Methodology for calculating the average time of entry into synchronism of stations of the system of quantum key distribution with sequential polling of fiber-optic line sections with decreasing length by the graphic-analytical method

Y Mironov¹, P Mironova¹,* and K Rumyantsev¹

¹Southern Federal University, Russia

Abstract. A method is proposed for calculating the average time of entry into synchronism of stations of the system of quantum key distribution (QKD) with sequential polling of sections of a fiber-optic communication line (FOCL) with decreasing length. A diagram of states and transitions for a sequential search for a photon pulse is constructed. Analytical expressions are obtained for finding the probability of detecting a photon pulse, the average number of steps for entry into synchronism of stations, the variance of the number of steps and the average time for entry into connection. It is noted that when the FOCL is divided into sections with decreasing length, the level of dark current pulses (DCP) significantly decreases from section to section. The latter allows to reduce the probability of false alarms of the photodetector. The analysis of the results obtained showed that the time of entry into synchronism for the proposed algorithm is 3 times less than the time required for entry into communication of stations in the case of an algorithm-analogue. The results obtained indicate the possibility of increasing the length of the FOCL while ensuring the value of the synchronization error probability at the level of 0.01.

1 Introduction

Ensuring the confidentiality of information during transmission between legitimate users is one of the main criteria for the security and efficiency of data transmission systems at present. To increase the security of the transmitted information, quantum key distribution protocols are used, which allow high-precision tracking of unauthorized access to communication lines, as well as the introduction of interference into them [1]. One of the ways to increase the security of quantum key distribution (QKD) systems is to synchronize the stations of the system QKD at a single-photon level [2].

* Corresponding author: tmiyap117@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
With at a distant location of the receiving-transmitting and coding stations of the QKD system, it is necessary to ensure accurate synchronization of the system as a whole. Accurate synchronization of the QKD system increases the efficiency of the system, including increasing the speed of information transfer in it. On the other hand, in addition to accurate synchronization of the two stations, it is necessary that the synchronization of the QKD system takes as little time as possible.

The issues of synchronization of the receiving-transmitting and coding stations of the QKD system are studied by domestic [3-9] and foreign [10, 11] scientists.

In [12], a technique for designing a subsystem of one-photon synchronization of the QKD system is proposed. The synchronization of the stations of the QKD system takes place in two stages: the search stage and the testing stage. A distinctive feature of this algorithm is the division of a fiber-optic communication line (FOCL) into sections with decreasing length. At the search stage, a time frame equal in duration to the repetition period of optical pulses $T_s$ is divided into time intervals (sections). Note that the repetition period of the optical pulses is chosen so that the optical pulses do not overlap. The equipment registers a photon pulse or dark current pulses (DCP) by analyzing the first time interval (section) in the first frame of the FOCL. If the photon pulse or DCP were not registered in this interval, the polling continues in the first section of subsequent frames. When registering a photon pulse or DCP, the equipment switches to the testing mode. The result of this stage is either confirmation of the presence of a photon pulse in the inspected section of the FOCL and, therefore, successful synchronization of the stations of the QKD system, or a negative testing result and transition to the analysis of the next section of the FOCL.

In [13-15], a method is proposed for calculating the average time required for the entry into synchronism of the stations of the QKD system for the algorithm-analogue. However, in view of the analysis of the entire length of the FOCL without dividing into sections, this approach can be applied in QKD systems with a FOCL length of up to 70 km. Therefore, it becomes urgent to develop an algorithm for synchronizing the stations of the QKD system while ensuring the length of the FOCL is more than 70 km and, at the same time, with the minimum possible time of entry into synchronism.

Let us calculate the average time required for entry into communication of the receiving-transmitting and coding stations of the QKD for the proposed algorithm and algorithm-analogue.

2 Simulation of the synchronization process

To find the average time required for entry into communication (synchronization) of the receiving-transmitting and coding stations, we will use the diagram of states and transitions presented in Figure 1 [16].
Fig. 1. State and transition diagram for sequential search.

