

К.Е. Румянцев, Я.К. Миронов, П.Д. Миронова

**ОЦЕНКА ХАРАКТЕРИСТИК ДВУХЭТАПНОГО АЛГОРИТМА
СИНХРОНИЗАЦИИ НА ОСНОВЕ ВЫБОРА СМЕЖНОЙ ПАРЫ СЕГМЕНТОВ
С МАКСИМАЛЬНЫМ СУММАРНЫМ ОТСЧЁТОМ В СИСТЕМЕ КРК**

Предложен двухэтапный алгоритм синхронизации на основе выбора смежной пары сегментов с максимальным суммарным отсчётом в системе КРК. В основе алгоритма известный подход к уменьшению времени вхождения в синхронизм – анализ смежных пар временных сегментов. Отличительной особенностью предложенного алгоритма является обеспечение вероятности успешного поиска и тестирования не хуже требуемого уровня. Необходимо отметить, благодаря этапу тестирования производится отбраковка ошибочных решений, принятых на этапе поиска, что позволяет минимизировать вероятность ложной синхронизации вследствие регистрации шумовых импульсов. На этапе поиска аппаратура последовательно регистрирует суммарные отсчёты со всех смежных пар сегментов. Далее выбирается пара сегментов с максимальным суммарным отсчётом, причём отсчёт в одной из пар сегментов надёжно превышает значения отсчётов со всех других пар сегментов, и аппаратура переходит к этапу тестирования. Тестирование состоит в опросе фотодетектора в течение импульса стробирования для повторной регистрации отсчёта. В случае положительного тестирования процесс «грубой» оценки момента приёма синхроимпульса считается успешно завершённым, в противном случае – аппаратура возвращается к поиску в следующем кадре. Отметим, этапам поиска и тестирования соответствуют предельно допустимые числа кадров и тестов соответственно. Получены аналитические выражения для расчёта временных и вероятностных характеристик этапов поиска и тестирования предложенного алгоритма обнаружения на основе выбора смежной пары сегментов с максимальным суммарным отсчётом, в том числе для расчёта допустимого числа кадров и тестов при обеспечении требуемых вероятностей успешного поиска и тестирования соответственно. Установлено, при увеличении среднего числа фотонов в синхроимпульсе средние числа кадров и тестов, а также среднее время успешного поиска и тестирования значительно снижаются. Например, при увеличении среднего числа фотонов в синхроимпульсе в 5 раз среднее число тестов для успешного тестирования и среднее время успешного тестирования уменьшаются в 1,5 раза, а допустимое число тестов – в 5 раз.

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

K.Ye. Rumyantsev, Ya.K. Mironov, P.D. Mironova

**EVALUATION OF THE CHARACTERISTICS OF A TWO-STAGE
SYNCHRONIZATION ALGORITHM BASED ON THE SELECTION
OF AN ADJACENT PAIR OF SEGMENTS WITH THE MAXIMUM TOTAL COUNT
IN THE QKD SYSTEM**

A two-stage synchronization algorithm is proposed based on the selection of an adjacent pair of segments with the maximum total count in the QKD system. The algorithm is based on a well-known approach to reducing the time of entering into synchronism - the analysis of adjacent pairs of time segments. A distinctive feature of the proposed algorithm is to ensure that the probability of successful search and testing is not worse than the required level. It should be noted that due to the testing stage, erroneous decisions made at the search stage are rejected, which minimizes the probability of false synchronization due to the registration of noise pulses. At the search stage, the equipment sequentially registers the total counts from all adjacent pairs of segments. Next, a pair of segments with the maximum total count is selected, and the count in one of the pairs of segments reliably exceeds the values of the counts from all other pairs of segments, and the equipment proceeds to the testing stage. Testing consists of polling the photodetector during the gating pulse to re-register the count. In case of positive testing, the process of «rough» estimation of the moment of reception of the sync pulse is considered successfully completed, otherwise the equipment returns to the search in the next frame. Note that the maximum allowable number of frames and tests correspond to the search and testing stages, respectively. Analytical expressions are obtained for calculating the time and probabilistic characteristics of the search and testing stages of the proposed detection algorithm based on the selection of an adjacent pair of segments with the maximum total count, including for calculating the allowable number of frames and tests while ensuring the required

probabilities of successful search and testing, respectively. It has been found that with an increase in the average number of photons in the sync pulse, the average number of frames and tests, as well as the average time of successful search and testing, decrease significantly. For example, when the average number of photons in a sync pulse increases by 5 times, the average number of tests for successful testing and the average time for successful testing decrease by 1.5 times, and the permissible number of tests by 5 times.

