

Polupanova Elena Evgenievna – Kuban State University; e-mail: jienka@mail.ru; Krasnodar, Russia; phone: +79284013301, the department of computational technologies; cand. of eng. sc.; associate professor; ORCID: <https://orcid.org/0000-0002-0364-1132>.

Oleynik Alexander Sergeevich – e-mail: wastocryter@mail.ru; phone: +89186725060, the department of computational technologies; master's degree student.

УДК 621.396.96

DOI 10.18522/2311-3103-2023-3-96-107

К.Е. Румянцев, П.Д. Миронова**ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ АЛГОРИТМА ОБНАРУЖЕНИЯ СИНХРОСИГНАЛОВ НА ОСНОВЕ ВЫБОРА СМЕЖНОЙ ПАРЫ СЕГМЕНТОВ С МАКСИМАЛЬНЫМ СУММАРНЫМ ОТСЧЁТОМ**

Предложен алгоритм обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом. Указанный алгоритм учитывает недостатки альтернативного алгоритма обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем, состоящие в необходимости знания уровня фонового и шумового воздействия, который определяет пороговый уровень и вероятность ошибочного обнаружения сигнальной пары сегментов. Исследована зависимость вероятности ошибки обнаружения синхроимпульса от среднего числа сигнальных фотонов в синхроимпульсе при различных значениях числа сегментов во временном кадре. Так, вероятность ошибочного обнаружения синхроимпульса в течение кадра значительно уменьшается по мере роста среднего числа фотонов в синхроимпульсе. Например, при увеличении среднего числа сигнальных фотонов в синхроимпульсе с 1 до 5 вероятность ошибки обнаружения синхроимпульса снижается в 37 раз. Необходимо отметить слабое влияние числа пар сегментов на вероятность ошибочного обнаружения, что указывает на слабое влияние импульсов темнового тока на вероятностные характеристики предложенного алгоритма обнаружения синхросигналов. Получены аналитические выражения для точного и экспресс-расчёта вероятностных характеристик обнаружения, учитывающие вероятность нахождения синхроимпульса на границе двух смежных сегментов в связи с равенством длительностей синхроимпульса и временного сегмента. Результаты расчёта по точным выражениям вероятности обнаружения синхроимпульса показали, что при отношении сигнал/шум равном 10 и выше влиянием шумовых импульсов на вероятность обнаружения синхроимпульса можно пренебречь. Отмечено, вероятность обнаружения будет тем больше, чем больше число регистрируемых событий, или, другими словами, чем больше сумма средних чисел сигнальных фотонов и импульсов темнового тока. Расчёт вероятности обнаружения синхроимпульса по упрощённым выражениям показывает незначительное отклонение от расчётов по точным формулам, которое не превышает 5,3 %, причём расчёт по приближённым выражениям даёт заниженный результат. Полученные приближённые аналитические выражения могут применяться для экспресс-расчёта вероятности обнаружения синхроимпульса в паре сегментов.

Квантовое распределение ключа; синхронизация; максимальный суммарный отсчёт; вероятностные характеристики.

К.Е. Rumyantsev, P.D. Mironova**PROBABILISTIC CHARACTERISTICS OF THE SYNC DETECTION ALGORITHM BASED ON THE SELECTION OF AN ADJACENT PAIR OF SEGMENTS WITH THE MAXIMUM TOTAL COUNT**

An algorithm for detecting sync signals based on the selection of an adjacent pair of segments with the maximum total count is proposed. This algorithm takes into account the shortcomings of an alternative algorithm for detecting a sync signal based on comparing the sum of samples from an adjacent pair of segments with a threshold level, consisting in the need to know the

level of background and noise influence, which determines the threshold level and the probability of erroneous detection of a signal pair of segments. The dependence of the probability of an error in detecting a sync pulse on the average number of signal photons in a sync pulse is studied for various values of the number of segments in a time frame. Thus, the probability of erroneous detection of a sync pulse during a frame decreases significantly as the average number of photons in a sync pulse increases. For example, by increasing the average number of signal photons in a sync pulse from 1 to 5, the probability of a sync detection error is reduced by a factor of 37. It should be noted that the number of pairs of segments has a weak effect on the probability of erroneous detection, which indicates a weak effect of dark current pulses on the probabilistic characteristics of the proposed algorithm for detecting sync signals. Analytical expressions are obtained for accurate and express calculation of probabilistic characteristics of detection, taking into account the probability of finding a sync pulse at the boundary of two adjacent segments due to the equality of the duration of the sync pulse and the time segment. The results of calculation using exact expressions for the probability of detecting a sync pulse showed that when the signal-to-noise ratio is equal to 10 and higher, the influence of noise pulses on the probability of detecting a sync pulse can be neglected. It has been noted that the greater the number of recorded events, or, in other words, the greater the sum of the average numbers of signal photons and dark current pulses, the greater the detection probability. The calculation of the probability of detecting a sync pulse using simplified expressions shows a slight deviation from calculations using exact formulas, which does not exceed 5,3%, and the calculation using approximate expressions gives an underestimated result. The resulting approximate analytical expressions can be used for express calculation of the probability of detecting a sync pulse in a pair of segments.

Quantum key distribution; synchronization; maximum total count; probabilistic characteristics.

Введение. Обеспечение стабильного и эффективного процесса квантового распределения ключей (КРК) невозможно без стабильной и точной работы подсистемы синхронизации, которая управляет временными настройками работы приёмопередающей и кодирующей станций системы КРК [1–21].