This diagram of transitions and states characterizes a sequential testing algorithm, where: $a_1$ – search for a photon pulse, analysis of a time frame with a duration $T_s$; $a_2 \ldots a_{2n}$ – testing mode at correct photon pulse detection; $a_3$ – synchronizing stations; $P_{11}$ – probability of not detecting a photon pulse and DCP at the search stage; $P_{12}$ – probability of detecting a photon pulse in the time interval $[0, T_s]$ and transition to state $a_2$; $Q_{23}$ – The probability of the absence of a photon pulse and DCP for the duration of the strobe pulse $\tau_{\text{strob}} = 2\tau_s + 2\Delta T_s$, where $\Delta T_s$ is the instability of the pulse repetition period; $P_{23}$ – the probability of receiving a photon pulse or DCP for the duration of the strobe pulse $\tau_{\text{strob}}$.

The diagram of states and transitions (Figure 1) can be represented in the form of a table (Table 1), which characterizes the probabilities of transitions between the states of the system.

|      | $a_1$ | $a_2$ | $a_{2a}$ | $a_{2b}$ | $\ldots$ | $a_{2n}$ | $a_3$ |
|------|-------|-------|---------|---------|---------|---------|------|
| $a_1$ | $P_{11}$ | $P_{12}$ |         |         |         |         |      |
| $a_2$ |       | $Q_{23}$ |         |         |         |         | $P_{23}$ |
| $a_{2a}$ |       |       | $Q_{23}$ |         |         |         | $P_{23}$ |
| $a_{2b}$ |       |       |       | $Q_{23}$ |         |         | $P_{23}$ |
| $\ldots$ |       |       |       |       | $Q_{23}$ |         | $P_{23}$ |
| $a_{2n}$ |       |       |       |       |       | $P_{23}$ |      |
| $a_3$ |       |       |       |       |       |       | $P_{33}$ |

Note that the sum of the probabilities in each row is 1.

Suppose that the number of tests $N_{\text{test}}$ required to ensure the specified probability of testing error $P_{\text{err.test}}$ is 1. This parameter $N_{\text{test}}$ is used at the 2nd stage of testing, when the repeated polling is performed only at the time intervals specified by the strobe pulse $\tau_{\text{strob}}$.

To find the statistical characteristics of the search, we form a stochastic matrix of transition probabilities between states:

$$
P = \begin{pmatrix}
P_{11} & P_{12} & 0 \\
Q_{23} & 0 & P_{23} \\
0 & 0 & P_{23}
\end{pmatrix}, \tag{1}
$$
where the first column corresponds to the state \( a_1 \), the second to \( a_2 \), the third to \( a_3 \), similarly, the first line corresponds to the state \( a_1 \), the second to \( a_2 \), and the third to \( a_3 \).

The average number of passages of the process through a nonabsorbing state \( a_j \) under the assumption that the initial state is a nonabsorbing state \( a_i \) is determined by the expression:

\[
T = (I - Q)^{-1},
\]

where \( I \) – «identity matrix», \( Q \) – matrix formed from matrix \( P \) by eliminating columns and rows of absorbing states:

\[
Q = \begin{pmatrix} P_{11} & P_{12} \\ Q_{23} & 0 \end{pmatrix}.
\]

Find the matrix \( A = 1 - Q \):

\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} P_{11} & P_{12} \\ Q_{23} & 0 \end{pmatrix} = \begin{pmatrix} P_{12} & -P_{12} \\ P_{23} - 1 & 1 \end{pmatrix}.
\]

To find the inverse matrix \( A^{-1} \), we find its determinant:

\[
|A| = P_{12} - (P_{23} - 1) \cdot (-P_{12}) = P_{12} + P_{12} \cdot (P_{23} - 1) = P_{12} \cdot P_{23}.
\]

The inverse matrix \( A^{-1} \) is defined by the following formula:

\[
A^{-1} = \frac{1}{|A|} \cdot A_d^T,
\]

where \( A_d^T \) – transposed matrix of algebraic complements.