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

Введение. Применение систем квантового распределения ключа (КРК) позволяет обеспечить абсолютную безопасность передаваемых данных между легитимными пользователями. В общем случае система КРК состоит из приёмопередающей и кодирующей станций, генерирующих секретный ключ посредством квантового канала, а также подсистемы синхронизации. Эффективное КРК невозможно без стабильной и точной синхронизации станций [1–6]. Известные исследования подсистем синхронизации в системах КРК направлены на повышение безопасности процесса синхронизации, увеличение протяжённости линии связи и быстродействия [7–17]. Однако обеспечение секретности процесса синхронизации накладывает значительные ограничения на дальность связи и время вхождения в синхронизм.

Известен подход к снижению времени синхронизации приёмопередающей и кодирующей станций системы КРК, заключающийся в анализе смежных пар сегментов, причём длительность одного временного сегмента равна длительности синхроимпульса [17]. В указанном подходе принятие решения об обнаружении синхроимпульса осуществляется посредством сравнения суммы отсчётов со смежной пары сегментов с пороговым уровнем, либо путём поиска смежной пары сегментов с максимальным суммарным отсчётом.

Предлагается алгоритм «грубой» оценки момента приёма синхросигнала, предполагающий поиск номера сигнальной смежной пары сегментов, на основе поиска смежной пары сегментов с максимальным суммарным отсчётом с добавлением этапа тестирования для отбраковки ошибочных решений на этапе поиска. Отличительной особенностью данного алгоритма является сравнение суммарного отсчёта со смежной пары сегментов не с пороговым уровнем, как в алгоритме аналоге [18, 19], а с отсчётами с других смежных пар сегментов и выбор пары сегментов с максимальным отсчётом. Данная особенность позволяет упростить поиск сигнальной смежной пары сегментов, исключая необходимость расчёта и выбора порогового уровня.

Оценка временных и вероятностных характеристик этапов поиска и тестирования двухэтапного алгоритма синхронизации на основе выбора смежной пары сегментов с максимальным суммарным отсчётом. Алгоритм предполагает оценку момента приёма синхроимпульса посредством двух последовательных этапов. Временной интервал, равный периоду следования синхроимпульсов T_s , делится на N_w временных сегментов, причём длительность одного временного сегмента равна длительности синхроимпульса $\tau_w = \tau_s$, поэтому анализ сегментов проводится попарно ввиду возможного нахождения синхроимпульса на границе двух смежных сегментов.

На рис. 1 представлена операция «грубой» оценки момента приёма синхроимпульса в 1-м временном кадре. Цель «грубой» оценки заключается в поиске сигнальной смежной пары сегментов. Операция подразделяется на два этапа – поиск и тестирование. На этапе поиска аппаратура последовательно, начиная с 1-й пары смежных сегментов, регистрирует суммарный отсчёт с каждой пары сегментов. После анализа всех пар сегментов в кадре выбирается пара сегментов с максимальным суммарным отсчётом, причём отсчёт в одной из пар сегментов надёжно превышает значения отсчётов со всех других пар сегментов. Далее аппаратура переходит на этап тестирования, задача которого состоит в опросе фотодетектора в течение импульса стробирования для повторной регистрации отсчёта. В случае повторной регистрации (превышения суммарным отсчётом порогового уровня) этап тестирования завершается, аппаратура переходит к «точной» оценке (выход 2 на рис. 1). В случае отрицательного тестирования аппаратура возвращается к поиску в следующем кадре (выход 1 на рис. 1). При отсутствии обнаружения синхроимпульса в течение анализа всех смежных пар сегментов в кадре аппаратура переходит к поиску в следующем кадре (выход 1 на рис. 1). Отметим, этапам поиска и тестирования соответ-

вуют предельно допустимые числа кадров $N_{T,2}$ и тестов $N_{test,2}$ соответственно. При отсутствии обнаружения синхроимпульса в течение допустимого числа кадров $N_{T,2}$ процесс синхронизации начинается с начала.

