18. *Regev O*. On lattices, learning with errors, random linear codes, and cryptography, *STOC*, 2005, pp. 84-93.
19. Helib. Available at: https://github.com/homenc/HElib (accessed 01 June 2020).
20. FHEW. Available at: https://github.com/lducas/FHEW (accessed 01 June 2020).
21. *Gentry C., Halevi S.* Implementing gentry's fully-homomorphic encryption scheme, *EUROCRYPT, ser. Lecture Notes in Computer Science*, K.G. Paterson, Ed.,Vol. 6632. Springer, 2011, pp. 129-148.
22. *Dijk M., Gentry C., Halevi S., Vaikuntanathan V.* Fully Homomorphic Encryption over the Integers, *Eurocrypt*, 2010.

Статью рекомендовал к опубликованию профессор И.А. Калмыков.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: +79054530191; кафедра безопасности информационных технологий; д.т.н.; профессор.

Русаловский Илья Дмитриевич – e-mail: ilya.rusalovskiy@mail.ru; тел.: +79885526701; кафедра безопасности информационных технологий; аспирант.

Babenko Lyudmila Kliment'evna – Southern Federal University; e-mail: blk@tsure.ru; Block "I", 2, Chekhov street, Taganrog, 347928, Russia; phone: +79054530191; the department of information technologies security; dr. of eng. sc.; professor.

Rusalovsky Il'ya Dmitrievich – e-mail: ilya.rusalovskiy@mail.ru; phone: +79885526701; the department of information technologies security; postgraduate student.

УДК 621.396.96 DOI 10.18522/2311-3103-2020-4-221-229

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

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ ПОРОГОВОГО АЛГОРИТМА ОБНАРУЖЕНИЯ СИНХРОИМПУЛЬСОВ В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОСНОВЕ ИНФОРМАЦИИ СО СМЕЖНОЙ ПАРЫ ВРЕМЕННЫХ СЕГМЕНТОВ*

Системы квантового распределения ключа (КРК) обеспечивают повышенную защищённость передаваемой информации. Для стабильной работы системы КРК необходима точная синхронизация станций пользователей при минимальных временных затратах. Предложен алгоритм обнаружения синхросигнала с пороговым тестом. Предполагается, что синхроимпульс одновременно находится в двух соседних временных сегментах. Вероятность обнаружения пары временных сегментов, где присутствует синхроимпульс, определяется вероятностью превышения порогового уровня суммарным количеством сигнальных и шумовых импульсов, регистрируемых в двух соседних сегментах. Цель исследований направлена на сравнительный анализ порогового уровня и вероятностных характеристик аппаратуры синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра, полученных при ориентации на модели Гаусса и Пуассона для числа фотонов и импульсов темнового тока (ИТТ), принимаемых за время анализа временного сегмента. Исследованы вероятностные характеристики алгоритма обнаружения синхросигналов в системе квантового распределения ключа на основе сравнения числа фотонов со смежной пары временных сегментов с пороговым уровнем. Анализируется применение аппроксимации статистических свойств процессов на выходе фотодетектора законом Пуассона и нормальным распределением. Оценивается влияния модели Пуассона и Гаусса на выбор порогового уровня и расчёт эффективности синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра,

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90040.

полученных при ориентации на модели Гаусса и Пуассона для числа фотонов и ИТТ, принимаемых за время анализа временного сегмента. Установлено, что выбор порогового уровня, исходя из нормального распределения, даёт заниженное значение. Аппроксимация статистики фотонов и импульсов темнового тока нормальным законом обеспечивает пороговый уровень ниже требуемого. Причём различие растёт с ужесточением требований к вероятности ложного срабатывания. Полученные вероятностные свойства алгоритма обнаружения синхросигнала на основе анализа суммы отсчетов со смежной пары сегментов с пороговым уровнем позволяют сформулировать рекомендации по выбору аппроксимации статистики сигнала: для экспресс-расчётов вероятностных характеристик целесообразно использовать модель Гаусса, в случае необходимости более высокой точности анализа рекомендуется использовать модель Пуассона.

Квантовое распределение ключа; синхронизация; пороговый уровень; вероятностные характеристики; модель Гаусса; модель Пуассона.

