СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 519.7

МЕТОДЫ УСКОРЕНИЯ И УСОВЕРШЕНСТВОВАНИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ НА ОСНОВЕ ЗАДАЧИ О НАХОЖДЕНИИ ГАМИЛЬТОНОВА ЦИКЛА В ГРАФЕ

METHODS OF AN ACCELERATION AND ENHANCEMENT OF THE CRYPTOGRAPHY AUTHENTICATION PROTOCOL WITH ZERO DISCLOSURE OF KNOWLEDGE ON THE BASIS OF THE TASK ABOUT FINDING OF A HAMILTON CYCLE IN THE GRAPH

С.М. Рацеев, М.А. Ростов
S.M. Ratseev, M.A. Rostov

Ульяновский государственный университет, 432017, г. Ульяновск, ул. Льва Толстого, 42

Ulyanovsk State University, 432017, Ulyanovsk, Lev Tolstoy 42

E-mail: ratseevsm@mail.ru

Аннотация
В работе исследуется протокол аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе. Актуальность данного протокола заключается в том, что он основан на NP-полной задаче, поэтому протокол является постквантовым (независим от квантовых вычислений, а именно, устойчив к квантовым атакам). Криптографические протоколы аутентификации с нулевым разглашением знания позволяют проверить подлинность сторон без утечки секретной информации в процессе обмена сообщениями. В качестве первого подхода к ускорению рассматриваемого протокола аутентификации предлагается использование технологии CUDA. Приводятся графики зависимости времени выполнения программной реализации протокола на некоторых популярных языках от количества вершин графа. В качестве второго подхода предлагается модификация данного протокола на основе эллиптических кривых. Приводится описание четырехходного протокола аутентифкации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе с использованием эллиптических кривых.

Abstract
The cryptography authentication protocol with zero disclosure of knowledge on the basis of the task about finding of a Hamilton cycle in the graph is researched. Relevance of this protocol is that it is based on the NP full task therefore the protocol is post-quantum (it is independent of quantum computings, namely, is steady against the quantum attacks). The cryptography authentication protocols based on the proof of knowledge with zero disclosure allow to verify authenticity of the sides without leakage of the classified information during information exchange. As the first approach to an acceleration of the considered authentication protocol use of CUDA technology is considered. Diagrams of dependence of runtime of program protocol implementation in some popular languages from quantity of peaks of a graph are provided. As the second approach modification of this protocol on the basis of elliptic curves which application allows to reduce considerably the sizes of parameters of protocols is offered and to increase their cryptography firmness. The description of the 4-passes protocol of an autentifkation with zero disclosure on the basis of the task about finding of a Hamilton cycle is provided in the graph with use of elliptic curves.

Ключевые слова: протокол аутентификации, нулевое разглашение, эллиптическая кривая, технология CUDA.
Keywords: authentication protocol, zero disclosure, elliptic curve, CUDA technology.

Введение

Протоколы аутентификации разделяют на следующие классы: протоколы, основанные на паролях (слабая аутентификация); протоколы, использующие технику «запрос-ответ» (сильная аутентификация); протоколы, основанные на технике доказательства знания; протоколы доказательства знания с нулевым разглашением.

В парольных схемах злоумышленник может запомнить передаваемые сообщения и в следующий раз использовать эту информацию. В протоколах типа «запрос-ответ» злоумышленник, контролируя канал связи, может навязывать специально подобранные запросы и, анализируя ответы, получить информацию о секрете. Чтобы избежать этого, применяют протоколы доказательства знания (некоторой секретной информации), которые обладают дополнительным свойством нулевого разглашения секрета. Нулевое разглашение – свойство протокола доказательства знания, обеспечивающее такое его выполнение, что никакая информация о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным проверяющим из переданных сообщений за время полиномиально зависящее от суммарной длины этих сообщений.

В данной работе исследуется протокол аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе.

Гамильтоновым циклом в графе называется непрерывный путь, проходящий через все вершины графа ровно по одному разу. Понятно, что если в графе n вершин (занумерованных числами 1, ..., n) и в нем имеется гамильтонов цикл, то путем перебора всех перестановок симметрической группы S_n мы найдем гамильтонов цикл $(\tau(1), ..., \tau(n))$ для некоторой перестановки $\tau \in S_n$. Так как $|S_n| = n!$, то уже при сравнительно небольших значений n (например, $n = 100$) такой подход становится практически нереализуемым. Доказано, что задача нахождения гамильтонова цикла в графе является NP-полной (для ее решения неизвестны алгоритмы, существенно более быстрые, чем метод перебора).