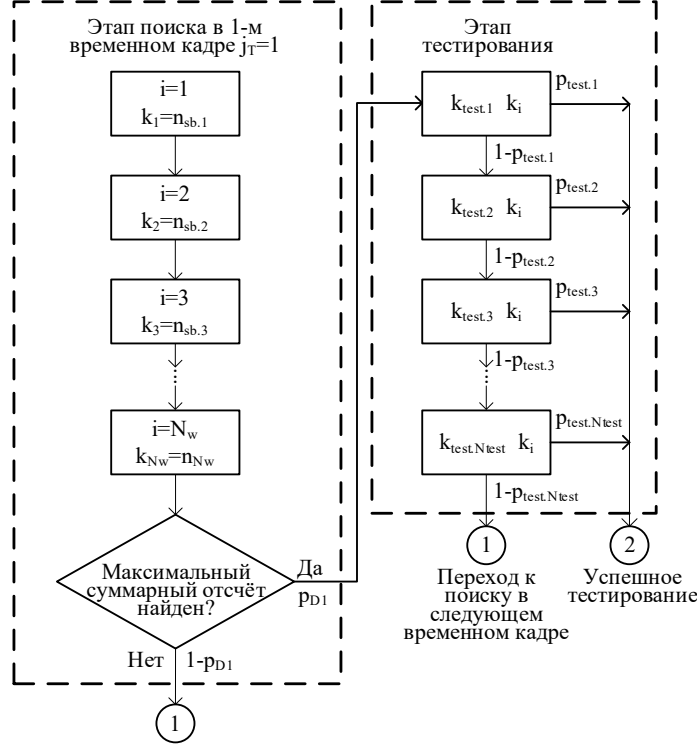


Рис. 1. Операция «грубой» оценки момента приёма синхроимпульса в 1-м кадре на основе выбора смежной пары сегментов с максимальным суммарным отсчётом

Определим допустимые числа кадров и тестов. Вероятность обнаружения синхроимпульса на этапе поиска в кадре может быть найдена по формуле [20]

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

где $\bar{k}_s = \bar{n}_s + \bar{k}_b = \bar{n}_s + 2\bar{n}_b$ – сумма сигнальных и шумовых импульсов в анализируемой смежной паре сегментов.

Используя метод математической индукции, находим условную вероятность обнаружения синхроимпульса в j_T -м временном кадре

$$p_{D,2}\{j_T\} = (1 - p_{D1,2})^{j_T-1} \cdot p_{D1,2}.$$

Используя свойства геометрической прогрессии, безусловная вероятность обнаружения синхроимпульса на этапе поиска с числом кадров $N_{T,2}$ равна

$$P_{D,2} = \sum_{j_T=1}^{N_{T,2}} p_{D,2}\{j_T\} = 1 - (1 - p_{D1,2})^{N_{T,2}}.$$

Таким образом, для обеспечения заданной вероятности обнаружения $P_{D,2}$ при известной вероятности $p_{D1,2}$ потребуется анализ не менее $N_{T,2,min}$ кадров

$$N_{T,2} \geq N_{T,2,min} = \left\lceil \frac{\lg(1 - P_{D,2})}{\lg(1 - p_{D1,2})} \right\rceil.$$

Учитывая, что для принятия решения аппаратурой о результате поиска необходимо проанализировать все смежные пары сегментов во временном кадре, то время, затраченное на этапе поиска в текущем кадре, будет равно $t_{search.j_T} = T_s$.

Среднее число кадров для успешного обнаружения на этапе поиска

$$\overline{N_{T.2}} = \sum_{j_T=1}^{N_{T.2}} j_T \cdot (1 - p_{D1.2})^{j_T-1} \cdot p_{D1.2}$$

определяет среднее время $\overline{T_{search.2}} = T_s \cdot \overline{N_{T.2}}$.