To determine the transposed matrix of algebraic complements, we find the matrix of minors:

\[
M = \begin{pmatrix} 1 & P_{23} - 1 \\ -P_{12} & P_{12} \end{pmatrix}.
\]

the matrix of algebraic complements:

\[
A_d = \begin{pmatrix} 1 & 1 - P_{23} \\ P_{12} & P_{12} \end{pmatrix},
\]

and transpose the matrix of algebraic complements

\[
A_d^T = \begin{pmatrix} 1 & P_{12} \\ 1 - P_{23} & P_{12} \end{pmatrix}.
\]

Therefore, it is now possible to calculate the inverse matrix \( A^{-1} \):

\[
A^{-1} = \frac{1}{P_{12}P_{23}} \cdot \begin{pmatrix} 1 & P_{12} \\ P_{23} - 1 & P_{12} \end{pmatrix} = \begin{pmatrix} \frac{1}{P_{12}P_{23}} & \frac{1}{P_{23}} \\ \frac{1}{P_{12}P_{23}} & \frac{1}{P_{23}} \end{pmatrix}.
\]

Thus, if the process starts from the non-absorbing state \( a_1 \), then it passes through the non-absorbing state \( a_2 \) on average \( 1/P_{23} \) times.

The dispersion of the number of passes is determined by the following expression:

\[
\{D_i[n_j]\} = T \cdot (2T_d - I) - T_q,
\]

where \( T = A^{-1}, T_d \) – «diagonal» matrix \( T \), \( T_q \) – «square» matrix \( T \), then
\[
\{D_1[n_j]\} = \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left[ 2 \cdot \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{0}{1} \right) - \left( \frac{0}{1} \right) \right] = \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right)
\]

(12)

If the process starts in a nonabsorbing state \(a_1\), then the dispersion of the number of passes the process passes through the nonabsorbing state \(a_2\) is

\[
\{D_1[n_2]\} = \frac{1 - P_{23}}{P_{23}^2}.
\]

(13)

The average number of steps \(t_1\), which is spent in the transition from the nonabsorbing state \(a_j\) to the absorbing state \(a_i\), is:

\[
t = T \cdot c = A^{-1} \cdot c,
\]

(14)

where \(c\) – a column vector whose components are all equal to one. Thus, the average number of steps will be:

\[
t = \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right) \cdot \left( \frac{1}{1} \right) = \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right) + \left( \frac{1}{P_{23}} \right)
\]

(15)

Accordingly, for the transition from the non-absorbing state \(a_1\) to the absorbing state \(a_3\), it is necessary to spend \(1/P_{12}P_{23} + 1/P_{23}\) steps, from the non-absorbing state \(a_2\) to the absorbing state \(a_3\) \((1-P_{23})/P_{12}P_{23} + 1/P_{23}\) steps.

In generalized form, for an arbitrary number \(N_{\text{test}}\), the average number of steps for the transition from the nonabsorbing state \(a_1\) to the absorbing state \(a_3\) is:

\[
t_1 = \frac{1}{P_{12} \cdot (1 - q_{\text{test}})} + \frac{1}{P_{23}}.
\]

(16)

The dispersion of the number of steps spent on the transition of the process from a non-absorbing state to an absorbing one is determined by the expression

\[
\{D_1[\alpha_m]\} = (2T - I) t - t_{sq},
\]

(17)

where \(\alpha_m\) – the number of steps spent on the transition from the non-absorbing state \(a_i\) to the absorbing, \(t_{sq}\) – «square » column vector \(t\).

\[
\{D_1[\alpha_m]\} = 2 \cdot \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{0}{1} \right) - \left( \frac{0}{1} \right) = \left( \frac{1}{P_{12} \cdot P_{23}} \right) \left( \frac{1}{1 - P_{23}} \right) \left( \frac{1}{P_{12} \cdot P_{23}} \right) ^2
\]

(18)

The dispersion of the number of steps spent on the transition of the process from the nonabsorbing state \(a_1\) to the absorbing state \(a_3\) is:
\[ d_1 = \frac{(1+P_{12})^2}{p_{12}^2 p_{23}^2} - \frac{3+P_{12}}{p_{12} p_{23}} \]  

(19)

The average time spent on the entry into communication of two stations is equal to \( t_1 \cdot \tau \), where \( \tau \) is the duration of the time frame \( T_s \).