В [12–16] предложены и исследованы алгоритмы обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем. Недостаток алгоритма обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем состоит в том, что необходимо знать уровень фонового и шумового воздействия, который определяет пороговый уровень k_{th} и вероятность ошибочного обнаружения сигнальной пары сегментов $p_{th.b}$. Это требует адаптации порогового уровня к фактической мощности фонового и шумового воздействия.

Другим существенным недостатком алгоритма обнаружения на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем является большое среднее время, затрачиваемое на обнаружение синхроимпульса, при высоком уровне срабатываний $p_{th.b}$.

При использовании алгоритма, основанного на сравнении отсчётов (в противоположность тесту сравнения суммы отсчётов с пары сегментов с порогом), задание порога не требуется. Решение об обнаружении принимается после истечения фиксированного времени. Здесь вероятность обнаружения в паре сегментов определяется вероятностью того, что суммарное число фотонов в этой паре превышает отсчёты в остальных парах сегментов. Следовательно, здесь не требуется контроль (измерения) мощности фонового излучения и частоты генерации импульсов темнового тока (ИТТ).

В [3] предложено для расчёта вероятности обнаружения синхроимпульса использовать формулу для расчёта вероятности выделения слова при тестовой процедуре в M-ричной системе коммуникации с позиционно-импульсной модуляцией и блочным кодированием. В формуле производится замена счётного интервала на длительность пары сегментов при синхронизации и удваивается среднее число шумовых импульсов. Это позволило получить расчётные соотношения для вероятности обнаружения синхроимпульса для двух правил принятия решения.

Алгоритм обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом

Правило 1. В случае равенства максимальных отсчётов в двух парах сегментов в течение одного временного кадра в качестве сигнальной случайно выбирается одна из них.

Здесь вероятность отсутствия ошибки в течение одного временного кадра рассчитывается по формуле

$$p_{D1} = \frac{\exp(-\bar{n}_s - N_w \cdot \bar{k}_b)}{N_w} + \rightarrow$$

$$\rightarrow \sum_{k=1}^{\infty} \left\{ P_{OS}(k, \bar{k}_s) \left[\sum_{j=0}^{k-1} P_{OS}(j, \bar{k}_b) \right]^{N_w-1} \cdot \frac{1}{N_w} \cdot \frac{1}{P_{OS}(k, \bar{k}_b)} \right. \quad (1)$$

$$\left. \cdot \left[\sum_{j=0}^{k-1} P_{OS}(j, \bar{k}_b) \right] \left[\left(1 + \frac{P_{OS}(k, \bar{k}_b)}{\sum_{j=0}^{k-1} P_{OS}(j, \bar{k}_b)} \right)^{N_w} - 1 \right] \right\}.$$

Первый член учитывает случай, когда во всех парах сегментов фиксируются нулевые отсчёты (отсутствие фотонов). Второе слагаемое учитывает случай отсутствия равенства отсчётов, а также все случаи равенства отсчётов.

Правило 2. Равенство максимальных отсчётов в любых двух парах сегментов в течение одного временного кадра трактуется как ошибка обнаружения.

Следовательно, обнаружение импульса имеет место лишь тогда, когда отсчёт в одной из пар сегментов надёжно превышает значения отсчётов со всех других пар сегментов. В противном случае необходимо повторное обнаружение в следующем временном кадре.

Выражение для вероятности обнаружения синхроимпульса в течение временного кадра существенно упрощается [3]

$$p_{D1} = \sum_{k_1=1}^{\infty} \left\{ P_{OS}(k_1, \bar{k}_s) \cdot \left[\sum_{k_2=0}^{k_1-1} P_{OS}(k_2, \bar{k}_b) \right]^{N_w-1} \right\} = \quad (2)$$

$$= \sum_{k=1}^{\infty} \left\{ P_{OS}(k, \bar{k}_s) \cdot \left[\frac{\Gamma(k-1, \bar{k}_b)}{\Gamma(k-1)} \right]^{N_w-1} \right\}.$$

На рис. 1 приведены зависимости вероятности ошибочного обнаружения синхроимпульса в течение временного кадра от среднего числа сигнальных фотонов в синхроимпульсе \bar{n}_s для различного числа сегментов N_w при $\bar{n}_b=0,001$. Выбор числа сегментов N_w , кратным 2, обоснован цифровой реализацией блока управления. Выбор среднего числа шумовых импульсов $\bar{n}_b=0,001$ ориентирован на применение в волоконно-оптической системе фотодетектора с частотой генерации ИТТ 3,3 МГц при длительности оптического импульса 300 пс.

Вероятность ошибочного обнаружения синхроимпульса в течение кадра значительно уменьшается по мере роста среднего числа фотонов в синхроимпульсе. Так, если при $\bar{n}_s = 0,1$ и $N_w=8$ вероятность ошибки обнаружения синхроимпульса равна 0,90, то при $\bar{n}_s = 1$ она падает до 0,37, а при $\bar{n}_s = 5$ – уже до 0,01. При этом отметим слабое влияние числа пар сегментов на вероятность ошибочного обнаружения: при $\bar{n}_s = 2$ и увеличении N_w с 8 до 64 вероятность ошибки обнаружения незначительно меняется с 0,14 до 0,17. Последнее указывает на слабое влияние ИТТ на вероятностные характеристики анализируемой системы.

