Study of the characteristics of the synchronization algorithm for a quantum key distribution system based on comparing the number of samples from an adjacent pair of time windows with a threshold level

Y K Mironov¹, P D Mironova¹, K E Rumyantsev¹
¹ Department of Information Security of Telecommunication Systems, Southern Federal University, Taganrog, str. Chekhov, 2, 347922, Russia

E-mail tmiyap117@gmail.com

Abstract. The analysis of time and probabilistic characteristics is carried out for a two-stage synchronization algorithm in a quantum key distribution (QKD) system with automatic compensation of polarization distortions. Formulas are obtained for calculating the missing probabilities a signal pair of windows, false alarm and successful synchronization. The dependences of the missing probability a signal pair on the average number of photons and noise pulses are investigated during the analysis of a pair of windows for different threshold levels. The numerical material obtained in the course of the study indicates the possibility of using for express calculations the probability of detecting a signal pair of windows formulas oriented to the normal distribution of the number of recorded pulses at the output of a single-photon avalanche photodiode.

Keywords: Quantum key distribution; Autocompensation system; Synchronization; Time parameters; Probabilistic characteristics; Fiber-optic line

1. Introduction

Systems of quantum key distribution (QKD) provide increased security of transmitted information. For the stable operation of the QKD system, accurate synchronization of user stations is required with minimal time. The issues of security of systems for quantum key distribution and station synchronization were studied in the works of domestic and foreign scientists [1-11].

In [12], the influence of the atmosphere on the accuracy of synchronization in the quantum key distribution in free space (QKD) was investigated. It is noted that fluctuations in the intensity of the synchronizing light due to atmospheric disturbances make a much larger contribution for the synchronization accuracy than others. In [13], the effect of random noise is studied, which is constantly present in synchronization in a practical CV-QKD (CV – continuous-variable) system, on system safety, including its effect on data sampling and parameter estimation.

In [14-15], synchronization algorithms imply the division of a frame into windows. The duration of the time window, equal to the duration of the pulse repetition period, significantly exceeds the duration of the synchronizing pulse. Time frames are analyzed sequentially. The signal window is the window where the largest number of photons is registered.
Another synchronization method also involves dividing a frame into windows [16]. However, the window duration is comparable to the duration of the synchronizing pulse. If the window durations and the synchronizing pulse are equal, the probability of finding the pulse at the border of adjacent windows is high. Therefore, at the first stage of synchronization, it is necessary to analyze windows in pairs.

The modified algorithm for searching for a photon pulse by analyzing a pair of adjacent windows, each of which is equal to the pulse duration, provides a higher probability of detecting a pair of windows compared to algorithms with an average number of registered photons in a pulse of more than 6 [17].

In the proposed algorithm for searching for a photon pulse, the decision to accept an adjacent pair of windows as a signal one follows when the total number of photons from an adjacent pair of time windows exceeds a given threshold level. Here, a photon pulse means an optical pulse, where the average number of photons during the observation time does not exceed 1. The tests continue until the threshold level \( k \) is exceeded or the time resources are exhausted.

The purpose of the research is a complex analysis of probabilistic and time characteristics of detecting an adjacent pair of time windows containing a photon pulse for an autocompensating fiber-optic quantum key distribution system.

2. The missing probability a signal pair
In the proposed algorithm, the detection process begins with dividing a frame equal in duration to the pulse repetition period \( T \) into time windows. The duration of the windows is commensurate with the duration of the synchronizing pulse \( \tau \). When the durations of the synchronizing pulse and frames are comparable, the latter must be analyzed in pairs. Sequential interrogation of adjacent time windows is performed until the number of photons (hereinafter photons) and/or dark current pulses (DCP) registered in them exceeds a given threshold level \( k_0 \). If the result of the threshold test is positive, the corresponding pair of adjacent windows is taken as a signal pair, and then the process of accuracy the time position of the synchronizing pulse in the adjacent pair of time windows begins.

Note that, when speaking about registered photons, we take into account the fact that not all received photons are converted into single-photon pulses (SPP), which represent the responses of a single-photon avalanche photodiode (SAPD). Indeed, the quantum efficiency of the SAPD photocathode is always less than 1.