Результаты расчёта характеристик этапа поиска в предлагаемом алгоритме представлены в табл. 1. Обеспечиваемые вероятности обнаружения на этапах поиска и тестирования равны $P_{D.2} \geq 0,99$ и $P_{test.2} \geq 0,99$. Протяжённость волоконно-оптической линии связи (ВОЛС) составляет 20 км, что соответствует периоду следования $T_s = 195,76$ мкс. Следовательно, число сегментов и смежных пар сегментов равно $N_w = 652553$. При ориентации на отклонение в $K_{pD1}=1,1$ раза от предельной вероятности синхронизации $p_{D1.lim2}$ и частоте генерации импульсов темнового тока (ИТТ) $f_{DCR} = 10$ Гц пороговый уровень равен $k_{th} = 1$. Отметим, по методике расчёта порогового уровня реально достижимая вероятность ложного срабатывания при ориентации на $k_{th} = 1$ составляет $p_{th.b} = 6 \cdot 10^{-9}$.

Обеспечение вероятности успешного обнаружения на этапе поиска $P_{D.2} \geq 0,99$ достигается за счёт последовательного анализа смежных пар сегментов в течение допустимого числа кадров $N_{T.2}$. Полученные результаты указывают на значительное снижение числа кадров $N_{T.2}$ при увеличении среднего числа фотонов в синхроимпульсе $\overline{n_s}$. Так, при $\overline{n_s} = 1$ для достижения $P_{D.2} \geq 0,99$ потребуется 5 кадров, при $\overline{n_s} = 2 - 3$ кадра, а при $\overline{n_s} \geq 5$ – всего 1 кадр. В целом увеличение среднего числа фотонов в синхроимпульсе в 5 раз (с 1 до 5) позволяет снизить допустимое число кадров также в 5 раз (с 5 до 1). Значительное снижение числа кадров по мере роста $\overline{n_s}$ обусловлено увеличением отношения среднего числа фотонов в синхроимпульсе к среднему числу шумовых импульсов за длительность пары сегментов $\overline{n_s}/(2\overline{n_b})$, и, следовательно, повышением вероятности обнаружения синхроимпульса в кадре $p_{D1.2}$. Соответственно, с ростом среднего числа фотонов $\overline{n_s}$ в связи со значительным снижением допустимого $N_{T.2}$ и среднего $\overline{N_{T.2}}$ чисел кадров уменьшается также и среднее время успешного поиска $\overline{T_{search.2}}$. Среднее время $\overline{T_{search.2}}$ достигает максимального значения при $\overline{n_s} = 1$ и составляет $\overline{T_{search.2}}=301,54$ мкс. Однако при $\overline{n_s} \geq 3$ скорость изменения среднего времени успешного поиска снижается и стремится к 0. Увеличение среднего числа фотонов в синхроимпульсе с 1 до 2 позволяет уменьшить среднее время успешного поиска на 25,5% (301,54 против 224,61 мкс), при увеличении среднего числа фотонов с 2 до 3 – на 8,9% (224,61 против 204,63 мкс), а при увеличении среднего числа фотонов с 3 до 4 различие составляет всего 2,6% (204,63 против 199,27 мкс).

Таблица 1

Результаты расчёта параметров этапа поиска

$\overline{n_s}$	Среднее число фотонов в синхроимпульсе				
	1	2	3	4	5
$100p_{D1.2}$	63,07	86,36	94,96	98,14	99,31
$N_{T.2}$	5	3	2	2	1
$\overline{N_{T.2}}$	1,540	1,147	1,045	1,018	0,993
$\overline{T_{search.2}}$, мкс	301,54	224,61	204,63	199,27	194,42
$\overline{n_s}$	Среднее число фотонов в синхроимпульсе				
	6	7	8	9	10
$100p_{D1.2}$	99,75	99,91	99,97	99,99	100,00
$N_{T.2}$	1	1	1	1	1
$\overline{N_{T.2}}$	0,997	0,999	1,00	1,00	1,00
$\overline{T_{search.2}}$, мкс	195,26	195,58	195,69	195,73	195,75

При переходе аппаратуры на этап тестирования повторный опрос фотодетектора производится в течение допустимого числа тестов $N_{test.2}$, пока не произойдет превышения суммарным отсчётом со смежной пары сегментов порогового уровня или не закончится допустимое число тестов. Длительность стробирующего импульса определяется удвоенной длительностью синхроимпульса $\tau_{strob} = 2 \cdot \tau_s$, что соответствует длительности смежной пары сегментов. Следовательно, среднее число шумовых импульсов за длительность импульса стробирования будет равно $2 \cdot \bar{n}_b$.