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

PROBABILISTIC CHARACTERISTICS OF THE THRESHOLD ALGORITHM FOR DETECTING SYNCHRONIZING PULSES IN THE QUANTUM KEY DISTRIBUTION SYSTEM BASED ON INFORMATION FROM AN ADJACENT PAIR OF TIME SEGMENTS

Quantum key distribution systems (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 costs. An algorithm for detecting a sync signal with a threshold test is proposed. It is assumed that the sync pulse is simultaneously in two adjacent time segments. The probability of detecting a pair of time segments where a sync pulse is present is determined by the probability of exceeding the threshold level by the total number of signal and noise pulses recorded in two adjacent segments. The purpose of the research is aimed at a comparative analysis of the threshold level and probabilistic characteristics of synchronization equipment during threshold testing of each pair of time segments within a time frame, obtained when orienting on the Gauss and Poisson model for the number of photons and dark current pulses (DCP) received during the time segment analysis. The probabilistic characteristics of the detection algorithm for sync signals are studied in a quantum key distribution system based on a comparison of the number of photons from an adjacent pair of time segments with a threshold level. The application of the approximation of the statistical properties of the processes at the output of the photodetector by the Poisson law and the normal distribution is analyzed. The influence of the Poisson and Gaussian models on the choice of the threshold level and the calculation of the synchronization efficiency during the threshold testing of each pair of time segments within the time frame are estimated, obtained by orientation on the Gauss and Poisson models for the number of photons and DCP received during the analysis of the time segment. It was established that the choice of the threshold level based on the normal distribution gives an underestimated value. The approximation of the statistics of photons and pulses of dark current by a normal law provides a threshold level lower than the required one. Moreover, the difference grows with stricter requirements for the probability of false positives. The obtained probabilistic properties of the sync signal detection algorithm based on the analysis of the sum of counts from an adjacent pair of segments with a threshold level allow us to formulate recommendations for choosing an approximation of the signal statistics: for express calculations of probabilistic characteristics, it is advisable to use the Gaussian model; if a higher analysis accuracy is required, it is recommended to use the Poisson model.

Quantum key distribution; synchronization; threshold level; probabilistic characteristics; Gaussian model; Poisson model.

Введение. Защищённые системы связи, использующие квантовую криптографию для безопасного распределения ключа (КРК) между удалёнными пользователями, рассматриваются как основа развития информационных сетей будущего [1–6]. При квантовом распределении ключа разнесённые приёмная и передающая станции должны работать синхронно для устранения влияния слу-

чайных задержек сигнала в информационном канале. Временная синхронизация обеспечивается подсистемами синхронизации, являющимися составными частями системы КРК [7, 8].

Вопросы синхронизации станций исследовались в работах отечественных и зарубежных учёных [9–16]. Причём период следования квантовых импульсов принимается за временной кадр, который, в свою очередь, разбивается на конечное число временных сегментов (окон).

В работах [17–19] положение временных сегментов, на которых может находиться синхроимпульс, определяется с помощью подсчёта однофотонных импульсов (ОФИ) и импульсов темнового тока (ИТТ) в каждом временном сегменте. Предполагается, что на первом этапе синхронизации время анализа временного сегмента значительно превышает длительность оптического синхроимпульса.

В отличие от этого в [20] предложено положение сигнального временного сегмента фиксировать посредством подсчёта фотонов в каждой паре временных сегментов. При использовании порогового теста для каждой пары сегментов, испытания продолжаются до тех пор, пока пороговый уровень не будет превышен. При этом принимается решение об обнаружении синхроимпульса в этой паре временных сегментов. Аппаратура переходит ко второму этапу уточнения местоположения синхроимпульса.

Основанием для использования такого алгоритма служит тот факт, что временные сегменты должны анализироваться попарно, так как синхроимпульс может одновременно принадлежать сразу двум соседним временным сегментам. Причём вероятность такого события велика при соизмеримости длительности оптического синхроимпульса и времени анализа временного сегмента.

Здесь для выбора порогового уровня и расчёта вероятностных характеристик предлагается использовать нормальное распределение для числа фотонов и ИТТ, принимаемых за время анализа временного сегмента. Однако теоретическое обоснование отказа от использования дискретного закона Пуассона для выбора порогового уровня и расчётов вероятностных характеристик не обосновано.

Цель исследований направлена на сравнительный анализ порогового уровня и вероятностных характеристик аппаратуры синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра, полученных при ориентации на модели Гаусса и Пуассона для числа фотонов и ИТТ, принимаемых за время анализа временного сегмента.

