drift} = \frac{\pi(\Delta\nu_A + \Delta\nu_B)}{f_{ref}}. \tag{19}$$

It can be noted that for the linear phase compensation algorithm, the variance of V_{drift} is half as large as for the phase compensation discussed in [16].

4. Secure key rate dependence on signal to reference ratio

The purpose of increasing the number of signal pulses in the cycle is to raise the secure key rate. This section examines the effect of the number of signal pulses in a cycle on the rate of secure key generation in the protocols of the CV-QKD. The value of the secure key rate is given in the approximation for the keys of infinite length by the expression [11]:

$$K = f_{sym} \cdot r, \tag{20}$$

where f_{sym} is the symbol rate (in units of symbols with $^{-1}$), and r is the key generation rate in terms of the parcel. The above expression already contains a fraction of signal pulses relative to all pulses. To simplify the analysis of the secure key rate dependence on the ratio of signal and reference pulses, let us assume that this expression takes into account the ratio of one reference pulse to one signal pulse. Then we rewrite the expression for the secure key rate to include the change in the number of signal pulses in the cycle relative to the above:

$$K' = \varepsilon \cdot K \tag{21}$$

where $\varepsilon = 2n_S \cdot (n_S + 1)^{-1}$ shows the change in the ratio of signal and reference pulses in the cycle relative to the one-to-one ratio.

Figure 2 reflects an increase in the secure key rate compared to that with one signal pulse from the number of signals in the cycle. Fig. 2 shows that when a ratio of about one hundred signal pulses per reference is reached, a further increase in the ratio only leads to a slight gain in the secure key rate and, perhaps, can only be reasonable if the number of reference pulses is increased by an order of magnitude.

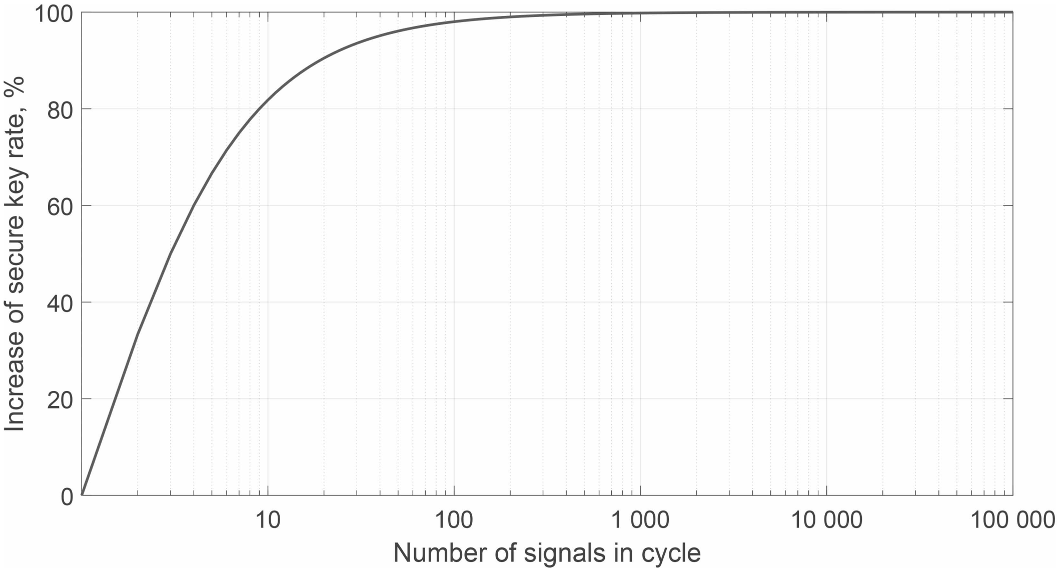


FIG. 2. Dependence of the increase of secure key rate (relative to one signal pulse in a cycle) on changing the number of reference pulses in a cycle

If the number of signals in the cycle is below one hundred, the effect of each additional signal is much more pronounced. For example, even using two reference pulses in a cycle instead of one increases secure key rate by 33 %.