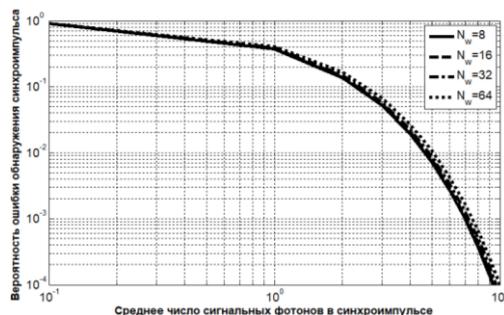


Рис. 1. Вероятности ошибочного обнаружения синхроимпульса в течение кадра при среднем числе ИТГ 0,001 за длительность сегмента в волоконно-оптической линии

Отметим, что лавинные фотодиоды (ЛФД), используемые в приёмной аппаратуре при КРК, имеют существенно меньший уровень шумов. Например, в случае применения однофотонного ЛФД с частотой ИТГ менее 100 Гц среднее число шумовых импульсов за длительность оптического импульса 300 пс не превышает $\bar{n}_b = 3 \cdot 10^{-10}$. Следовательно, в системах КРК можно полагать $\bar{k}_b \cong 0$. Тогда

$$p_{D1} = \sum_{k=1}^{\infty} \{Pos(k, \bar{k}_s) \cdot [1]^{N_w-1}\} = \sum_{k=1}^{\infty} Pos(k, \bar{k}_s) = 1 - Pos(k=0, \bar{k}_s) \quad (3)$$

$$= 1 - \exp(-\bar{k}_s) = 1 - \exp(-\bar{n}_s).$$

В системах КРК передаваемый квантовый импульс имеет среднее число фотонов в импульсе 0,1...0,5, а после распространения на 50 км будет ослаблен минимум в 10 раз до 0,01...0,05. Учитывая это, возможно использование приближённой формулы для экспресс-расчёта предельной вероятности обнаружения синхроимпульса в течение временного кадра

$$p_{D1} = 1 - \exp(-\bar{n}_s) = \bar{n}_s - \frac{\bar{n}_s^2}{2} + \frac{\bar{n}_s^3}{6}.$$

Погрешность не превышает 21 % при расчёте по формуле

$$p_{D1} \approx \bar{n}_s,$$

даже при $\bar{n}_s = 0,5$, падая до 5 % при $\bar{n}_s = 0,1$.

На рис. 2 представлены графики зависимостей вероятностей ошибки обнаружения синхроимпульса от среднего числа сигнальных фотонов в синхроимпульсе для атмосферной оптической системы при $\bar{n}_b=0,2$ для сравнения с предшествующим алгоритмом на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем [23].

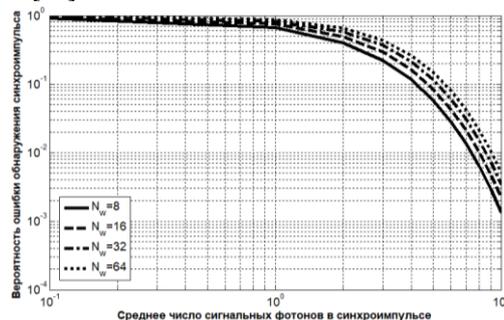


Рис. 2. Вероятности ошибочного обнаружения синхроимпульса в течение кадра при среднем числе фоновых фотонов 0,2 за длительность сегмента

Сравнительный анализ графиков показывает, что вероятность ошибочного обнаружения синхроимпульса в алгоритме на основе выбора смежной пары сегментов с максимальным суммарным отсчётом зависит от суммы средних чисел сигнальных и шумовых импульсов и числа сегментов в кадре, в то время как в предложенном ранее алгоритме обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем вероятность ошибочного обнаружения сигнальной пары сегментов зависит только от среднего числа шумовых импульсов.

Действительно при $\bar{n}_b=0,2$ вероятность ошибочного обнаружения 0,005 достигается при $N_w=8$ путём выбора порогового уровня $k_{th}=2$ (алгоритм обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем), либо путём увеличения среднего числа сигнальных фотонов в синхроимпульсе до $\bar{n}_s=8,5$ (алгоритм обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом).

Остановимся на ограничениях использования для расчёта вероятности обнаружения синхроимпульса формулы для расчёта вероятности выделения слова при тестовой процедуре в M-ричной системе коммуникации с позиционно-импульсной модуляцией и блочным кодированием. Приём сигналов с позиционно-импульсной модуляцией предполагает фиксацию временного интервала, внутри которого может присутствовать сигнальный импульс. Он не может одновременно принадлежать двум соседним временным интервалам. В противоположность этому в анализируемой системе КРК это возможно.

Обратимся к рис. 3. Временной кадр, равный по длительности периоду следования синхроимпульсов T_s , разбит на N_w временных сегментов с длительностью τ_w , равной длительности синхроимпульса τ_s . Как и ранее временные сегменты анализируются попарно (1, 2), (2, 3), ..., $(N_w - 1, N_w)$, $(N_w, 1)$. Пусть центр тяжести синхроимпульса располагается в i-м сегменте с левой стороны от его середины. При этом среднее число фотонов, регистрируемое в (i-1)-м и i-м сегментах, определим как \bar{n}_{s1} и \bar{n}_{s2} , причём всегда $\bar{n}_s = \bar{n}_{s1} + \bar{n}_{s2}$.