Вероятность повторной регистрации синхроимпульса на этапе тестирования за 1-й тест может быть найдена по формуле

$$p_{test.1.2} = p_{th.s} = \sum_{k_1=k_{th}}^{\infty} Pos(k_1, \bar{k}_s).$$

Условная вероятность повторной регистрации синхроимпульса при k_{test} -м тестировании

$$p_{test.2}\{k_{test}\} = (1 - p_{test.1.2})^{k_{test}-1} p_{test.1.2}.$$

Безусловная вероятность успешного тестирования при допустимом числе тестов $N_{test.2}$ равна

$$P_{test.2} = \sum_{k_{test}=1}^{N_{test.2}} p_{test.2}\{k_{test}\} = \frac{p_{test.1.2}}{1 - p_{test.1.2}} \sum_{k_{test}=1}^{N_{test.2}} (1 - p_{test.1.2})^{k_{test}}.$$

Используя свойства геометрической прогрессии, находим

$$P_{test.2} = 1 - (1 - p_{test.1.2})^{N_{test.2}}.$$

Для обеспечения заданной вероятности успешного тестирования $P_{test.2}$ при произвольной вероятности $p_{test.1.2}$ потребуется не менее $N_{test.2.min}$ тестов:

$$N_{test.2} \geq N_{test.2.min} = \left\lceil \frac{\lg(1 - P_{test.2})}{\lg(1 - p_{test.1.2})} \right\rceil.$$

Затраченное время в случае успешного тестирования при повторной регистрации в смежной паре сегментов в течение k_{test} -го теста равно $T_{test.2} = T_s \cdot k_{test}$, в противном случае, при отрицательном результате тестирования время равно $T_{test.2} = T_s \cdot N_{test.2}$.

Среднее число тестов для успешного тестирования определяется формулой

$$\overline{N_{test.2}} = \sum_{k_{test}=1}^{N_{test.2}} k_{test} \cdot (1 - p_{test.1.2})^{k_{test}-1} \cdot p_{test.1.2}.$$

При этом среднее время тестирования будет равно $\overline{T_{test.2}} = T_s \cdot \overline{N_{test.2}}$.

Результаты расчёта характеристик этапа тестирования в предлагаемом алгоритме представлены в табл. 2. Требуемая безусловная вероятность успешного тестирования составляет $P_{test.2} \geq 0,99$. Протяжённость ВОЛС составляет 20 км, что соответствует периоду следования $T_s = 195,76$ мкс. Следовательно, число сегментов и, соответственно, смежных пар сегментов равно $N_w = 652553$. При ориентации на отклонение в $K_{pD1}=1,1$ раза от предельной вероятности синхронизации $p_{D1.lim2}$ и частоте генерации ИГТ $f_{DCR} = 10$ Гц пороговый уровень равен $k_{th} = 1$, а вероятность ложного срабатывания $p_{th.b} = 6 \cdot 10^{-9}$.

Отметим, увеличение среднего числа фотонов в синхроимпульсе позволяет достичь вероятности успешного тестирования $P_{test.2} \geq 0,99$ при минимально допустимом числе тестов, и, следовательно, значительно уменьшить время тестирования. Так, при увеличении среднего числа фотонов в синхроимпульсе в 2 раза (с 1 до 2) среднее число тестов и среднее время успешного тестирования уменьшаются на 25%, а при увеличении среднего числа фотонов в синхроимпульсе в 10 раз (с 1 до 10) различие составляет уже 35%.

Таблица 2

Результаты расчёта параметров этапа тестирования

$\bar{n}_s$	Среднее число фотонов в синхроимпульсе				
	1	2	3	4	5
$100p_{test1.2}$	63,21	86,47	95,02	98,17	99,33
$N_{test.2}$	5	3	2	2	1
$\bar{N}_{test.2}$	1,538	1,146	1,045	1,018	0,993
$\bar{T}_{test.2}$, мкс	301,01	224,38	204,54	199,21	194,44
$\bar{n}_s$	Среднее число фотонов в синхроимпульсе				
	6	7	8	9	10
$100p_{test1.2}$	99,75	99,91	99,97	99,99	100,00
$N_{test.2}$	1	1	1	1	1
$\bar{N}_{test.2}$	0,998	0,999	1,00	1,00	1,00
$\bar{T}_{test.2}$, мкс	195,27	195,58	195,69	195,74	195,75

