SINCONF 2020

13th International Conference on Security of Information and Networks

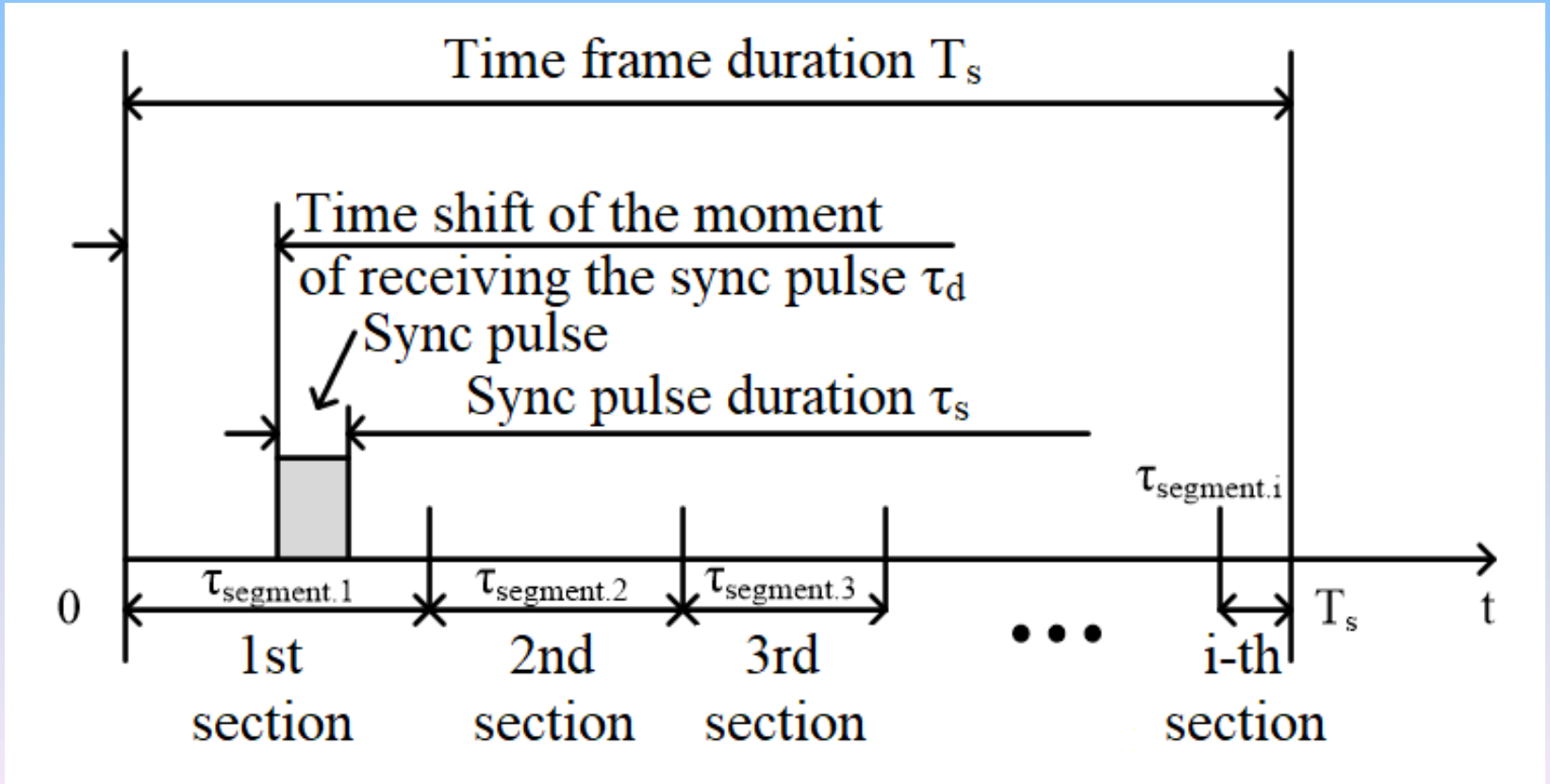
Characteristics of a two-stage synchronization algorithm in the system of quantum key distribution with dividing a fiber-optic line into sections with decreasing length

Yakov Mironov
Postgraduate student
Southern Federal University, Russia
tmiyap117@gmail.com