The duration of the time frame \( T_s \) must be chosen so that the generated optical pulses do not "overlap" each other, thereby creating interference and deteriorating the efficiency of the entire QKD system. Therefore, we represent the duration of the time frame \( T_s \) as the repetition period of optical pulses depending on the length of the FOCL:

\[ T_s = \frac{2L_{\text{FOL}}}{v_{\text{OF}}} = \frac{2L_{\text{FOL}} \cdot n_{\text{OF}}}{c_{\text{opt}}} \]  

(20)

where \( L_{\text{FOL}} \) – length of FOCL, \( v_{\text{OF}} \) – speed of propagation of an optical pulse in an optical fiber, \( n_{\text{OF}} \) – refractive index of optical radiation in an optical fiber core, \( c_{\text{opt}} \) – speed of propagation of radiation in vacuum.

The multiplier 2 in the formula takes into account that in the autocompensating system of the QKD, the photon passes through the FOCL twice: the receiving-transmitting station → the FOCL → the coding station → the FOCL → the receiving-transmitting station.

Let us present the necessary formulas for calculating the average time of the receiving-transmitting and coding stations entry into connection for the proposed synchronization algorithm with the division of the FOCL into sections with decreasing length. The method of dividing a fiber-optic line into sections is described in detail in [12]. The generation frequency of the DCP is taken to be \( \xi_{\text{DCR}} = 6 \text{ Hz} \), which corresponds to the use of a single-photon avalanche photodiode ID210 SFM C (Standard) with a quantum efficiency of the photocathode of 10\%.

Let the length of the FOCL of the QKD system be \( L_{\text{FOL}} = 78.2 \text{ km} \), the linear attenuation of the signal in the optical fiber \( \alpha_{\text{OF}} = 0.2 \text{ dB/km} \), \( n_{\text{OF}} = 1.4682 \), \( c_{\text{opt}} = 300000 \text{ km/s} \), \( P_{\text{err.test}} = 0.01 \). The duration of the time frame \( T_s \) will be equal to:

\[ T_s = \frac{2 \cdot 78.2 \cdot 1.4682}{300000} \approx 0.8 \text{ ms} \]  

(21)

Analysis time \( \tau_{\text{segment,i}} \) of the i-th section of the FOCL:

\[ \tau_{\text{segment,i}} = \frac{2L_{\text{segment,i}}}{v_{\text{OF}}} \]  

(22)

In the proposed algorithm, the signal is transmitted at a single-photon level, i.e. at the exit from the coding station, one pulse contains on average \( n_{\text{s,0,mid}} = 0.1 \) photon. When passing through the FOCL, the signal undergoes weakening due to the properties of the optical fiber, therefore, the level of the transmitted signal \( n_{\text{s,i,mid}} \) at the upper boundary of the i-th section of the FOCL can be represented in the following form:

\[ n_{\text{s,i,mid}} = n_{\text{s,(i-1),mid}} \cdot 10^{-\alpha_{\text{OF}} \cdot \frac{l_{\text{segment,i}}}{10}}. \]  

(23)

Average number of DCP \( n_{\text{DCR,i,mid}} \) during the analysis of the i-th section:

\[ n_{\text{DCR,i,mid}} = \xi_{\text{DCR}} \cdot \tau_{\text{segment,i}} \]  

(24)

The smallest average number of registered photons and DCP \( n_{\text{strob,i,mid}} \) at the upper boundary of the i-th section:

\[ n_{\text{strob,i,mid}} = n_{\text{s,i,mid}} + \xi_{\text{DCR}} \cdot \tau_{\text{strob}} \]  

(25)