Выводы. Получены аналитические выражения для расчёта временных и вероятностных характеристик этапов поиска и тестирования предложенного алгоритма обнаружения на основе выбора смежной пары сегментов с максимальным суммарным отсчётом, в том числе для расчёта допустимого числа кадров и тестов при обеспечении требуемых вероятностей успешного поиска и тестирования соответственно. Результаты расчётов подтверждают значительное снижение допустимого и среднего чисел кадров и тестов и, следовательно, среднего времени успешного поиска и тестирования при увеличении среднего числа фотонов в синхроимпульсе. Так, например, при заданных исходных данных допустимое число тестов, среднее число тестов и среднее время успешного тестирования снижаются в 5; 1,5; 1,6 раза соответственно при увеличении среднего числа фотонов в синхроимпульсе в 5 раз (с 1 до 5).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Румянцев К.Е. Системы квантового распределения ключа: учеб. пособие. – Ростов-на-Дону: ЮФУ, 2011. – 264 с.
2. Румянцев К.Е. Квантовые технологии в телекоммуникационных системах: учебник. – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2021. – 346 с.
3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
4. Rumyantsev K.E., Pljonkin A.P. Single-photon Synchronization Mode of Quantum Key Distribution System // 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). – 2016. – P. 1-6.
5. Lindsey W.C. Synchronization Systems in Communication and Control. – Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
6. Курочкин В.Л. и др. Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – Т. 5. – С. 54-66.
7. Rumyantsev K.E., Linenko 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 - Radiation and Scattering of Electromagnetic Waves, RSEMW 2019. – 2019. – P. 392-395.
8. Миронов Я.К., Миронова П.Д. Вероятность обнаружения сигнального окна в алгоритме поиска фотонного импульса с разбиением временного интервала на временные окна // VI Всероссийская научно-техническая конференция молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности»: Сб. статей Всероссийской научно-технической конференции, 06-12 апреля 2020 г. – Таганрог, 2020. – С. 135-138.
9. 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 // Communications in Computer and Information Science. – 2020. – Vol. 1206. – P. 87-97. – DOI: https://doi.org/10.1007/978-981-15-4451-4_8.

10. 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.
11. 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.
12. Миронов Я.К., Миронова П.Д., Румянцев К.Е. Вероятностные характеристики порогового алгоритма обнаружения синхросигналов в системе квантового распределения ключа на основе информации со смежной пары временных сегментов // Известия ЮФУ. Технические науки. – 2020. – № 4 (214). – С. 221-229.
13. Румянцев К.Е., Миронова П.Д., Шакир Хайдер Хуссейн. Оценка влияния функциональных элементов на параметры системы квантового распределения ключа на основе протокола B92 // Известия ЮФУ. Технические науки. – 2022. – № 4. – С. 63-77.
14. Румянцев К.Е. Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 2. – С. 32-40.
15. Румянцев К.Е., Рудинский Е.А. Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Известия ЮФУ. Технические науки. – 2017. – № 5 (190). – С. 75-89.
16. Румянцев К.Е., Плёткин А.П. Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.
17. Гальярди Р.М., Карп Ш. Оптическая связь. – М.: Связь, 1978. – 424 с.
18. Миронова П.Д. Алгоритм обнаружения синхросигнала в системе квантового распределения ключа на основе сравнения суммы отсчетов со смежной пары сегментов с пороговым уровнем // Digital Era: Матер. I Всероссийской научно-практической конференции. – Грозный: Чеченский государственный университет, 2021. – С. 91-94. – DOI: 10.36684/38-2021-1-91-94.
19. 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 // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сб. докладов II Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь, Россия Ноябрь 30, 2020. – Ставрополь: СКФУ, 2020. – С. 219-226.
20. Румянцев К.Е., Миронова П.Д. Вероятностные характеристики алгоритма обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом // Известия ЮФУ. Технические науки. – 2023. – № 3 (233). – С. 96-107.