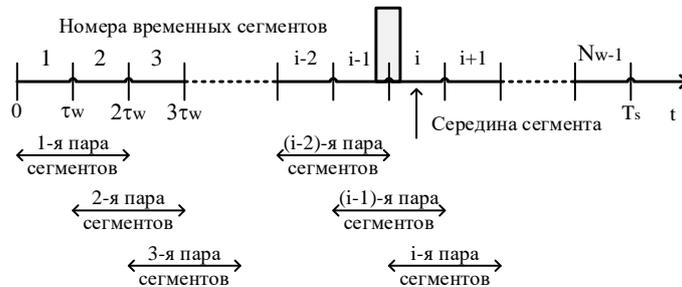


Рис. 3. Поиск максимального отсчёта в парах сегментов в течение временного кадра

Поскольку сигнальные фотоны могут приниматься в (i-1)-м и i-м сегментах, то обнаружение синхроимпульса может быть в (i-2)-й, (i-1)-й и i-й паре сегментов при условии, что отсчёт в одной из этих пар надёжно превышает отсчёты со всех других пар сегментов. В противном случае повторно анализируется следующий временной кадр.

Заметим, что среднее число событий, регистрируемых в (i-2)-й, (i-1)-й и i-й парах сегментов соответственно равны $\bar{k}_{s1} = \bar{n}_{s1} + 2 \cdot \bar{n}_b$, $\bar{k}_s = \bar{n}_s + 2 \cdot \bar{n}_b$ и $\bar{k}_{s2} = \bar{n}_{s2} + 2 \cdot \bar{n}_b$.

Выражение для вероятности обнаружения синхроимпульса в течение временного кадра складывается из трёх составляющих

$$p_{D1} = p_{D11} + p_{D12} + p_{D13}, \quad (4)$$

определяющих соответственно вероятности обнаружения синхроимпульса в (i-2)-й, (i-1)-й или i-й паре сегментов.

Если центр тяжести синхроимпульса располагается на границе между (i-1)-м и i-м сегментами, то

$$\bar{k}_{s1} = \bar{n}_s/2 + 2 \cdot \bar{n}_b, \quad \bar{k}_s = \bar{n}_s + 2 \cdot \bar{n}_b \quad \text{и} \quad \bar{k}_{s2} = \bar{n}_s/2 + 2 \cdot \bar{n}_b.$$

Тогда формулы упрощаются

$$p_{D11} = p_{D13} = \sum_{k_1=1}^{\infty} \left\{ P_{OS}(k_1, \bar{k}_{s1}) \left[\left(\sum_{k_2=0}^{k_1-1} P_{OS}(k_2, \bar{k}_b) \right)^{N_w-3} \left(\sum_{k_3=0}^{k_1-1} P_{OS}(k_3, \bar{k}_s) \right) \cdot \left(\sum_{k_4=0}^{k_1-1} P_{OS}(k_4, \bar{k}_{s2}) \right) \right] \right\}. \quad (5)$$

$$p_{D12} = \sum_{k_1=1}^{\infty} \left\{ P_{OS}(k_1, \bar{k}_s) \left[\left(\sum_{k_2=0}^{k_1-1} P_{OS}(k_2, \bar{k}_b) \right)^{N_w-3} \cdot \left(\sum_{k_3=0}^{k_1-1} P_{OS}(k_3, \bar{k}_{s1}) \right)^2 \right] \right\}. \quad (6)$$

На рисунке 4 представлены зависимости вероятности обнаружения синхроимпульса в паре сегментов от среднего числа сигнальных фотонов в синхроимпульсе при количестве временных сегментов $N_w=8$ и среднем числе ИТТ $\bar{n}_b = 10^{-7}$, что характерно для волоконно-оптической системы. Отметим, количество итераций при суммировании сокращено до $k_1 = 1 \dots 1000$ для увеличения быстродействия программы для расчёта указанных характеристик.

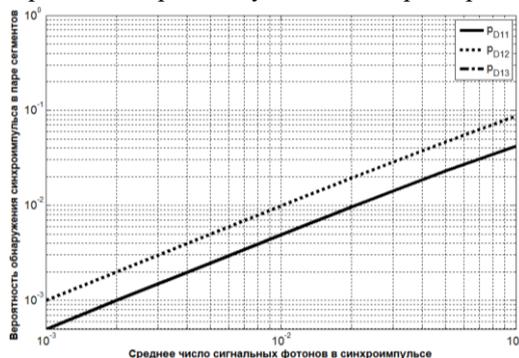


Рис. 4. Вероятность обнаружения синхроимпульса в паре сегментов

Из рисунка видно, увеличение вероятности обнаружения синхроимпульса в паре сегментов прямо пропорционально увеличению среднего числа сигнальных фотонов в синхроимпульсе. Так, при увеличении среднего числа сигнальных фотонов в синхроимпульсе в 100 раз (с 0,001 до 0,1) вероятность обнаружения синхроимпульса увеличивается в 84,2 раза (0,0005 против 0,0421) для (i-2)-й и i-й пар сегментов и в 86,5 раза (0,001 против 0,0865) для (i-1)-й пары сегментов. Также отметим, различие вероятности обнаружения синхроимпульса в (i-1)-й паре сегментов и вероятности обнаружения в (i-2)-й или i-й паре сегментов составляет ~ 2 раза.

Для волоконно-оптических систем КРК $\overline{k_s} \cong \overline{n_s}$, $\overline{k_{s1}} = \overline{k_{s2}} \cong \overline{n_s}/2 = \overline{k_s}/2$. и $(\exp(-\overline{k_b}))^{N_w-3} \cong \exp(-(N_w-3) \cdot \overline{k_b})$.