Let the average number of photons in a photon pulse be \( \bar{n}_s \), and the average number of noise pulses (DCP) in the time window \( \bar{n}_b \).

The probability of detection in the signal pair \( p_{th,s} \) at a given threshold level \( k_0 \) when orientation on the description of the statistical properties of photodetection by the Poisson model is

\[
p_{th,s} = \sum_{k=k_0}^{\infty} \frac{\bar{n}_b^{-k}}{k!} \cdot \exp(-\bar{n}_s) = \sum_{k=k_0}^{\infty} \frac{\bar{n}_b^{-k}}{k!} \cdot \exp(-\bar{n}_s), \tag{1}
\]

where \( \bar{n}_{sb} = \bar{n}_s + 2 \cdot \bar{n}_b \) – average total number of photons and DCP in a signal pair of windows.

If the Gaussian model is used, then

\[
p_{th,s} = \frac{1}{2} - \frac{1}{2} \cdot \text{erf} \left( \frac{k_0 - \bar{n}_sb}{\sqrt{2} \bar{n}_b} \right), \tag{2}
\]

where \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \cdot \int_0^x \exp(-t^2) \cdot dt \) – error function.

The threshold value is selected from the requirement of the admissible probability of a false alarm \( p_{th,b} \), i.e. exceeding the threshold level \( k_0 \) by the total number of \( k=\bar{n}_s+\bar{n}_b \) noise pulses recorded in an adjacent pair of noise time windows.

The false alarm probability \( p_{th,b} \) is related to the threshold level \( k_0 \) by the ratio

\[
p_{th,b} = \sum_{k=k_0}^{\infty} P_{os}(k, 2 \cdot \bar{n}_b) \tag{3},
\]

when orientation on the Poisson model, and the relation

\[
p_{th,b} = \frac{1}{2} - \frac{1}{2} \cdot \text{erf} \left( \frac{k_0 - \bar{n}_b}{2 \sqrt{\bar{n}_b}} \right), \tag{4}
\]

when orientation on the Gaussian model.

For \( \bar{n}_{sb} \geq 9 \) (multiphoton or current synchronization mode), the threshold level \( k_0 \) for a given probability \( p_{th,b} \) is determined using the inverse function \( \text{erf}^{-1}(x) \) to \( \text{erf}(x) \):
\[ k_{th} = 2 \cdot \bar{n}_b + \sqrt{4 \cdot \bar{n}_b \cdot erf^{-1}(1 - 2 \cdot p_{th,b})}. \tag{5} \]

Figure 1 shows the dependences of the missing probability a signal pair \( p_{th, sb} = 1 - p_{th,s} \) on the average number of signal SPP and noise pulses \( \bar{n}_{sb} \) for threshold levels \( k_{th} \) equal to 2 (solid line), 4 (dashed line) and 8 (dotted line). The calculations were performed according to formula (1) with orientation to the Poisson model (step functions) and (2) with orientation to the Gaussian model (continuous functions).

Figure 1. Dependences of the missing probability a signal pair on the average number of photons and noise pulses in a signal pair of time windows

It can be seen that the missing probability a signal pair, calculated when orienting to a normal distribution, gives an over value. Moreover, the probabilities differ by a factor of 2 for the average number of photons and noise pulses \( \bar{n}_{sb} = 5 \) and the threshold level \( k_{th} = 2 \). The difference exceeds 4 times with an average number of pulses \( \bar{n}_{sb} \geq 7 \).

Note that the difference decreases with increasing threshold level. So, for example, if with the average total number of photons and noise pulses \( \bar{n}_{sb} = 3 \) the difference in the missing probability is 1.42 times at the threshold level \( k_{th} = 2 \), then already only 1 % at \( k_{th} = 8 \).