5. Experimental setup

5.1. Comparison of the phase compensation algorithms efficiency

First, we compare the efficiency of phase compensation algorithm [7] and the linear algorithm for different frequencies of reference pulses. The characteristic phase noise for the experimental scheme shown in Fig. 3 is of the order of one Hz, therefore, for a more visual demonstration of the difference in the algorithms, there were used reference pulses with the power in order of 1 mW and the frequency $f_{ref} = 4$ Hz, which is close to phase noise. For more information of the evaluation of the phase noise in the CV-QKD system, see Section 4.2. The experimental setup is a Mach–Zehnder interferometer – a simplified version of the CV-QKD system. The first amplitude modulator AM1 sets pulses with a frequency of f_{rep}, the second amplitude modulator AM2 generates reference pulses with a frequency of f_{ref}. In this experiment, all pulses are classical, which allows to ignore the phase error ϕ from the expression (2), which has quantum nature. The phase of the pulses sent by Alice is set to zero, so the phase measured by the receiver corresponds to the phase shift $\widehat{\theta}$.

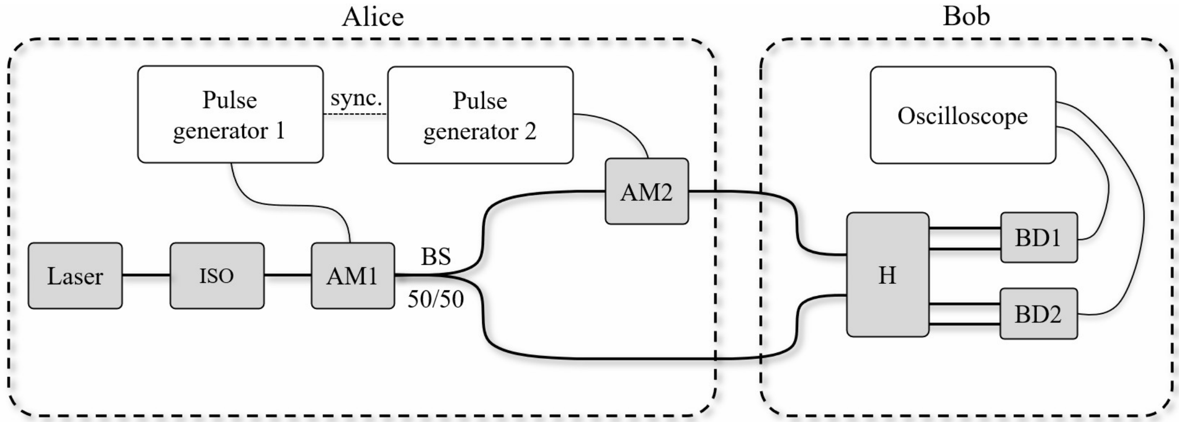


FIG. 3. Scheme of experimental setup No. 1, where ISO is optical isolator, BS is 50/50 beam splitter, AM1 and AM2 are amplitude modulators, H is 90-degree hybrid, BD1 and BD2 are balanced detectors

The graph presented in Fig. 4(a) shows the measured phase shift of the signal and reference pulses, the phase shift reconstructed by the method of a single reference pulse and the linear algorithm. With strong phase changes, the phase compensation algorithm using two reference pulses is characterized by a smaller error in the phase adjustment of signal pulses, especially in the areas of strong linear changes, for instance, in the area from 52 to 80 pulses.

The graph presented in Fig. 4(b) shows the averaged error values for each signal pulse over all cycles. The phase error for the algorithm with one reference pulse increases as it moves away from the reference pulse. For a linear phase