Учитывая, что для волоконно-оптических систем справедливо условие $\overline{n_s} < 1$, получим

$$p_{D11} = p_{D13} = \frac{\overline{k_s}}{2} \cdot \exp(-(N_w-3) \cdot \overline{k_b}) \cdot \exp(-2 \cdot \overline{k_s}), \quad (7)$$

$$p_{D12} = \overline{k_s} \cdot \exp(-(N_w-3) \cdot \overline{k_b}) \cdot \exp(-2 \cdot \overline{k_s}). \quad (8)$$

Откуда $p_{D12} = 2 \cdot p_{D11} = 2 \cdot p_{D13}$ и $p_{D12} = p_{D11} + p_{D13}$.

Наконец

$$p_{D1} = p_{D11} + p_{D12} + p_{D13} = 2 \cdot p_{D12}. \quad (9)$$

Действительно, как отмечено ранее, вероятность обнаружения синхроимпульса в (i-2)-й или i-й паре сегментов в 2 раза больше, чем вероятность обнаружения в (i-1)-й паре сегментов.

На рис. 5 представлены зависимости вероятности обнаружения синхроимпульса в паре сегментов от среднего числа сигнальных фотонов в синхроимпульсе при количестве временных сегментов $N_w=8$ и среднем числе ИТТ за длительность сегмента $\overline{n_b} = 10^{-7}$, полученные по упрощённым выражениям.

Расчёт вероятности обнаружения синхроимпульса по упрощённым выражениям показывает незначительное отклонение от точных расчётов, которое составляет не более 5,3 %, причём расчёт по приближённым выражениям даёт заниженный результат. Таким образом, полученные приближённые аналитические выражения могут применяться для экспресс-расчёта вероятности обнаружения синхроимпульса в паре сегментов.

На рис. 6 представлены результаты расчёта по точным выражениям (5)-(6) вероятности обнаружения синхроимпульса в (i-1)-й паре сегментов p_{D12} при различных значениях среднего числа ИТТ $\overline{n_b}$ за длительность сегмента от среднего числа сигнальных фотонов в синхроимпульсе $\overline{n_s}$ при количестве временных сегментов $N_w=8$.

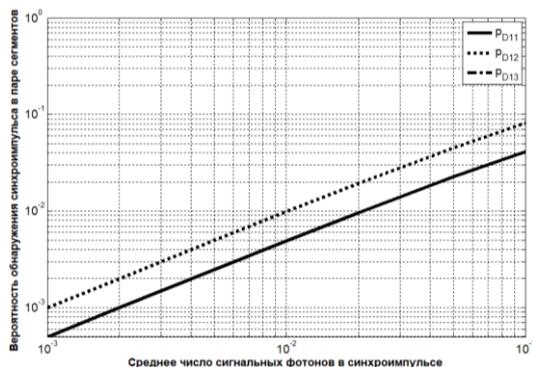


Рис. 5. Вероятность обнаружения синхроимпульса в паре сегментов (экспресс-расчёт)

При $\overline{n_b} \leq 10^{-5}$ различие в вероятности обнаружения синхроимпульса стремится к 0 при различных средних числах сигнальных фотонов в синхроимпульсе, следовательно, при $\overline{n_b} \leq 10^{-5}$ влиянием ИТТ на вероятность обнаружения синхроимпульса можно пренебречь. Однако при $\overline{n_b} \geq 10^{-4}$ влияние ИТТ на вероятность обнаружения синхроимпульса значительно увеличивается, что обусловлено соизмеримостью средних чисел сигнальных фотонов и ИТТ.

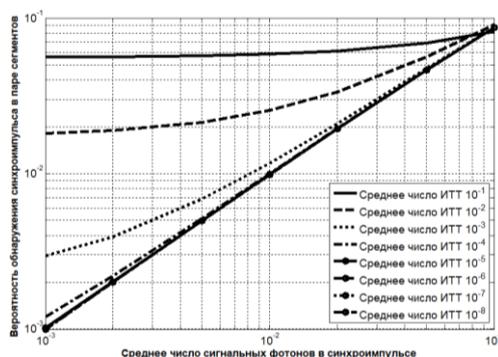


Рис. 6. Вероятность обнаружения синхрои́мпульса в сигнальной (i-1)-й паре сегментов (точный расчёт)

Отметим, чем меньше \bar{n}_b , тем быстрее возрастает вероятность обнаружения синхрои́мпульса. Так, при $\bar{n}_b = 0,1$ различие в вероятности обнаружения составляет 1,46 раза при увеличении \bar{n}_s от 0,001 до 0,1. При уменьшении среднего числа ИТТ до $\bar{n}_b = 10^{-8}$ различие в вероятности обнаружения составляет уже 86,5 раза при увеличении \bar{n}_s от 0,001 до 0,1.

Графики на рисунке 6 показывают, что влиянием шумовых импульсов на вероятность обнаружения синхрои́мпульса можно пренебречь уже при отношении $SNR = \bar{n}_s/\bar{n}_b > 10$.

Учитывая, что вероятность обнаружения синхрои́мпульса в (i-1)-й паре сегментов при расчёте по точным аналитическим выражениям зависит от суммы средних чисел сигнальных фотонов и ИТТ, вероятность обнаружения будет тем больше, чем больше число регистрируемых событий, или, другими словами, чем больше сумма средних чисел сигнальных фотонов и ИТТ, что и подтверждают графики на рис. 6.

На рис. 7 представлены результаты экспресс-расчёта по (7)-(8) вероятности обнаружения синхрои́мпульса в (i-1)-й паре сегментов p_{D12} при количестве временных сегментов $N_w=8$ и различных значениях среднего числа ИТТ \bar{n}_b за длительность сегмента от среднего числа сигнальных фотонов в синхрои́мпульсе \bar{n}_s .