An acceptable difference in the missing probabilities (about 10…20 %) is provided under the condition \( k_{th} \cdot p_{th, sb} > 1 \). From the formula

\[ p_{th,s} = \frac{1}{2} \left[ 1 - erf \left( \frac{k_{th} - \bar{n}_{sb}}{\sqrt{2n_{sb}}} \right) \right] = \frac{1}{2} \cdot erfc \left( \frac{k_{th} - \bar{n}_{sb}}{\sqrt{2n_{sb}}} \right). \tag{6} \]

for normal approximation with \( k_{th} = \bar{n}_{sb} \) we find \( p_{th,s} = 0.5 \). Therefore, according to the normal approximation, the threshold level \( k_{th} \) should exceed the value of the average total number of photons and noise pulses \( \bar{n}_{sb} \) to ensure the detection probability in the signal pair is more than 0.5. The same conclusion is also valid when orientation on the Poisson model.

The missing probability a signal pair of 0.1 is provided at the threshold level \( k_{th} = 2 \) and the average number of photons and noise pulses in a pair of time windows \( \bar{n}_{sb} \approx 4 \) for the Poisson model and \( \bar{n}_{sb} \approx 4.8 \) for the Gaussian model. The difference in the average number of photons and noise pulses in the signal pair increases from 20% to 32 and 41% while ensuring the probability of missing, respectively, to 0.01 and 0.001. The numerical material indicates the possibility of using formula (2) or (6) for express calculations of the probability of detecting a signal pair of windows.

It is important to note that the missing probability a signal pair is determined not only by the signal-to-noise ratio, but also by the average number of noise pulses in a pair of time windows (Figure 2).

3. Synchronization probability

The synchronization process continues until the registered number of photons and noise pulses in the signal pair of windows exceeds the value of the set threshold. During synchronization, errors are possible
due to a false alarm in a pair of windows preceding the signal pair in time. In addition, it is possible to miss a signal pair if the number of pulses registered in it does not exceed the set threshold.

Figure 2. Working characteristic of detection

Therefore, to estimate the efficiency of synchronization, the synchronization probability is introduced, which will mean the probability of detecting a signal pair of windows, in which the synchronization signal is located, for a given number of time frames.

Let the sync pulse be located in the \( i \)-th pair of windows. The total number of paired windows \((1, 2), (2, 3), \ldots, (N_w-1, N_w), (N_w, 1)\) in the time frame is equal to \(N_w\). It is considered that the sync pulse can be equally likely to be present in any pair of time windows.

The conditional probability of synchronization during the analysis of the first time frame \( j_{T}=1 \) is

\[ p_{\text{sync}}(i, j_{T}=1) = p_{\text{sync}}(i) = (1 - p_{\text{th,b}})^{i-1} \cdot p_{\text{th,s}}. \]

Averaging this probability over all possible pairs of windows (sync pulse positions) gives the conditional synchronization probability during the analysis of the first time frame

\[ p_{D1}(j_{T}=1) = p_{D1} = \frac{1}{N_w} \cdot \sum_{i=1}^{N_w} p_{\text{sync}}(i) = \frac{1}{N_w} \cdot \sum_{i=1}^{N_w} (1 - p_{\text{th,b}})^{i-1} \cdot p_{\text{th,s}}, \]

from where

\[ p_{D1} = p_{\text{th,s}} \cdot \frac{1 - (1 - p_{\text{th,b}})^{N_w}}{p_{\text{th,b}}}. \]

Figure 3 shows the graphs of the dependences of the conditional probability of synchronization in the process of analyzing the first frame on the average number of signal SPP over the duration of the sync pulse. When plotting the graphs, it is assumed that the average number of noise pulses in the window is 2. The choice of the threshold level 10 provides the probability of a false alarm when analyzing a pair of noise windows for a sync pulse duration of 0.0081.

The graphs show that with an increase in the average number of photons over the duration of the sync pulse, the probability of synchronization increases during the analysis of the first frame. However, this growth is slowing down, tending to a certain limiting value. To find this limiting value, we use the power series expansion function

\[ (1 - p_{\text{th,b}})^{N_w} = 1 - N_w \cdot p_{\text{th,b}} + \frac{(N_w p_{\text{th,b}})^2}{2!} + \frac{(N_w p_{\text{th,b}})^3}{3!} - \ldots. \]

Then, expression (7), limited by three terms, transforms to the form

\[ p_{D1,\text{lim1}} = p_{\text{th,s}} \cdot \left[1 - \frac{N_w p_{\text{th,b}}}{2}\right]. \]