Алгоритм обнаружения синхросигнала с пороговым тестом. Рассмотрим процесс обнаружения, где синхроимпульсы имеют длительность τ_s. Количество сигнальных ОФИ за длительность синхроимпульса равно n_s, а фоновых ОФИ и ИТТ – n_b. Предположим, что при непрерывном поиске синхроимпульса используется пороговый тест для каждой пары временных сегментов.

Пусть число зарегистрированных импульсов в i-м временном сегменте равно n_i, а в соседнем (i+1)-м сегменте – n_{i+1}. Причём предполагаем, что синхроимпульс одновременно находится в i-м и (i+1)-м временных сегментах.

Вероятность обнаружения $p_{th.s}$ пары i-го и (i+1)-го временных сегментов, где присутствует синхроимпульс, определяется вероятностью превышения порогового уровня k_{th} суммарным количеством $k = n_i + n_{i+1}$ сигнальных и шумовых импульсов, регистрируемых в двух соседних сегментах.

Если распределение отсчётов подчиняется закону Пуассона, то вероятность обнаружения в сигнальной паре i-го и (i+1)-го временных сегментов при среднем суммарном числе сигнальных ОФИ и шумовых импульсов $\overline{n_{sb}} = \overline{n_s} + 2 \cdot \overline{n_b}$ может быть рассчитана по формуле

$$p_{th.s} = \sum_{k=k_{th}}^{\infty} \frac{\overline{n_{sb}}^{k}}{k!} \cdot exp(-\overline{n_{sb}}).$$

Утверждается, что при $\overline{n_{sb}} \geq 9$ (многофотонный или токовый режим синхронизации) распределение Пуассона стремится к нормальному распределению с математическим ожиданием $\overline{n_{sb}}$ и дисперсией $\overline{n_{sb}}$:

$$p(k, \overline{n_{sb}}) = \frac{1}{\sqrt{2\pi\overline{n_{sb}}}} \cdot exp\left(-\frac{(k-\overline{n_{sb}})^2}{2\overline{n_{sb}}}\right).$$

Используя функцию распределения стандартного нормального распределения, находим

$$p_{th.s} = 1 - \Phi\left(\frac{k_{th} - \overline{n_{sb}}}{\sqrt{\overline{n_{sb}}}}\right).$$

Из формулы при $k_{th} = \overline{n_{sb}}$ находим $p_{th.s}$ =0,5. Следовательно, пороговый уровень k_{th} должен превышать значение среднего суммарного числа сигнальных ОФИ и шумовых импульсов $\overline{n_{sb}}$ для обеспечения вероятности обнаружения в сигнальной паре более 0,5.

При ориентации на использование функции ошибок расчёт выполняется по формуле

$$p_{th.s} = \frac{1}{2} \cdot \left[1 - erf\left(\frac{k_{th} - \overline{n_{sb}}}{\sqrt{2\overline{n_{sb}}}}\right)\right] = \frac{1}{2} \cdot erfc\left(\frac{k_{th} - \overline{n_{sb}}}{\sqrt{2\overline{n_{sb}}}}\right).$$

Значение порога выбирается из требования допустимой вероятности $p_{th.b}$ превышения порогового уровня k_{th} суммарным количеством $k = n_i + n_{i+1}$ шумовых импульсов, регистрируемых в паре шумовых временных сегментов.

Вероятность $p_{th.b}$ связана с пороговым уровнем k_{th} соотношением

$$p_{th.b} = \sum_{k=k_{th}}^{\infty} Pos(k, 2 \cdot \overline{n_b}).$$

При ориентации на нормальное распределение вероятность $p_{th.b}$ рассчитывается по формуле

$$p_{th.b} = 1 - \Phi\left(\frac{k_{th} - 2 \cdot \overline{n_b}}{\sqrt{2 \cdot \overline{n_b}}}\right).$$

При $\overline{n_{sb}} \geq 9$ (многофотонный или токовый режим синхронизации) пороговый уровень k_{th} для заданной вероятности $p_{th.b}$ определяется с помощью обратных функций $\Phi^{-1}(x)$ к $\Phi(x)$ или $erf^{-1}(x)$ к $erf(x)$:

$$k_{th} = \begin{cases} 2 \cdot \overline{n_b} + \sqrt{2 \cdot \overline{n_b}} \cdot \Phi^{-1}(1 - p_{th.b}); \\ 2 \cdot \overline{n_b} + \sqrt{4 \cdot \overline{n_b}} \cdot erf^{-1}(1 - 2 \cdot p_{th.b}). \end{cases}$$

На возможности использования и определении границ применимости нормального распределения для расчёта вероятности ложного срабатывания при наблюдении пары фоновых временных сегментов следует остановиться подробнее.