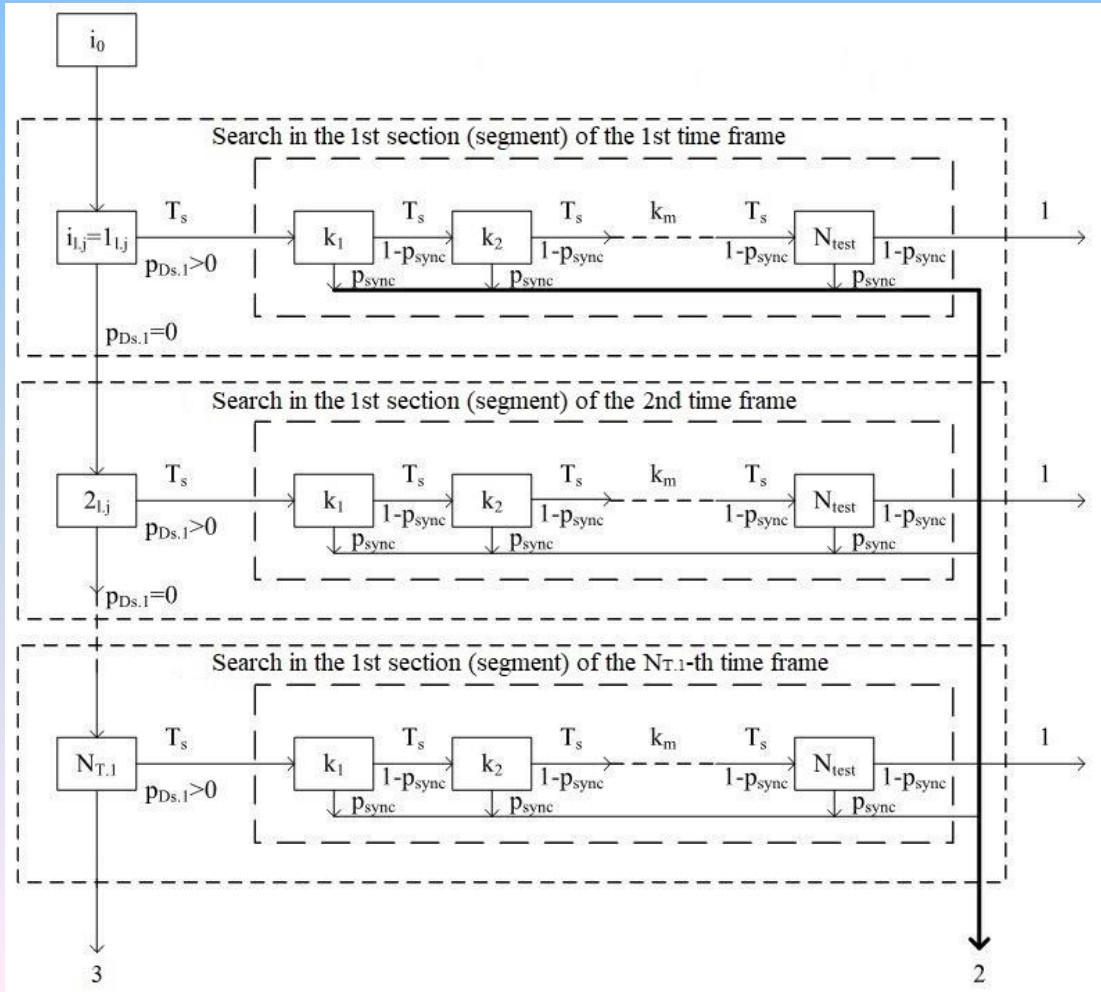
Polina Mironova
Postgraduate student
Southern Federal University, Russia
linenkopdem@gmail.com

Konstantin Rumyantsev
Doctor of Engineering Science
Southern Federal University, Russia
rke2004@mail.ru

Algorithm for the synchronization of stations in the quantum key distribution system



Scheme of the search for a photon in the first section of the FOCL



Time parameters of the algorithm

1. Time of detection of a sync pulse in the $i_{l.j}$-th frame ($N_{T.j} \geq i_{l.j} \geq 1$) of the j-th section of the fiber-optic link of length l_j during the k_m-th testing ($N_{test} \geq k_m \geq 1$)

$$\tau_{l.j.D} = t_{l.(j-1)} + x_{sj} + \left(i_{l.j} + k_m - 1\right) \cdot T_s + \Delta\tau + 0{,}5 \cdot \tau_{strob}.$$