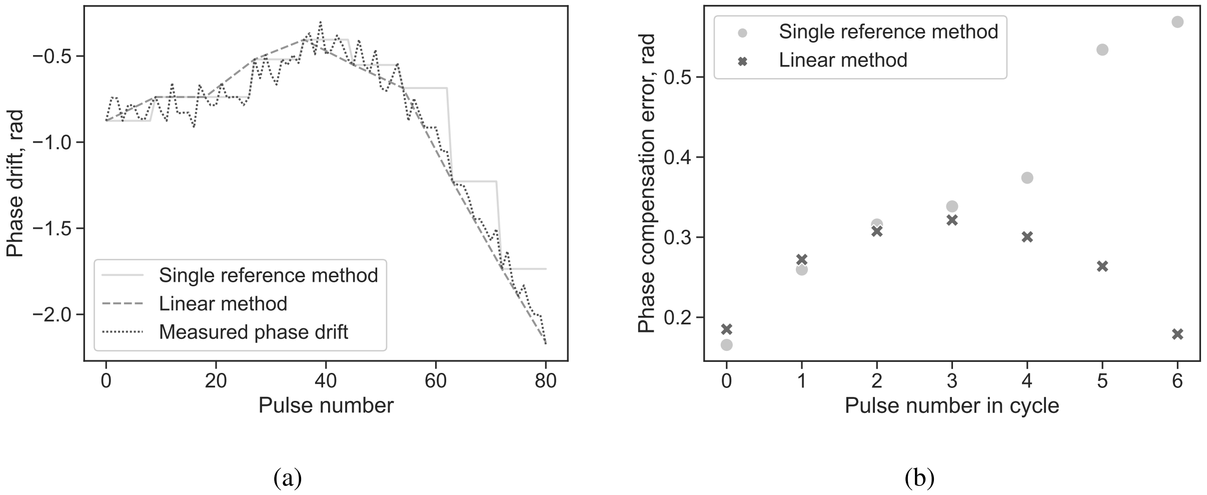
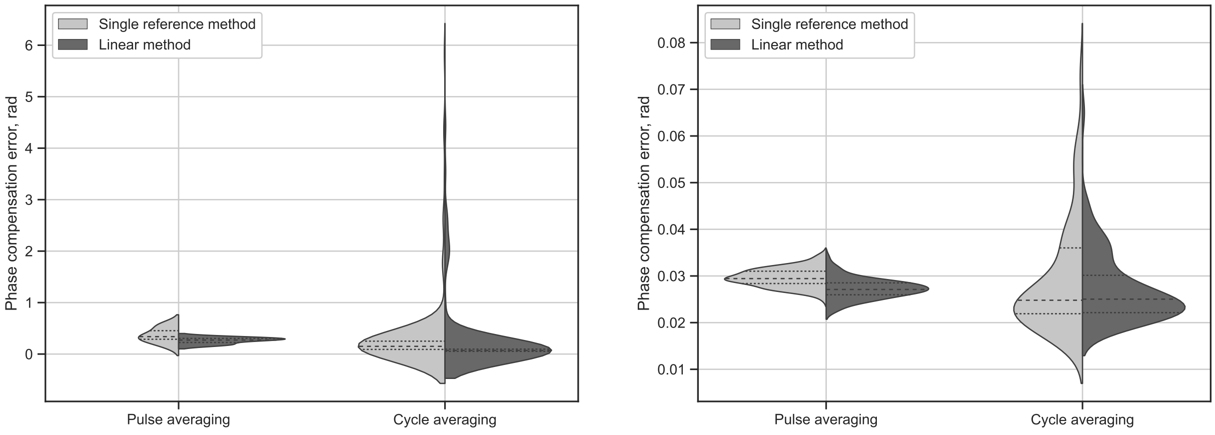


FIG. 4. (a) Phase shift of the pulses for $f_{ref} = 4$ Hz and (b) dependence of the cycle-averaged phase compensation error on the number of the signal pulse

compensation algorithm using two reference pulses, an increase is observed first, whereas there is a decrease in the phase error after the middle signal pulse. This results from the fact that the phase of the signal pulses of the cycle second half is closer to the phase of the second reference pulse, and it is this phase that is used to a greater extent to compensate for the phase distortions of the signal pulses. The phase error in this experiment is characterized by large values due to the low frequency of pulse transmission. During the characteristic time of this experiment, the phase of the pulses relative to the LO appears to shift by significant amounts. The graph in Fig. 5(a) shows the statistics of the phase error when averaging by pulses and by cycle. When using two reference pulses, the median of the phase recovery error decreases.