Probability of detecting a photon pulse \( P_{12} \) in the i-th section:

\[ P_{12,i} = 1 - e^{-n_{\text{s,i,mid}} - n_{\text{DCR,i,mid}}}. \]  

(26)
Maximum number of tests $N_{\text{test}, \text{max}, i}$ for the i-th section:

$$N_{\text{test}, \text{max}, i} = \frac{\log(1/P_{\text{err}, \text{test}})}{n_{\text{strobi, mid}}}.$$  \hspace{1cm} (27)

Probability of error during one test $Q_{23,i}$ for the i-th section:

$$Q_{23,i} = e^{-n_{\text{strobi, mid}} - n_{\text{DCR, mid}}}.$$  \hspace{1cm} (28)

The average number of steps $t_{\text{step, i, mid}}$ during the transition from the search for a photon pulse (state $a_i$) to the synchronization of the receiving-transmitting and coding stations (state $a_3$) for the i-th section:

$$t_{\text{step, i, mid}} = \frac{1}{1 - Q_{23,i}} - \frac{1}{p_{12,i}(Q_{23,i}^{N_{\text{test, max, i}} - 1})}.$$  \hspace{1cm} (29)

In the case of the proposed synchronization algorithm with splitting the FOCL into sections, when calculating the average time of entry into the connection, it is necessary to take into account the probability that the photon pulse will be exactly in the i-th section of the FOCL, therefore, the average time of entry into the connection $t_{\text{i, mid}}$ can be written as follows:

$$t_{\text{i, mid}} = t_{\text{step, i, mid}} \cdot \frac{l_{\text{segment, i}}}{l_{\text{FOL}}} \cdot T_5.$$  \hspace{1cm} (30)

The calculation results of the above formulas are shown in Table 2.

Consequently, the total average time of entry into communication $t_{\Sigma, \text{mid}}$ of the entire system is equal to the sum $t_{\text{i, mid}}$ of all sections of the FOCL:

$$t_{\Sigma, \text{mid}} = \sum_{i=1}^{10} t_{\text{i, mid}} = 177.9 \text{ ms.}$$  \hspace{1cm} (31)

Carrying out a similar calculation with identical initial data for the algorithm-analogue [13-15] without splitting the FOCL into sections, it turned out that the total average time of entry into the connection $t_{\Sigma, \text{mid}}$ of the entire system is 590.1 ms.

Analyzing the data obtained, we can say that when the FOCL is divided into sections with decreasing length, the DCP level becomes significantly lower from section to section. The proposed algorithm for the synchronization of receiving-transmitting and encoding stations with the division of FOCL into sections wins more than 3 times in terms of the time of entry into the communication of stations, compared with the algorithm-analogue [13-15], and allows you to increase the communication range at a fixed value of the synchronization error probability $P_{\text{err, test}} = 0.01$.

**Table 2.** The results of calculating the parameters of the QKD system.

| FOCL section number i | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |
|-----------------------|----|----|----|----|----|----|----|----|----|----|
| $l_{\text{segment, i}}$, km | 26.5 | 14 | 9.2 | 6.7 | 5.3 | 4.3 | 3.7 | 3.2 | 2.8 | 2.5 |
| $l_{\text{segment, i}}$, mcs | 259.4 | 137 | 90 | 65.6 | 51.9 | 42.1 | 36.2 | 31.3 | 27.4 | 24.5 |
| $n_{\text{strobi, mid}}$ | 0.0295 | 0.0155 | 0.0101 | 0.0074 | 0.0058 | 0.0048 | 0.0040 | 0.0035 | 0.0031 | 0.0027 |
| $n_{\text{DCR, mid}}$ | 0.0016 | 8.2·10^{-4} | 5.4·10^{-4} | 3.9·10^{-4} | 3.1·10^{-4} | 2.5·10^{-4} | 2.2·10^{-4} | 1.9·10^{-4} | 1.6·10^{-4} | 1.5·10^{-4} |
| $p_{12,i}$ | 0.0295 | 0.0155 | 0.0101 | 0.0074 | 0.0058 | 0.0048 | 0.0040 | 0.0035 | 0.0031 | 0.0027 |
| $P_{12,i}$ | 0.0306 | 0.0162 | 0.0106 | 0.0078 | 0.0061 | 0.0050 | 0.0042 | 0.0037 | 0.0032 | 0.0029 |
| $N_{\text{test, max, i}}$ | 156 | 297 | 454 | 618 | 789 | 962 | 1141 | 1322 | 1504 | 1687 |
| $Q_{23,i}$ | 0.9694 | 0.9838 | 0.9894 | 0.9922 | 0.9939 | 0.9950 | 0.9958 | 0.9963 | 0.9968 | 0.9971 |
| $t_{\text{step, i, mid}}$ | 65.63 | 124.1 | 189 | 257.1 | 327.7 | 399.5 | 473 | 547.9 | 623.3 | 699.2 |
| $t_{\text{i, mid}}$, ms | 17.8 | 17.8 | 17.8 | 17.6 | 17.8 | 17.6 | 17.9 | 17.9 | 17.9 | 17.9 |
3 Conclusions