REFERENCES

1. Rumyantsev K.E. Sistemy kvantovogo raspredeleniya klyucha: ucheb. posobie [Systems of quantum key distribution: a study guide]. Rostov-on-Donu: YuFU, 2011, 264 p.
2. Rumyantsev K.E. Kvantovye tekhnologii v telekommunikatsionnykh sistemakh: uchebnik [Quantum technologies in telecommunication systems: textbook]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2021, 346 p.
3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography, *Reviews of Modern Physics*, 2002, Vol. 74, No. 1, pp. 145-195.
4. Rumyantsev K.E., Pljonkin A.P. Single-photon Synchronization Mode of Quantum Key Distribution System, *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016, pp. 1-6.
5. Lindsey W.C. Synchronization Systems in Communication and Control. Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
6. 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.
7. Rumyantsev K.E., Linenko 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 - Radiation and Scattering of Electromagnetic Waves, RSEMW 2019*, 2019, pp. 392-395.
8. Mironov Ya.K., Mironova P.D. Veroyatnost' obnaruzheniya signal'nogo okna v algoritme poiska fotonnogo impul'sa s razbieniem vremennogo intervala na vremennye okna [The probability of detecting a signal window in the photon pulse search algorithm with a time interval split into time windows], *VI Vserossiyskaya nauchno-tehnicheskaya konferentsiya molodykh uchenykh, aspirantov, magistrantov i studentov «Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i*

- informatsionnoy bezopasnosti»: Sb. statey Vserossiyskoy nauchno-tekhnicheskoy konferentsii, 06-12 aprelya 2020 g.* [VI All-Russian Scientific and Technical Conference of Young Scientists, postgraduates, undergraduates and students «Fundamental and applied aspects of computer technology and information security»: Collection of articles of the All-Russian Scientific and Technical Conference, 06-12 April 2020]. Taganrog, 2020, pp. 135-138.
9. 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, *Communications in Computer and Information Science*, 2020, Vol. 1206, pp. 87-97. DOI: https://doi.org/10.1007/978-981-15-4451-4_8.
 10. 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.
 11. 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.
 12. 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 (214), pp. 221-229.
 13. Rumyantsev K.E., Mironova P.D., Shakir Khayder Khussey. Otsenka vliyaniya funktsional'nykh elementov na parametry sistemy kvantovogo raspredeleniya klyucha na osnove protokola B92 [Evaluation of the influence of functional elements on the parameters of the quantum key distribution system based on the B92 protocol], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2022, No. 4, pp. 63-77.
 14. Rumyantsev K.E. Sinkhronizatsiya v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polarizatsionnykh iskazheniy [Synchronization in a quantum key distribution system with automatic compensation of polarization distortions], *Telekommunikatsii* [Telecommunications], 2017, No. 2, pp. 32-40.
 15. Rumyantsev K.E., Rudinskiy E.A. Dvukhetapnyy vremennyy algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polarizatsionnykh iskazheniy, *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 5 (190), pp. 75-89.
 16. 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.
 17. Gal'yardi R.M., Karp Sh. Opticheskaya svyaz' [Optical communication]. Moscow: Svyaz', 1978, 424 s.
 18. Mironova P.D. Algoritn obnaruzheniya sinkhrosignala v sisteme kvantovogo raspredeleniya klyucha na osnove sravneniya summy otschetov so smezhnoy pary segmentov s porogovym urovnem [An algorithm for detecting a sync signal in a quantum key distribution system based on comparing the sum of count from an adjacent pair of segments with a threshold level], *Digital Era: Mater. I Vserossiyskoy nauchno prakticheskoy konferentsii* [Digital Era: Materials of the I All-Russian scientific and practical conference]. Groznyy: Chechenskiy gosudarstvennyy universitet, 2021, pp. 91-94. DOI: 10.36684/38-2021-1-91-94.
 19. 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], *Fundamental'nye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii: Sb. dokladov II Vserossiyskoy nauchnoy konferentsii (s priglasheniem zarubezhnykh uchenykh)*, Stavropol', Rossiya Noyabr' 30, 2020 [Collection of reports of the II All-Russian scientific conference (with the invitation of foreign scientists), Stavropol, Russia November 30, 2020]. Stavropol': SKFU, 2020, pp. 219-226.
 20. Rumyantsev K.E., Mironova P.D. Veroyatnostnye kharakteristiki algoritma obnaruzheniya sinkhrosignalov na osnove vybora smezhnoy pary segmentov s maksimal'nym summarnym otschetom [Probabilistic characteristics of the algorithm for detecting sync signals based on the selection of an adjacent pair of segments with the maximum total count], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2023, No. 3 (233), pp. 96-107.