(a) (b)

FIG. 5. Statistics of phase error when averaging by state and by cycle. When averaging over a pulse, statistics of the average phase error for each signal pulse in a cycle are built; when averaging over a cycle it is the statistics of the average error in a cycle. The strokes indicate the distribution of quantiles: 25, 50, 75 %

To analyze phase compensation with parameters close to the real parameters of a CV-QKD system, we handled measurements with a pulse frequency f_{rep} of 50 MHz, duration of 3 ns, reference pulses with a frequency f_{ref} of 500 kHz. The resulting statistics of the phase compensation performed are shown in Fig. 5(b). Since the characteristic operating time of the system determined by the frequency of sending pulses is too small compared to the characteristic phase change time, the error in phase noise compensation is relatively small. Therefore, the difference between algorithms with one and two reference pulses is insignificant either.

Summarizing, it can be concluded that with the frequency of reference pulses close to the frequency of phase noise in the system, the linear phase compensation algorithm is more effective, especially with strong phase noise in the system, which allows to increase the number of signal pulses in the cycle, and consequently, increase the speed of secure key rate. When the frequency of the reference pulses is much higher than the characteristic frequencies of the reference pulses, the difference in the operation of the algorithms is negligible.

5.2. Phase noise and phase compensation accuracy

This section discusses a method for estimating phase noise in the CV-QKD system and the effect of the selected frequency of reference pulses on the accuracy of the linear phase compensation algorithm.

Phase noise evaluation was evaluated before starting the CV-QKD protocol. It consists of the accumulation and analysis of phase shifts within a few seconds [19]. Let us consider phase noise on an experimental setup (Fig. 6), similar to the one used in the previous section. In this scheme, a channel is added for transmitting the LO and the signal from Alice to Bob, where the LO and the signal are multiplexed. The channel consists of 500 meters of polarization-maintaining optical fiber, thus, it allows avoiding polarization distortion.

To collect statistics, Alice sends a sequence of identical pulses with zero phase, the quadrature values of which are recorded by Bob. Next, using the formula (1), the receiver calculates the phase shift $\widehat{\theta}$. Phase noises are low-frequency compared to the rest of the noise, therefore, for the rest of the noise not to affect further analysis, the dependence obtained of the phase shift on time was smoothed using the moving average method. The resulting graph is shown in Fig. 6(a). The amplitude spectrum of phase noise is shown in Fig. 6(b). For the experimental setup presented, the main phase noises are up to 80 Hz. Note that a phase noise could be higher in real systems with longer channels. Nevertheless, the further analysis and conclusions about results of current experimental setup are also relevant to higher phase noises.

Let us simulate the phase compensation for a different number of signal pulses in a cycle and, consequently, a different frequency of reference pulses. To do this, we will consider some of the pulses as reference ones, and the rest of the pulses