Calculations by formula (8) give results that differ from calculations by formula (7) by less than 10% when the number of time windows is 80. Moreover, the difference decreases rapidly with decreasing number of windows (only 1% at \(N_w=20\)).
More accurate results are given using the formula

\[ p_{D1,lim2} = p_{ths} \times \left[ 1 - \frac{N_w p_{th,b}}{2} + \frac{(N_w p_{th,b})^2}{6} \right], \]  

(9)

is obtained from (7) under the restriction of 4 terms in the expansion in a power series. The difference relative to the calculations using the exact formula is 1% even with 80 windows.

![Figure 3. Dependences of the probability of synchronization in the analysis of the first frame on the average number of signal SPP for the duration of the sync pulse](image)

Note that the calculation according to the formula (8) gives an underestimated value, and according to the formula (9) – an overestimated value. Using these features, it is possible to formulate requirements for the probability of a false alarm in a noise pair \( p_{th,b} \). Naturally, while ensuring the limiting probability of synchronization when analyzing the first frame, the difference in the values calculated by formulas (8) and (9) will be minimal.

Let the distinction be \( K_{pD1} \) times. Then \( K_{pD1} = \frac{p_{D1,lim2}}{p_{D1,lim1}} \). Solving the quadratic equation we find

\[ N_w \cdot p_{th,b} = -1.5 \cdot (K_{pD1} - 1) + \sqrt{2.25 \cdot (K_{pD1} - 1)^2 + 6 \cdot (K_{pD1} - 1)}. \]

Therefore, the choice of the probability of a false alarm in a noise pair \( p_{th,b} \) must always satisfy the condition

\[ p_{th,b} \leq p_{th,b,max} = \frac{2.25(K_{pD1}-1)^2+6(K_{pD1}-1)-1.5(K_{pD1}-1)}{N_w}. \]  

(10)

It follows from (10) that the maximum permissible probability of a false alarm in a noise pair is inversely proportional to the number of time windows. In the particular case with \( K_{pD1}=1.1 \), we have \( N_w p_{th,b,max} \approx 0.64 \).

Having performed similar calculations, we find the ratios for calculating the limiting permissible probability of a false alarm in a noise pair \( p_{th,b,max} \) for a given permissible deviation of \( K_{pD1} \) times from the limiting synchronization probability \( p_{D1,lim1} \):

\[ N_w \cdot p_{th,b,max} \approx \begin{cases} 0.84 & \text{at } K_{pD1} = 1.20; \\ 0.64 & \text{at } K_{pD1} = 1.10; \\ 0.48 & \text{at } K_{pD1} = 1.05; \\ 0.32 & \text{at } K_{pD1} = 1.02; \\ 0.23 & \text{at } K_{pD1} = 1.01. \end{cases} \]  

(11)

A decrease in the deviation of the real probability of synchronization from the limiting value implies the presentation of more stringent requirements for the probability of a false alarm in a noise pair. For
example, the requirement to reduce the deviation from 20% to 10% will require a decrease in the probability of a false alarm by at least 1.3 times, to 5% – by 1.75 times, and to 1% – by almost 4 times.

According to the adopted synchronization algorithm, if no sync pulse is detected during the first frame, then it is necessary to repeat the analysis of the second time frame. The conditional probability of detecting a sync pulse during the second frame is \( p_{D2} = (1 - p_{D1}) \cdot p_{D1} \).

Using the method of mathematical induction, we find the conditional probability of detecting a sync pulse in the \( j \)-th time frame \( p_{Dj} = (1 - p_{D1})^{j-1} \cdot p_{D1} \).

Successful synchronization with the assumption of search in \( N_T \) time frames is possible with an unconditional probability (hereinafter the probability)

\[
P_D = \sum_{j=1}^{N_T} p_{Dj} = \sum_{j=1}^{N_T} (1 - p_{D1})^{j-1} \cdot p_{D1} = \frac{p_{D1}}{1 - p_{D1}} \cdot \sum_{j=1}^{N_T} (1 - p_{D1})^j.
\]

Using the properties of a geometric progression, we find

\[
P_D = 1 - (1 - p_{D1})^{N_T}.
\]  \( \text{Equation 12} \)

Note that as \( N_T \to \infty \), the probability of successful synchronization tends to 1.