В табл. 1 приведен числовой материал, полученный в ходе анализа зависимостей вероятности ложного срабатывания от среднего числа шумовых импульсов за длительность синхроимпульса для различных пороговых уровней.

Видно, что вероятность ложного срабатывания при анализе пары сегментов, рассчитанная при ориентации на нормальное распределение, даёт заниженное значение. Причём различие превышает 6 порядков при среднем числе шумовых импульсов $\overline{n_b}$=0,5 и пороговом уровне k_{th}=8 (вероятность ложного срабатывания равна $1{,}3\cdot10^{-12}$). Различие уменьшается до двух порядков при среднем числе шумовых импульсов $\overline{n_b}$=1.

Отметим, что различие сокращается с уменьшением порогового уровня. Так, например, если при среднем числе шумовых импульсов $\overline{n_b}$=1,5 различие в вероятности ложного срабатывания составляет 6,12 раз при пороговом уровне k_{th}=8 (вероятность ложного срабатывания равна 0,002), то уже всего 25 % при k_{th}=4 (вероятность ложного срабатывания равна 0,28).

Приемлемое различие вероятностей ложного срабатывания (порядка 20…30 %) обеспечивается при условии $k_{th} \cdot p_{th.b}$>1,2.

Таблица 1

Зависимости вероятности ложного срабатывания от среднего числа шумовых импульсов за длительность синхроимпульса для трёх пороговых уровней. Модели Пуассона и Гаусса

Порог	*Условия. Параметр*	*Среднее число шумовых импульсов*							
		0,5	*1,0*	*1,5*	*2,0*	*2,5*	*3,0*	*3,5*	*4,0*
2	Модель Пуассона	0,26	0,59	0,80	0,91	0,96	0,98	0,99	1,00
	Модель Гаусса	0,16	0,50	0,72	0,84	0,91	0,95	0,97	0,98
	Различие, раз	1,67	1,19	1,12	1,08	1,05	1,04	1,02	1,01
	Произведение порога на вероятность	0,53	1,19	1,60	1,82	1,92	1,97	1,99	1,99
4	Модель Пуассона	0,02	0,14	0,35	0,57	0,73	0,85	0,92	0,96
	Модель Гаусса	0,001	0,08	0,28	0,50	0,67	0,79	0,87	0,92
	Различие, раз	14,1	1,82	1,25	1,13	1,09	1,07	1,05	1,04
	Произведение порога на вероятность	0,08	0,.57	1,41	2,27	1,94	3,40	3,67	3,83
8	Модель Пуассона	10^{-5}	10^{-3}	0,01	0,05	0,13	0,26	0,40	0,55
	Модель Гаусса	$1{,}3\cdot 10^{-12}$	10^{-5}	0,002	0,02	0,09	0,21	0,35	0,50
	Различие, раз	$8\cdot10^{6}$	100	6,12	2,25	1,48	1,24	1,14	1,09
	Произведение порога на вероятность	0,00	0,01	0,10	0,41	1.07	2,05	3,21	4.38

На рис. 1 представлены зависимости вероятности ложного срабатывания от порогового уровня k_{th} при 4-х средних числах шумовых импульсов в сегменте $\overline{n_b}$: 2 (сплошная линия), 3 (штриховая линия), 4 (пунктирная линия) и 5 (штрихпунктирная линия). Ступенчатыми зависимостями представлены результаты расчётов при ориентации на распределение Пуассона, а непрерывными зависимостями – на нормальное распределение.

Из графиков видно, что выбор порогового уровня при ориентации на распределение Гаусса даёт при фиксированной вероятности ложного срабатывания заниженное значение. Например, при среднем числе шумовых импульсов в паре

шумовых временных сегментов 2 при ориентации на распределение Гаусса потребуется для обеспечения вероятности ложного срабатывания менее 10^{-6} выбор порогового уровня 14, а при ориентации на распределение Пуассона – 18 (различие в 1,3 раза). Для более высоких значений среднего числа шумовых импульсов в паре шумовых временных сегментов результаты аналогичны. При обеспечении вероятности ложного срабатывания в паре шумовых временных сегментов ниже 0,01 при среднем числе шумовых импульсов в сегменте $\overline{n_b} \geq 1$ пороговый уровень должен быть более 7, при $\overline{n_b} \geq 2 - k_{th} \geq 10$, а при $\overline{n_b} \geq 5 - k_{th} \geq 18$.