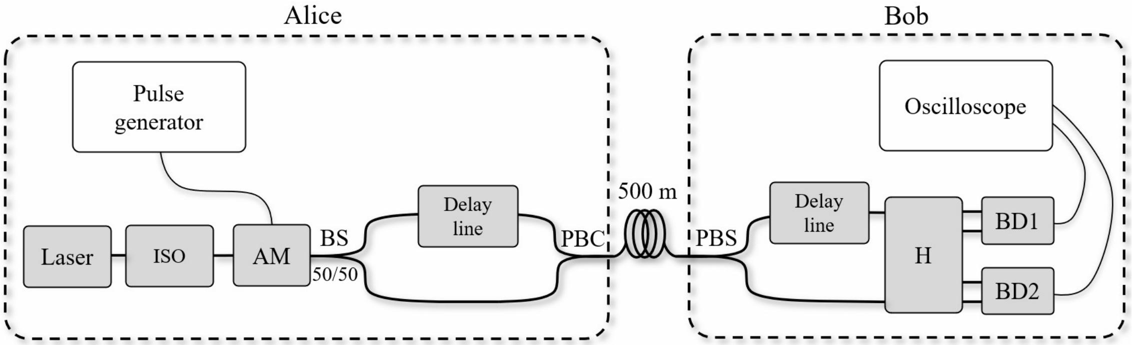
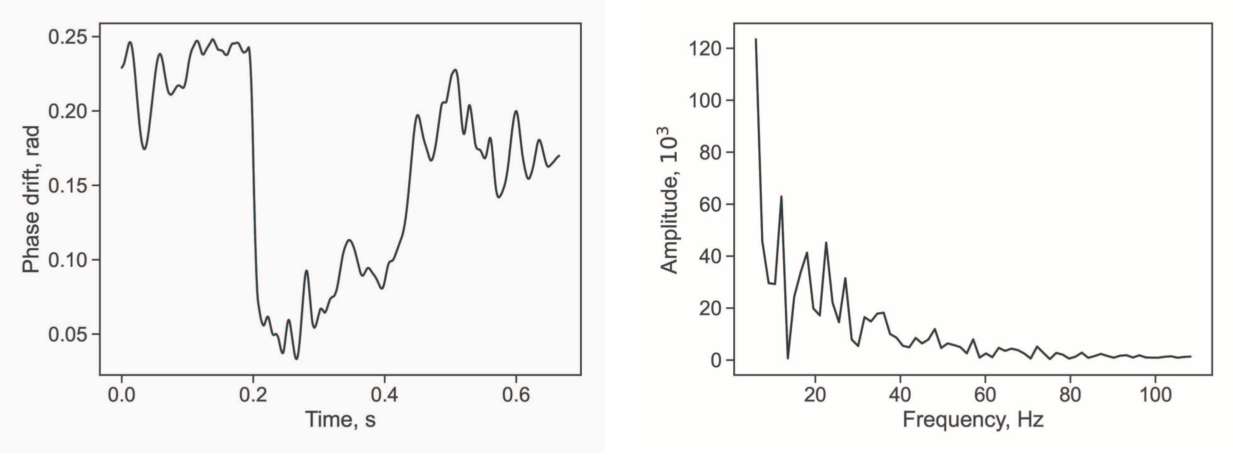


FIG. 6. Scheme of experimental setup No. 2, where ISO is optical isolator, AM is amplitude modulator, BS is beam splitter 50/50, PBS is polarization beam splitter, PBC is polarization beam combiner, H is 90-degree hybrid, BD1 and BD2 are balanced detectors

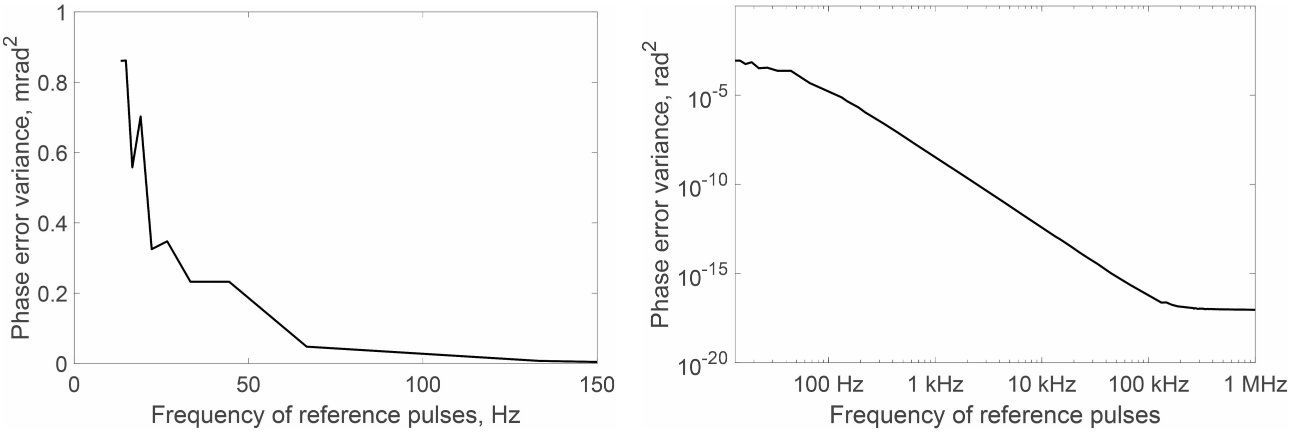


(a) (b)