From (12) it follows that to provide a given synchronization probability \( P_D \) with a known probability \( p_{D1} \), an analysis of at least \( N_{T,\text{min}} \) time frames is required. Thus,

\[
N_T \geq N_{T,\text{min}} = \left\lceil \frac{\lg(1 - p_{D1})}{\lg(1 - p_{D1})} \right\rceil,
\]  \( \text{Equation 13} \)

where \( \lceil E \rceil \) – smallest integer greater than \( E \).

The average number of time frames for successful synchronization is determined by the formula:

\[
\overline{N_T} = \sum_{j=1}^{N_T} j \cdot (1 - p_{D1})^{j-1} \cdot p_{D1}.
\]

In the limiting case, at \( N_T \to \infty \), we find the limiting-maximum value of the average number of time frames for successful synchronization:

\[
\overline{N_T} = \frac{1}{p_{D1}} = \frac{N_T}{p_{\text{ths}}} \left[ \frac{p_{\text{th.b}}}{1 - (1 - p_{\text{th.b}})^{N_T}} \right].
\]

Therefore, the average time of entry into synchronism

\[
\overline{T_{\text{sync}}} = T_s \cdot \overline{N_T} = \frac{N_T T_s}{p_{\text{ths}}} \left[ \frac{p_{\text{th.b}}}{1 - (1 - p_{\text{th.b}})^{N_T}} \right].
\]  \( \text{Equation 14} \)

If the probability of false alarms \( p_{\text{th.b}} \) is close to one, then the average time taken to detect a sync pulse can be very large \( \overline{T_{\text{sync}}} \approx N_w \cdot T_s/p_{\text{ths}} \). On the contrary, if \( N_w p_{\text{th.b}} \ll 1 \), to \( (1 - p_{\text{th.b}})^{N_w} \approx 1 - N_w p_{\text{th.b}} \).

Then \( \overline{T_{\text{sync}}} \approx 1/p_{\text{ths}} \). Taking into account condition (14), it can be argued that the average time spent on detecting a sync pulse will always exceed the value

\[
\overline{T_{\text{sync}}} = T_s \cdot \overline{N_T} = N_{T,\text{min}} \cdot \frac{T_s}{p_{\text{ths}}} \left[ \frac{p_{\text{th.b}}}{1 - (1 - p_{\text{th.b}})^{N_T}} \right] = \frac{\lg(1 - p_{D1})}{\lg(1 - p_{D1})} \cdot \frac{T_s}{p_{\text{ths}}} \left[ \frac{p_{\text{th.b}}}{1 - (1 - p_{\text{th.b}})^{N_T}} \right].
\]  \( \text{Equation 15} \)

The formulas obtained make it possible to develop a technique for designing equipment for detecting a sync signal based on an analysis of the sum of counts from an adjacent pair of windows with a threshold level in the course of further research.

4. Conclusion

Formulas for calculating the missing probabilities a signal pair, successful synchronization and a false alarm have been determined. The dependences of the missing probability a signal pair on the average number of photons and noise pulses are investigated for various threshold levels. The missing probability a signal pair, calculated when orienting to the normal distribution, gives an overestimated value, compared to the missing probability a signal pair, calculated when orienting to the Poisson distribution. The dependences of the conditional synchronization probability during the analysis of the first frame on the average number of photons over the duration of the sync pulse are investigated. With an increase in the average number of photons over the duration of the sync pulse, the probability of synchronization increases during the analysis of the first frame. The numerical material obtained in the course of the study indicates the possibility of using formulas oriented to the normal distribution for express calculations of the probability of detecting a signal pair of windows.

Relationships are obtained for calculating the limiting permissible probability of a false alarm in a noise pair for a given permissible deviation from the limiting synchronization probability. A decrease
in the deviation of the real probability of synchronization from the limiting value implies the presentation of more stringent requirements for the probability of a false alarm in a noise pair.