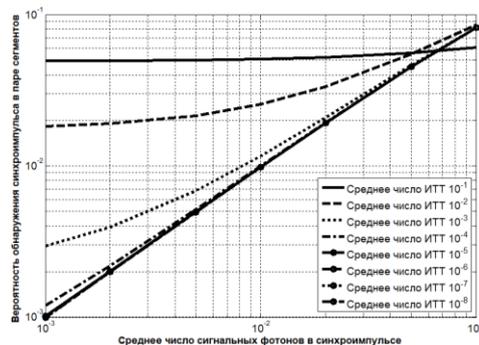


Рис. 7. Вероятность обнаружения синхрои́мпульса в сигнальной (i-1)-й паре сегментов (экспресс-расчёт)

Проводя сравнительный анализ полученных результатов при расчёте по точным выражениям и экспресс-расчёте, отклонение вероятности обнаружения синхрои́мпульса при реализации алгоритма на основе ЛФД со средним числом ИТТ $\bar{n}_b = 10^{-7}$ составляет не более 5,6%.

Выводы. Предложен алгоритм обнаружения синхросигнала подсистемы синхронизации приёмопередающей и кодирующей станций КРК, отличительной особенностью которого является обнаружение синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом. Преимуществом указанного алгоритма, по сравнению с ранее предложенным алгоритмом обнаружения синхросигнала на основе сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем, является отсутствие необходимости знания уровня фоновое и шумового воздействия, определяющего пороговый уровень и вероятность ошибочного обнаружения сигнальной пары сегментов в предшествующем алгоритме, что значительно упрощает и сокращает время подготовительного этапа перед процессом синхронизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Lindsey W.C.* Synchronization Systems in Communication and Control. – Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
2. *Стиффлер Дж.* Теория синхронной связи: пер. с англ. / под ред. Э.М. Габидулина. – М.: Связь, 1975.
3. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.
4. *Витерби А.Д., Омура Дж.К.* Принципы цифровой связи и кодирования: пер. с англ. / под ред. К.Ш. Зигангирова. – М.: Радио и связь, 1982. – 536 с.
5. *Yilong Geng, Shiyu Liu, and Zi Yin.* Exploiting a Natural Network Effect for Scalable, Fine-grained Clock Synchronization // NSDI'18: Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation. – 2018. – P. 81-94.
6. *Govindan Kannan Pravein., Joshi Raj., Chan Mun Choon.* Precise Time-synchronization in the Data-Plane Using Programmable Switching ASICs // Proceedings of the 2019 ACM Symposium on SDN Research, ACM. – 2019. – P. 8-20. – DOI: 10.1145/3314148.3314353.
7. *Румянцев К.Е.* Системы квантового распределения ключа: монография. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 264 с.
8. *Румянцев К.Е.* Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 2. – С. 32-40.
9. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.
10. *Plenkin A., Rumyantsev K., Rudinsky E.* Comparative analysis of single-photon synchronization algorithms in the quantum key distribution system // Proceedings of IEEE East-West Design & Test Symposium (EWDTS). – 2017. – P. 1-5. – DOI: 10.1109/EWDTS.2017.8110047.
11. *Rumyantsev K.E., Rudinsky E.A.* Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions // Proceedings of the 2nd International Conference on Multimedia and Image Processing (ICMIP). – 2017. – P. 346-349. – DOI: 10.1109/ICMIP.2017.68.
12. *Mironov Y.K., Mironova P.D., Rumyantsev K.E.* 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 // IOP Conf. Series: Materials Science and Engineering, 1069. – 2021. – Paper 012011. – P. 1-8. – DOI: 10.1088/1757-899X/1069/1/012011.
13. *Mironov Y., Mironova P., Rumyantsev K.* 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 // ACM International Conference Proceeding Series. – 2020. – Paper №3433596. – P. 1-5. – DOI: 10.1145/3433174.3433595.
14. *Mironov Y.K., Mironova P.D., Rumyantsev K.E.* 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 // E3S Web of Conferences. – 2020. – Vol. 224. – P. 1-9. – DOI: 10.1051/e3sconf/202022401032.
15. *Mironov Y.K., Rumyantsev K.E.* 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. – 2020. – P. 87-97. – DOI: https://doi.org/10.1007/978-981-15-4451-4_8.