FIG. 7. (a) Phase noise versus time plot and (b) phase noise spectrum

between them as signal ones. We will estimate the accuracy of the phase compensation by the value V_{comp}, determined by formula (9). Fig. 8(a) shows the phase compensation error variance V_{comp} for reference pulse frequencies up to 150 Hz.

Comparison of this graph with the spectrum (Fig. 7(b)) shows the similarity of these dependencies. For the highest characteristic frequency of phase noise, the phase error is already relatively small (of the order of 10^{-5}). However, in



(a) (b)

FIG. 8. Plot of phase compensation error variance V_{comp} versus reference pulse frequency f_{ref}: f_{ref} up to 150 Hz (a); f_{ref} up to 1 MHz (b)

this case, the phase noise itself is quite small due to the experimental conditions. In practice, phase noise can be much higher, however it is still limited to $[-\pi/2, \pi/2]$. Fig. 8(b) shows the phase compensation error for higher reference pulse frequencies, which rapidly decreases with their growth.

The optimal frequency of the reference pulses is selected based on the condition that $V_{ref} \gg V_{comp}$. For strong phase noise, the frequency of the reference pulses can be taken an order of magnitude or two higher than the characteristic maximum phase noise frequency f_{phase}; for weak phase noise, phase compensation will be highly accurate even at a frequency of reference pulses comparable to the characteristic frequency of phase noise. On the other hand, the frequency of the reference pulses has to be chosen for one reference pulse to accounts for as many signal pulses as possible up to the ratio of 1:100; a further increase in the ratio gives a minuscule increase in the secure key generation rate. Summing up, for a linear phase compensation algorithm, the optimal frequency of the reference pulses at low-frequency phase noise ($f_{phase} \ll f_{rep}$) can be roughly estimated as

$$10 f_{phase} < f_{ref}^{optimal} < 10^{-2} f_{rep}. \tag{22}$$

With high-frequency phase noise, the left boundary of the estimate can be reduced if the phase noise is weak, otherwise the right boundary of the estimation can be changed, based on the dependence of the secure key generation rate on the number of reference pulses in the cycle (Fig. 2).

Conclusion

We analyzed the effect of the signal to reference ratio on the secure key rate in the CV-QKD system, as well as its influence on the accuracy of the phase compensation. To increase the number of signal pulses in a cycle, we proposed a linear method of phase compensation. The experiment showed that linear phase compensation algorithm works more efficiently than conventional method, which makes it applicable to increase the number of signals in systems with strong and high-frequency phase noise. We also proposed a method for estimating phase noise in a system that provides evaluating optimal frequency of reference pulses for phase noise with the characteristic frequency of the latter much lower than that of sending reference pulses.

References

[1] Gleim A.V., Egorov V.I., Nazarov Yu.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics express*, 2016, **24** (3), P. 2619–2633.

[2] Goncharov R., Vorontsova I., Kirichenko D., Filipov I., Adam I., Chistiakov V., Smirnov S., Nasedkin B., Pervushin B., Kargina D., et al. The rationale for the optimal continuous-variable quantum key distribution protocol. *Optics*, 2022, **3** (4), P. 338–351.

[3] Hirano T., Yamanaka H., Ashikaga M., Konishi T., Namiki R. Quantum cryptography using pulsed homodyne detection. *Physical review A*, 2003, **68** (4), 042331.

[4] Jouguet P., Kunz-Jacques S., Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A*, 2013, **87** (6), 062313.

[5] Wang T., Huang P., Zhou Y., Liu W., Ma H., Wang S., Zeng G. High key rate continuous-variable quantum key distribution with a real local oscillator. *Optics express*, 2018, **26** (3), P. 2794–2806.