2. Time of analyze the *j*-th section of the FOCL with a negative testing result in the $i_{l.j}$-th frame ($N_{T.j} \geq i_{l.j} \geq 1$)

$$\tau_{l.j.ND} = t_{l.(j-1)} + x_{s.j} + \left(i_{l.j} + N_{test} - 1\right) \cdot T_s + \Delta\tau + 0{,}5 \cdot \tau_{strob}.$$

3. Time of analyze the *j*-th section of the FOCL, where the photon was not registered for the maximum number of time frames $N_{t.j}$

$$\tau_{l.j.lim} = t_{l.(j-1)} + N_{T.j} \cdot T_s.$$

Energy parameters of the algorithm

Average number of registered photons per quantum pulse duration in the analysis of the *j*-th section of the FOCL

$$\overline{n_{s.j}} = \overline{n_{s.0}} \cdot 10^{-\frac{K_{s.j}[dB]}{10}},$$

where $\overline{n_{s.0}}$ – average number of photons per pulse at the output of the coding station; $K_{s.j}$ – attenuation coefficient of a quantum pulse when analyzing the j-th section of a FOCL.

Average number of dark current pulses during the analysis of the *j*-th section of the FOCL $\tau_{l.j}$

$$\overline{n_{DCR.j}} = \xi_{DCR} \cdot \tau_{l.j},$$

where ξ_{DCR} – frequency (rate) of generation of dark current pulses in a single-photon photodetector.

Average number of dark current pulses over the duration τ_s of an optical pulse

$$\overline{n_{DCR.s}} = \xi_{DCR} \cdot \tau_s.$$

Probability characteristics of a two-stage time synchronization algorithm

1. Probability of finding a quantum pulse in the j_s-th section of the FOCL with length l_{js}

$$p(l_{js}) = l_{js}/L_{FOL}\,, \qquad j_s = \overline{1, N_{FOL}},$$

where L_{FOL} – total length of FOCL; N_{FOL} – number of FOCL sections.

2. Probability of the absence of reception of a photon and/or dark current pulses during the analysis of the j-th section of the FOCL τ_{lj}

$$P_{DCR0.j} = \begin{cases} exp\left(-\overline{n_{DCR.j}}\right), & j = \overline{1, j_s - 1} \text{ и } j = \overline{j_s + 1, N_{FOL}}; \\ exp\left(-\overline{n_{s.j}} - \overline{n_{DCR.j}}\right), & j = j_s. \end{cases}$$

Probability characteristics of a two-stage time synchronization algorithm

3. The calculation of the probability of registering at least one photon or dark current pulse when analyzing the *j*-th FOCL section

$$P_{Ds.j} = \begin{cases} 1 - exp\left(-\overline{n_{DCR.j}}\right) = 1 - P_{DCR0.j}\,, & j \neq j_s; \\ 1 - exp\left(-\overline{n_{s.j}} - \overline{n_{DCR.j}}\right), & j = j_s. \end{cases}$$

4. Probability of the absence of registration of a photon and/or a dark current pulse for the limiting number of time frames $N_{T.j}$ in the *j*-th FOCL section

$$P_{D.j}\{N_{T.j}\} = \begin{cases} 1 - \dfrac{1 - exp\left(-\overline{n_{DCR0.j}}\right)}{\overline{n_{DCR0.j}}} \cdot \left(1 - {P_{DCR0.j}}^{N_{T.j}}\right), & j \neq j_s; \\ 1 - \dfrac{1 - exp\left(-\overline{n_{DCR0.j}}\right)}{\overline{n_{DCR0.j}}} \cdot \dfrac{1 - {P_{DCR0.j}}^{N_{T.j}}}{1 - P_{DCR0.j}} \cdot P_{Ds.j}, & j = j_s. \end{cases}$$

Conclusions

A two-stage synchronization algorithm is formulated in the QKD system with the division of FOCL into sections with decreasing length.

The analysis of time and energy parameters of the proposed algorithm is carried out.

The probabilistic characteristics of a two-stage time algorithm of synchronization in the absence of a priori information about the distance between stations are established.

Thank you for attention!