16. *Rumyantsev K.Y., Vamatgireeva K.B., Mironov Y.K.* Single Photon Algorithm of Search of a Pulse Radiation Source // *Communications in Computer and Information Science*. – 2019. – 958. – P. 95-108. – DOI: 10.1007/978-981-13-3804-5_8.
17. *Курочкин В.Л. и др.* Экспериментальные исследования в области квантовой криптографии // *Фотоника*. – 2012. – Т. 5. – С. 54-66.
18. *Румянцев К.Е., Плёткин А.П.* Безопасность режима синхронизации системы квантового распределения ключей // *Известия ЮФУ. Технические науки*. – 2015. – № 5 (166). – С. 135-153.
19. *Миронов Я.К.* Моделирование этапа тестирования двухэтапного временного алгоритма синхронизации при нахождении однофотонного источника излучения в сигнальном участке ВОЛС // *Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: материалы VIII Всероссийской научно-технической конференции*. – 2022. – С. 19-21.
20. *Mironov Y.K., Rumyantsev K.E.* Providing the Required Probability of Synchronization Error When Splitting a Fiber-Optic Line into Sections with Decreasing Length in a Quantum Key Distribution System // *Proceedings - 2021 3rd International Conference on System Reliability and Safety Engineering, SRSE 2021*. – 2021. – P. 145-149. – DOI: 10.1109/SRSE54209.2021.00032.
21. *Миронов Я.К.* Синхронизация станций системы квантового распределения ключа с последовательным опросом участков волоконно-оптической линии с убывающей длиной // *Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Матер. VII Всероссийской научно-технической конференции*. – 2021. – С. 109-112.
22. *Миронов Я.К., Миронова П.Д., Румянцев К.Е.* Вероятностные характеристики порогового алгоритма обнаружения синхроимпульсов в системе квантового распределения ключа на основе информации со смежной пары временных сегментов // *Известия ЮФУ. Технические науки*. – 2020. – № 4 (207). – С. 221-229.
23. *Миронов Я.К., Миронова П.Д., Румянцев К.Е.* Исследование характеристик алгоритма синхронизации системы квантового распределения ключа на основе сравнения числа отсчетов со смежной пары временных окон с пороговым уровнем // *Сб. докладов II Всероссийской научной конференции (с приглашением зарубежных ученых)*. – 2020. – С. 219-226.
24. *Миронова П.Д.* Синхронизация станций системы квантового распределения ключа на основе порогового теста для отсчетов со смежной пары временных сегментов // *Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Матер. VII Всероссийской научно-технической конференции*. – 2021. – С. 107-109.
25. *Миронова П.Д.* Алгоритм синхронизации станций системы квантового распределения ключа на основе порогового теста для отсчетов со смежной пары временных сегментов с учетом дисперсионных и поляризационных свойств ВОЛС // *Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Матер. VIII Всероссийской научно-технической конференции*. – 2022. – С. 22-25.
26. *Rumyantsev K.E., Lnenko P.D., Shakir H.H.-Sh.* Evaluation of the Influence of the Dispersion Properties of a Fiber-Optic Line on the Efficiency of an Algorithm for Single-Photon Synchronization of Quantum Key Distribution System // *Conference Proceedings - 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019*. – 2019. – P. 392-395. – DOI: 10.1109/RSEMW.2019.8792769.

REFERENCES

1. *Lindsey W.C.* Synchronization Systems in Communication and Control. Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
2. *Stiffler Dzh.* Teoriya sinkhronnoy svyazi [Synchronous communication theory]: transl. from engl., ed. by E.M. Gabidulina. Moscow: Svyaz', 1975.
3. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communication]: transl. from engl., ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.
4. *Viterbi A.D., Omura Dzh.K.* Printsipy tsifrovoy svyazi i kodirovaniya [Principles of digital communication and coding]: transl. from engl., ed. by K.Sh. Zigangirova. Moscow: Radio i svyaz', 1982, 536 p.
5. *Yilong Geng, Shiyu Liu, and Zi Yin.* Exploiting a Natural Network Effect for Scalable, Fine-grained Clock Synchronization, *NSDI'18: Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation*, 2018, pp. 81-94.

6. Govindan Kannan Pravein., Joshi Raj., Chan Mun Choon. Precise Time-synchronization in the Data-Plane Using Programmable Switching ASICs, *Proceedings of the 2019 ACM Symposium on SDN Research, ACM*, 2019, pp. 8-20. DOI: 10.1145/3314148.3314353.
7. Rumyantsev K.E. Sistemy kvantovogo raspredeleniya klyucha: monografiya [Systems of quantum key distribution: monograph]. Taganrog: Izd-vo TTI YuFU, 2011, 264 p.
8. Rumyantsev K.E. Sinkhronizatsiya v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Synchronization in a quantum key distribution system with automatic compensation of polarization distortions], *Telekommunikatsii* [Telecommunications], 2017, No. 2, pp. 32-40.
9. Rumyantsev K.E., Plenkin A.P. Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Synchronization of the system of quantum key distribution when using photon pulses to increase security], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8, pp. 81-96.
10. Plenkin A., Rumyantsev K., Rudinsky E. Comparative analysis of single-photon synchronization algorithms in the quantum key distribution system, *Proceedings of IEEE East-West Design & Test Symposium (EWDTS)*, 2017, pp. 1-5. DOI: 10.1109/EWDTS.2017.8110047.
11. Rumyantsev K.E., Rudinsky E.A. Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions, *Proceedings of the 2nd International Conference on Multimedia and Image Processing (ICMIP)*, 2017, pp. 346-349. DOI: 10.1109/ICMIP.2017.68.
12. Mironov Y.K., Mironova P.D., Rumyantsev K.E. 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, *IOP Conf. Series: Materials Science and Engineering*, 1069, 2021, Paper 012011, pp. 1-8. DOI: 10.1088/1757-899X/1069/1/012011.
13. Mironov Y., Mironova P., Rumyantsev K. 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, *ACM International Conference Proceeding Series*, 2020, Paper No. 3433596, pp. 1-5. DOI: 10.1145/3433174.3433595.
14. Mironov Y.K., Mironova P.D., Rumyantsev K.E. 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, *E3S Web of Conferences*, 2020, Vol. 224, pp. 1-9. DOI: 10.1051/e3sconf/202022401032.
15. Mironov Y.K., Rumyantsev K.E. 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*, 2020, pp. 87-97. DOI: https://doi.org/10.1007/978-981-15-4451-4_8.
16. Rumyantsev K.Y., Bamatgireeva K.B., Mironov Y.K. Single Photon Algorithm of Search of a Pulse Radiation Source, *Communications in Computer and Information Science*, 2019, 958, pp. 95-108. DOI: 10.1007/978-981-13-3804-5_8.
17. Kurochkin V.L. i dr. Eksperimental'nye issledovaniya v oblasti kvantovoy kriptografii [Experimental research in the field of quantum cryptography], *Fotonika* [Photonics], 2012, Vol. 5, pp. 54-66.
18. Rumyantsev K.E., Plenkin A.P. Bezopasnost' rezhima sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey // *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 135-153.
19. Mironov Ya.K. Modelirovanie etapa testirovaniya dvukhetapnogo vremennogo algoritma sinkhronizatsii pri nakhozhenii odnofotonnogo istochnika izlucheniya v signal'nom uchastke VOLS [Simulation of the testing stage of a two-stage time synchronization algorithm when a single-photon radiation source is in the signal section of the FOCL], *Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti: materialy VIII Vserossiyskoy nauchno-tekhnikeskoy konferentsii* [Fundamental and Applied Aspects of Computer Technologies and Information Security: Proceedings of the VIII All-Russian Scientific and Technical Conference], 2022, pp. 19-21.
20. Mironov Y.K., Rumyantsev K.E. Providing the Required Probability of Synchronization Error When Splitting a Fiber-Optic Line into Sections with Decreasing Length in a Quantum Key Distribution System, *Proceedings - 2021 3rd International Conference on System Reliability and Safety Engineering, SRSE 2021*, 2021, pp. 145-149. DOI: 10.1109/SRSE54209.2021.00032.