[6] Shao Y., Wang H., Pi Y., Huang W., Li Y., Liu J., Yang J., Zhang Y., Xu B. Phase noise model for continuous-variable quantum key distribution using a local local oscillator. *Physical Review A*, 2021, **104** (3), 032608.

[7] Soh D.B.S., Brif C., Coles P.J., Lütkenhaus N., Camacho R.M., Urayama J., Sarovar M. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, 2015, **5** (4), P. 1–15.

[8] Ren S., Yang S., Wonfor A., White I., Penty R. Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator. *Scientific Reports*, 2021, **11** (1), P. 1–13.

[9] Weedbrook C., Lance A.M., Bowen W.P., Symul T., Ralph T.C., Ping Koy Lam. Quantum cryptography without switching. *Physical review letters*, 2004, **93** (17), 170504.

[10] Grosshans F., Van Assche G., Wenger J., Brouri R., Cerf N.J., Grangier P. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, **421** (6920), P. 238–241.

[11] Laudenbach F., Pacher C., Fung C.-H.F., Poppe A., Peev M., Schrenk B., Hentschel M., Walther P., Hübel H. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 2018, **1** (1), 1800011.

[12] Huang D., Huang P., Lin D., Wang C., Zeng G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Optics letters*, 2015, **40** (16), P. 3695–3698.

[13] Ma X.-C., Sun S.-H., Jiang M.-S., Liang L.-M. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Physical Review A*, 2013, **88** (2), 022339.

[14] Zou M., Mao Y., Chen T.-Y. Phase estimation using homodyne detection for continuous variable quantum key distribution. *J. of Applied Physics*, 2019, **126** (6), 063105.

[15] Qi B., Lougovski P., Pooser R., Grice W., Bobrek M. Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 2015, **5** (4), 041009.

[16] Marie A., Alleaume R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 2017, **95** (1), 012316.

[17] Wang T., Huang P., Zhou Y., Liu W., Zeng G. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. *Physical Review A*, 2018, **97** (1), 012310.

[18] Bartolo R.E., Tveten A.B., Dandridge A. Thermal phase noise measurements in optical fiber interferometers. *IEEE J. of Quantum Electronics*, 2012, **48** (5), P. 720–727.

[19] Zhang L., Wang Y., Yin Z., Chen W., Yang Y., Zhang T., Huang D., Wang S., Li F., Han Z. Real-time compensation of phase drift for phase-encoded quantum key distribution systems. *Chinese Science Bulletin*, 2011, **56** (22), P. 2305–2311.

Submitted 22 November 2022; revised 3 December 2022; accepted 12 December 2023

Information about the authors:

Fedor Mikhailovich Goncharov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-7370-4450; fedor_goncharov@itmo.ru

Boris Evgenevich Pervushin – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-0935-2614; borispervushin@itmo.ru

Boris Aleksandrovich Nasedkin – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-4507-8616; banasedkin@itmo.ru

Roman Konstantinovich Goncharov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-9081-8900; rkgoncharov@itmo.ru

Daniil Aleksandrovich Yashin – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0001-5127-0578; dayashin@itmo.ru

Mikhail Evgenevich Gellert – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-2180-7052; mihailgellert@yandex.ru

Danil Vasilevich Sulimov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-7964-0697; dvsulimov@itmo.ru

Polina Alekseevna Morozova – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0003-3741-3506; 283021@edu.itmo.ru

Ilya Maksimovich Filipov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0003-4564-8284; imfilipov@itmo.ru

Iurii Alexandrovich Adam – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-5040-0040; adam_yura@mail.ru

Vladimir Viktorovich Chistiakov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-2414-3490; v_chistyakov@itmo.ru

Eduard Olegovich Samsonov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0002-4349-6603; eosamsonov@itmo.ru

Vladimir Ilyich Egorov – ITMO University, Kronverksky Pr. 49, bldg. A, Saint Petersburg, 197101, Russia; ORCID 0000-0003-0767-0261; viegorov@itmo.ru

Conflict of interest: the authors declare no conflict of interest.