A methodology is proposed for calculating the average time of entry into synchronism of stations the system of quantum key distribution with sequential polling of fiber-optic line sections with decreasing length.

A diagram of states and transitions for sequential search for a photon pulse has been constructed. Analytical expressions are obtained for finding the probability of detecting a photon pulse and the dispersion of the number of steps for entry into synchronism of stations.

The analysis of the results obtained showed that when the FOCL is divided into sections with decreasing length, the level of the dark current pulses significantly decreases from section to section. In comparison with the algorithm-analogue, the proposed algorithm wins more than 3 times in terms of the time of entry into communication of stations. The results obtained indicate the possibility of increasing the communication range while ensuring the synchronization error probability at the level of 0.01.

Acknowledgments

The reported study was funded by RFBR according to the research project 20-37-90040.

References

1. Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Reviews of Modern Physics 74(1) 145–195
2. Rumyantsev K E and Pljonkin A P 2014 Izvestia SFedU. Technical science 8 81–96
3. Rumyantsev K E 2011 Systems of quantum key distribution (Taganrog: Publishing House of TTI SFU) p 264
4. Rumyantsev K E and Pljonkin A P 2015 Izvestia SFedU. Technical science 5 135–153
5. Kurochkin V L 2012 Photonika 5 54–66
6. Rumyantsev K E and Pljonkin A P 2016 International Conference on Electronics, Information, and Communications (ICEIC’16) 1–4 DOI: 10.1109/ELINFOCOM.2016.7562955
7. Rumyansev K E and Pljonkin A P 2015 Radio engineering 2 125–134
8. Rudinsky E and Rumyansev K 2017 2nd International Conference on Multimedia and Image Processing (ICMIP’17) 346–349 DOI: 10.1109/ICMIP.2017.68
9. Plenkin A, Rumyantsev K and Rudinsky E 2017 IEEE East-West Design & Test Symposium (EWDTS’17) DOI: 10.1109/EWDTS.2017.8110047
10. Gal'yardi R M and Karp Sh 1978 Optical communication (Moscow: Svya') p 424
11. Boumejstera D, Ekerta A and Cajlingera A 2002 Physics of Quantum Information: Quantum Cryptography. Quantum teleportation. Quantum computing (Moskva: Postmarket) p 376
12. Mironov Y K and Rumyantsev K E 2019 Futuristic Trends in Networks and Computing Technologies (FTNCT’19) 87–97 DOI: https://doi.org/10.1007/978-981-15-4451-4_8
13. Rudinsky E and Rumyansev K 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC’18) 765–769, DOI: 10.1109/PDGC.2018.8745863
14. Rumyansev K and Rudinsky E 2017 Proceedings of the 10th International Conference
15. Rumyansev K E and Rudinsky E A 2017 Izvestia SFedU. Technical science 5 75-89
16. Sheremet'yev A G 1971 Statistical theory of laser communication (Moscow: Svyaz') p 264