21. *Mironov Ya.K.* Sinkhronizatsiya stantsiy sistemy kvantovogo raspredeleniya klyucha s posledovatel'nyim oprosom uchastkov volokonno-opticheskoy linii s ubyvyayushchey dlinoi [Synchronization of stations of the quantum key distribution system with sequential polling of sections of a fiber-optic line with decreasing length], *Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti: Mater. VII Vserossiyskoy nauchno-tekhnicheskoy konferentsii* [Fundamental and applied aspects of computer technology and information security: materials of the VII All-Russian Scientific and Technical Conference], 2021, pp. 109-112.
22. *Mironov Ya.K., Mironova P.D., Rumyantsev K.E.* Veroyatnostnye kharakteristiki porogovogo algoritma obnaruzheniya sinkhroimpul'sov v sisteme kvantovogo raspredeleniya klyucha na osnove informatsii so smezhnoy pary vremennykh segmentov [Probabilistic Characteristics of a Threshold Sync Detection Algorithm in a Quantum Key Distribution System Based on Information from an Adjacent Pair of Time Segments], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 4 (207), pp. 221-229.
23. *Mironov Ya.K., Mironova P.D., Rumyantsev K.E.* Issledovanie kharakteristik algoritma sinkhronizatsii sistemy kvantovogo raspredeleniya klyucha na osnove sravneniya chisla otschetov so smezhnoy pary vremennykh okon s porogovym urovnem [Investigation of the characteristics of the synchronization algorithm of the quantum key distribution system based on the comparison of the number of samples from an adjacent pair of time windows with a threshold level], *Sb. dokladov II Vse-rossiyskoy nauchnoy konferentsii (s priglazheniem zarubezhnykh uchenykh)* [Collection of reports of the II All-Russian scientific conference (with the invitation of foreign scientists)], 2020, pp. 219-226.
24. *Mironova P.D.* Sinkhronizatsiya stantsiy sistemy kvantovogo raspredeleniya klyucha na osnove porogovogo testa dlya otschetov so smezhnoy pary vremennykh segmentov [Synchronization of stations of the quantum key distribution system based on a threshold test for readings from an adjacent pair of time segments], *Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti: Mater. VII Vserossiyskoy nauchno-tekhnicheskoy konferentsii* [Fundamental and applied aspects of computer technology and information security: materials of the VII All-Russian Scientific and Technical Conference], 2021, pp. 107-109.
25. *Mironova P.D.* Algoritm sinkhronizatsii stantsiy sistemy kvantovogo raspredeleniya klyucha na osnove porogovogo testa dlya otschetov so smezhnoy pary vremennykh segmentov s uchetom dispersionnykh i polarizatsionnykh svoystv VOLS [Synchronization algorithm for stations of a quantum key distribution system based on a threshold test for readings from an adjacent pair of time segments, taking into account the dispersion and polarization properties of FOCL], *Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti: Mater. VIII Vserossiyskoy nauchno-tekhnicheskoy konferentsii* [Fundamental and applied aspects of computer technology and information security: materials of the VIII All-Russian Scientific and Technical Conference], 2022, pp. 22-25.
26. *Rumyantsev K.E., Lnenko P.D., Shakir H.H.-Sh.* Evaluation of the Influence of the Dispersion Properties of a Fiber-Optic Line on the Efficiency of an Algorithm for Single-Photon Synchronization of Quantum Key Distribution System, *Conference Proceedings - 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019*, 2019, pp. 392-395. DOI: 10.1109/RSEMW.2019.8792769.

Статью рекомендовала к опубликованию к.т.н., доцент Л.А. Албогачиева.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; г. Таганрог, Россия; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Миронова Полина Демьяновна – e-mail: lnenkopdem@gmail.com; тел.: 89081924053; кафедра информационной безопасности телекоммуникационных систем; ассистент; аспирант.

Rumyantsev Konstantin Evgenievich – Southern Federal University; e-mail: rke2004@mail.ru; Taganrog, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Mironova Polina Demyanovna – e-mail: lnenkopdem@gmail.com; phone: +79081924053; the department of information security of telecommunication systems; assistant; graduate student.