Аппроксимация статистики сигнала моделью Гаусса даёт значение порога, которое меньше на 3-4 единицы реально требуемого. Причём различие растёт с ужесточением требований к вероятности ложного срабатывания.

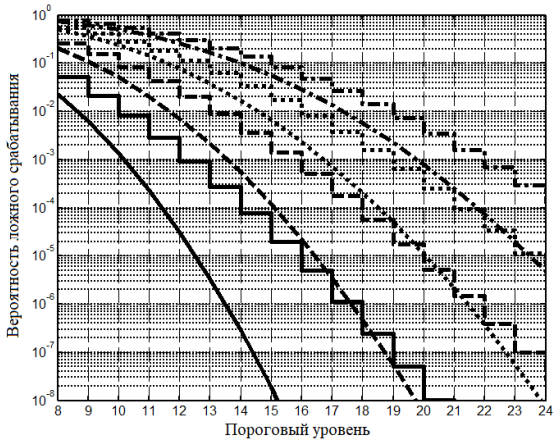

Рис. 1. Зависимости вероятности ложного срабатывания от порогового уровня

Полученные вероятностные свойства алгоритма обнаружения синхросигнала на основе анализа суммы отсчетов со смежной пары сегментов с пороговым уровнем позволяют сформулировать рекомендации по выбору аппроксимации статистики сигнала: для экспресс-расчётов вероятностных характеристик целесообразно использовать модель Гаусса, в случае необходимости более высокой точности анализа рекомендуется использовать модель Пуассона.

Выводы. Получены формулы для расчета порогового уровня, вероятностей ложного срабатывания и обнаружения в сигнальной паре временных сегментов, ориентированные на распределения Пуассона и Гаусса.

Проведен сравнительный анализ порогового уровня и вероятностных характеристик аппаратуры синхронизации при пороговом тестировании каждой пары временных сегментов внутри временного кадра, полученных при ориентации на модели Гаусса и Пуассона для числа фотонов и ИТТ, принимаемых за время анализа временного сегмента.

Выбор порогового уровня при ориентации на распределение Гаусса даёт при фиксированной вероятности ложного срабатывания меньшее значение, чем при использовании распределения Пуассона. Однако распределение Гаусса уместно использовать в случае необходимости проведения быстрого анализа. В связи с этим сформулированы рекомендации по выбору аппроксимации статистики сигнала: для экспресс-расчётов вероятностных характеристик целесообразно использовать модель Гаусса, в случае необходимости более высокой точности анализа рекомендуется использовать модель Пуассона.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ростелеком объявил о внедрении квантовой криптографии на своих сетях. – URL: https://tass.ru/ekonomika/5685597 (дата обращения: 17.10.2018).
2. *Румянцев К.Е.* Системы квантового распределения ключа: монография. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 264 с.
3. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / под ред. Д. Боумейстера, А. Экерта, А. Цайлингера. – М.: Постмаркет, 2002. – 376 с.
4. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
5. *Bennett C., Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE international conference on computers, systems and signal processing. Bangalore. India. – New York: Institute of Electrical and Electronics Engineers, 1984. – P. 175-179.
6. *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol // Physical Review Letters. – 2000. – Vol. 85. – P. 441-444.
7. *Румянцев К.Е.* Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 2. – С. 32-40.
8. *Румянцев К.Е., Плёнкин А.П.* Безопасность режима синхронизации системы квантового распределения ключей // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 135-153.
9. *Курочкин В.Л. и др.* Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – Т. 5. – С. 54-66.
10. *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.
11. *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 - 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019. – 2019. – P. 392-395. DOI: 10.1109/RSEMW.2019.8792769.
12. *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.
13. *Rumyansev K., Rudinsky E.* 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'17). – 2017. – P. 140-147. DOI: 10.1145/3136825.3136888.
14. *Lindsey W.C.* Synchronization Systems in Communication and Control. Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
15. *Стиффлер Дж.* Теория синхронной связи: пер. с англ. / под ред. Э.М. Габидулина. – М.: Связь, 1975.
16. *Румянцев К.Е., Шакир Хайдер Хуссейн.* Ограничения на дальность двухэтапной синхронизации в автокомпенсационной системе квантового распределения ключа // Телекоммуникации. – 2019. – № 12. – С. 2-10.
17. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 81-96.
18. *Rumyantsev K.E., Pljonkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security // International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang. – P. 1-4. DOI: 10.1109/ELINFOCOM.2016.7562955. WOS:000389518100035. IDS: BG5KP.
19. *Румянцев К.Е., Плёнкин А.П.* Эффективность синхронизации системы квантового распределения ключа на однофотонных лавинных фотодиодах // Известия ЮФУ. Технические науки. – 2016. – № 9 (182). – С. 4-15.
20. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.