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; д.т.н.; профессор, зав. кафедрой.

Миронов Яков Константинович – e-mail: tmiyap117@gmail.com; тел.: +78632184000, доб. 30004; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; старший преподаватель.

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

Rumyantsev Konstantin Yevgenievich – Southern Federal University; e-mail: rke2004@mail.ru; Taganrog, Russia; phone: +79281827209; the Department of Information Security of Telecommunication Systems; dr. of eng. sc.; professor; head of department.

Mironov Yakov Konstantinovich – e-mail: tmiyap117@gmail.com; phone: +78632184000 (30004); the Department of Information Security of Telecommunication Systems; cand. of eng. sc.; senior lecturer.

Mironova Polina Demyanovna – e-mail: mironova.polina.dem@gmail.com; phone: +79081924053; the Department of Information Security of Telecommunication Systems; assistant.

УДК 519.143

DOI 10.18522/2311-3103-2024-3-126-137

А.О. Новиков, Э.И. Ватутин, С.И. Егоров, В.С. Титов**ИССЛЕДОВАНИЕ АЛГОРИТМА ДАББАГЯНА-ВУ ДЛЯ ПОСТРОЕНИЯ НЕЦИКЛИЧЕСКИХ ПАНДИАГОНАЛЬНЫХ ЛАТИНСКИХ КВАДРАТОВ**

Рассматривается математическая модель и базирующийся на ней алгоритм Даббагяна-Ву, предназначенный для построения нециклических пандиагональных латинских квадратов. Показано, что из-за высокой вычислительной сложности и факта существования других разновидностей пандиагональных квадратов, применение классических алгоритмов, таких как полный перебор и циклических сдвигов, недостаточно для построения полного перечня пандиагональных латинских квадратов. Этим подтверждается цель работы – исследование и экспериментальная апробация математических моделей и алгоритмов, предназначенных для задачи построения за приемлемое время. Здесь производится исследование алгоритма, представленного Даббагяном В. и Ву. Т, который предназначен для построения пандиагональных латинских квадратов простых порядков p , определяемых выражением $p=6n+1$. Можно сказать, что он является модификацией алгоритма циклического построения. То есть, позволяет получить из исходного циклического квадрата пандиагональный нециклический. Преобразование выполняется путем циклических сдвигов в определенных ячейках в каждой строке исходного квадрата. Была разработана программная реализация алгоритма Даббагяна-Ву. Результат экспериментов подтвердил корректность предложенной Даббагяном В. и Ву. Т. методики построения. Таким образом, для порядка 13 удалось найти 72 уникальных квадрата. К тому же, проведена попытка построения для порядка, не являющегося нечетным простым числом, например 25. В данном случае удалось получить 4 корректных пандиагональных латинских квадрата. Путем дополнительных преобразований полученных наборов увеличить количество квадратов, так, для порядка 13 коллекция расширена до 1570, а для 25 – до 210. Исследование позволило углубленно ознакомиться с алгоритмом Даббагяна-Ву и сделать вывод о его особенностях – к достоинствам относится его относительно низкая вычислительная сложность, а к недостаткам – полноценная корректность построений только для нечетных простых порядков. Полученные наборы квадратов в дальнейшем будут задействованы для получения их числовых характеристик при помощи распределенных вычислений.

Пандиагональные латинские квадраты; нециклические латинские квадраты; циклический сдвиг; построение; алгоритм; математическая модель; вычислительная сложность.

A.O. Novikov, E.I. Vatutin, S.I. Egorov, V.S. Titov**RESEARCH OF THE DABBAGHIAN-WU ALGORITHM FOR CONSTRUCTING NON-CYCLIC PANDIAGONAL LATIN SQUARES**

In this paper we consider a mathematical model and the Dabbaghian-Wu algorithm based on it, designed to construct non-cyclic pandiagonal Latin squares. It is shown that due to the high computational complexity and the fact of existence of other varieties of pandiagonal squares, the application of classical algorithms, such as brute force and cyclic shifts, is insufficient to construct a complete list of pandiagonal Latin squares. This