The resulting formulas and dependencies made it possible to form relationships for calculating the average time spent on detecting a sync pulse.

5. Acknowledgment
The reported study was funded by RFBR, project number 20-37-90040.

References

[1] Pljonkin A and Rumiantsev K 2016 Single-photon synchronization mode of quantum key distribution system Proceeding of the International Conference on Computational Techniques in In-formation and Communication Technology pp 531–534 DOI: 10.1109/ICICTICT.2016.7514637

[2] Salvail L, Peev M, Diamanti E, Alleaume R, Lütkenhaus N and Länger T 2010 Security of trusted repeater quantum key distribution networks Journal of Computer Security 18 (1) pp 61–87

[3] Gobby C, Yuan Z and Shields A 2004 Quantum key distribution over 122 km of standard telecom fiber Applied Physics Letters 84 (19) pp 3762–3764 DOI: 10.1063/1.1738173

[4] Cabello A 2000 Quantum key distribution without alternative measurements Physical Review A 61 (5) 052312 pp 1–4 DOI: doi.org/10.1103/PhysRevA.61.052312

[5] Hiskett P A, Rosenberg D, Peterson C G, Hughes R J, Nam S, Lita A E, Miller A J and Nordholt J E 2006 Long-distance quantum key distribution in optical fibre New Journal of Physics 8 pp 1–7 DOI: 10.1088/1367-2630/8/9/193

[6] Patel K A, Dynes J F, Choi I, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2012 Coexistence of high-bit-rate quantum key distribution and data on optical fiber Physical Review X 2 (4) pp 1–8 DOI: 10.1103/PhysRevX.2.041010

[7] Lindsey W C 1972 Synchronization Systems in Communication and Control (Prentice-Hall, Englewood Cliffs, New Jersey)

[8] Gobby G, Yuan Z L and Shields A J 2004 Unconditionally secure quantum key distribution over 50 km of standard telecom fibre Electronics Letters 40 pp 1603–1605 DOI: 10.1049/el:20045038

[9] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices Proceedings of International Symposium On Information Theory p 136

[10] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W S, Plews A, Sharpe A W, Yuan Z and Shields A J 2017 Long-distance quantum key distribution secure against coherent attacks Optica 4 pp 163–167 DOI: 10.1364/OPTICA.4.000163

[11] Kurochkin V L 2012 Eksperimental'nye issledovaniya v oblasti kvantovoj kriptografii [Experimental research in the field of quantum cryptography] Fotonika [Photonika] 5 pp 54–66

[12] Wu Qing-Lin, Han Zheng-Fu, Miao Er-Long, Liu Yun, Dai Yi-Min and Guo Guang-Can 2007 Synchronization of free-space quantum key distribution Optics Communications 275 (2) pp 486–490

[13] Xie Cailang, Guo Ying, Liao Qin, Zhao Wei, Huang Duan, Zhang Ling and Zeng Guihua 2018 Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization Physics Letters A 382 (12) pp 811–817

[14] Rumiantsev K and Rudinsky E 2017 Parameters of the two-stage synchronization algorithm for the quantum key distribution system Proceedings of the 10th International Conference on Security of Information and Networks (SIN-2017) pp 140–150 DOI: 10.1145/3136825.3136888
[15] Mironov Y K and Rumyantsev K E 2020 Single-Photon Algorithm for Synchronizing the System of Quantum Key Distribution with Polling Sections of a Fiber Optic Line *Futuristic Trends in Networks and Computing Technologies* pp 87–97 DOI: https://doi.org/10.1007/978-981-15-4451-4_8

[16] Gagliardi R M and Karp Sh 1976 *Optical communication* p 432

[17] Mironov Y K and Mironova P D 2020 Veroyatnost' obnaruzheniya signal'nogo okna v algoritme poiska fotonnogo impul'sa s razbieniem vremennogo intervala na vremennye okna [Probability of detecting a signal window in the algorithm for searching for a photon pulse with a division of the time interval into time windows] *Fundamental'nye i prikladnye aspekty komp'yuternyh tekhnologij i informacionnoj bezopasnosti [Fundamental and applied aspects of computer technology and information security]* pp 135–138