REFERENCES

1. Rostelekom ob"yavil o vnedrenii kvantovoy kriptografii na svoikh setyakh [Rostelecom announced the introduction of quantum cryptography on its networks]. Available at: https://tass.ru/ekonomika/5685597 (accessed 17 October 2018).
2. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha: monografiya [Systems of quantum key distribution: monograph]. Taganrog: Izd-vo TTI YuFU, 2011, 264 s.
3. Fizika kvantovoy informatsii: Kvantovaya kriptografiya. Kvantovaya teleportatsiya. Kvantovye vychisleniya [Physics of Quantum Information: Quantum Cryptography. Quantum teleportation. Quantum computing], ed. by D. Boumeystera, A. Ekerta, A. TSaylingera. Moscow: Postmarket, 2002, 376 p.
4. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics*, 2002, Vol. 74, No. 1, pp. 145-195.
5. *Bennett C., Brassard G.* Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE international conference on computers, systems and signal processing. Bangalore. India*. New York: Institute of Electrical and Electronics Engineers, 1984, pp. 175-179.
6. *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol, *Physical Review Letters*, 2000, Vol. 85, pp. 441-444.
7. *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.
8. *Rumyantsev K.E., Plenkin A.P.* Bezopasnost' rezhima sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Security of the synchronization mode of a system of quantum key distribution], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 135-153.
9. *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.
10. *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.
11. *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 - 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019*, 2019, pp. 392-395. DOI: 10.1109/RSEMW.2019.8792769.
12. *Rumyantsev K.E., Rudinskiy E.A.* Dvukhetapnyy vremennoy algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Two-stage time synchronization algorithm in a quantum key distribution system with automatic compensation for polarization distortion], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 5 (190), pp. 75-89.
13. *Rumyansev K., Rudinsky E.* 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'17)*, 2017, pp. 140-147. DOI: 10.1145/3136825.3136888.
14. *Lindsey W.C.* Synchronization Systems in Communication and Control. Prentice-Hall, Englewood Cliffs, New Jersey, 1972.
15. *Stiffler Dzh.* Teoriya sinkhronnoy svyazi [Synchronous communication theory]: transl. from engl., ed.by E.M. Gabidulina. Moscow: Svyaz', 1975.
16. *Rumyantsev K.E., Shakir Khayder khusseyn.* Ogranicheniya na dal'nost' dvukhetapnoy sinkhronizatsii v avtokompensatsionnoy sisteme kvantovogo raspredeleniya klyucha [Restrictions on the range of two-stage synchronization in the autocompensation system of quantum key distribution], *Telekommunikatsii* [Telecommunications], 2019, No. 12, pp. 2-10.
17. *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 (157), pp. 81-96.

18. *Rumyantsev K.E., Pljonkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security, *International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang,* pp. 1-4. DOI: 10.1109/ELINFOCOM.2016.7562955. WOS:000389518100035. IDS: BG5KP.
19. *Rumyantsev K.E., Plenkin A.P.* Effektivnost' sinkhronizatsii sistemy kvantovogo raspredeleniya klyucha na odnofotonnykh lavinnykh fotodiodakh [Efficiency of synchronization of a system of quantum key distribution based on single-photon avalanche photodiodes], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 9 (182), pp. 4-15.
20. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz': [Optical communication]. Moscow: Svyaz', 1978, 424 p.

Статью рекомендовала к опубликованию к.т.н. К.Б. Дахкильгова.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Миронов Яков Константинович – e-mail: tmiyap117@gmail.com; 347922, г. Таганрог, пер. Некрасовский, 19; тел.: 89285723456; аспирант.

Миронова Полина Демьяновна – e-mail: linenkopdem@gmail.com; тел.: 89081924053; аспирант.

Rumyantsev Konstantin Evgenievich – Southern Federal University; e-mail: rke2004@mail.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr .of eng. sc.; professor.

Mironov Yakov Konstantinovich – e-mail: tmiyap117@gmail.com; 19, Nekrasovsky lane, Taganrog, 347922, Russia; phone: +79285723456; graduate student.

Mironova Polina Demyanovna – e-mail: linenkopdem@gmail.com; phone: +79081924053; graduate student.