Рассмотрим протокол, в котором абонент A будет доказывать абоненту B, что он знает гамильтонов цикл в некотором графе G так, чтобы абонент B не получил никаких знаний о самом этом цикле (доказательство с нулевым разглашением).

Пусть абонент A знает гамильтонов цикл в графе G из n вершин, который передал ему доверенный центр. Он может это доказывать абоненту B (и всем, кто имеет этот граф) с помощью описываемого ниже протокола.

Протокол доказательства состоит из следующих шагов.

1. Абонент A случайно выбирает перестановку $\sigma \in S_n$ и применяет ее к номерам вершин графа G, получив при этом граф $H = \sigma(G)$. Понятно, что графы G и H изоморфны. Зная гамильтонов цикл в графе G, абонент A знает гамильтонов цикл и в графе H. Граф H передается проверяющему B.

2. Абонент B, получив граф H, случайным образом выбирает $a \in \{0,1\}$ и передает a абоненту A.

3. Если $a = 0$, то абонент A предоставляет абоненту B перестановку σ (тем самым показывая, что он знает изоморфизм графов G и H). Если $a = 1$, то абонент A предоставляет проверяющему B гамильтонов цикл графа H.

4. Проверяющий B проверяет, что в случае $a = 0$ предъявленная перестановка σ действительно переводит граф G в граф H, а в случае $a = 1$ проверяет гамильтонов цикл графа H.

Весть протокол повторяется t раз. Вероятность обмана при t реализациях протокола не превосходит 2^{-t}.

1. Сравнительный анализ производительности протокола для различных языков программирования

Приведенный выше протокол аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе был реализован вторым автором на следующих широко используемых языках программирования: Java, C, C#, PHP. Ниже приведены графики зависимости времени выполнения протокола от количества вершин графа G. Тесты проводились на ПК со следующими характеристиками: ОС Windows 10, GPU GeForce GTX 550 TI 2 Gb, ОЗУ 8 Gb, CPU Intel Core i5 1,7 GHz.

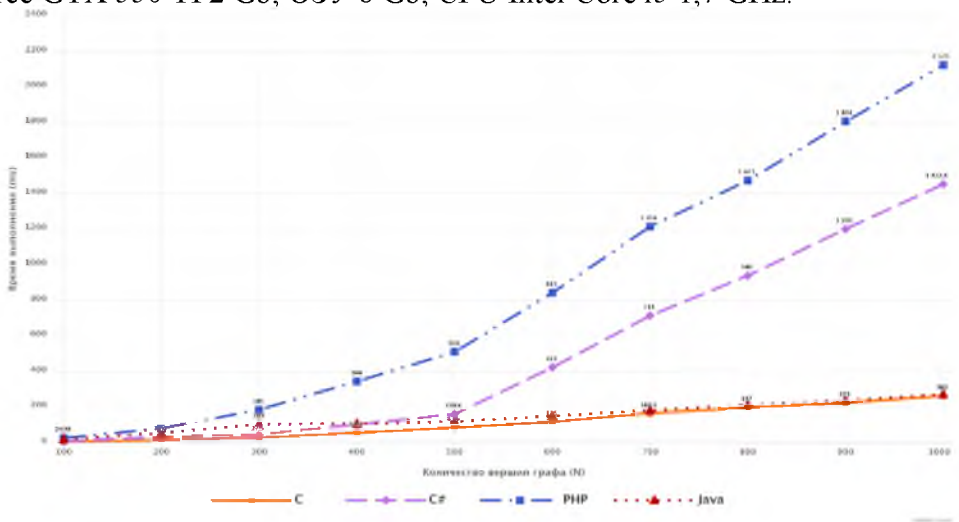

Рис. 1. Графики скоростей выполнения протокола на языках Java, C, C#, PHP
Fig.1. Diagrams of speeds of execution of the protocol in the languages Java, C, C#, PHP

Как видно из рис. 1, асимптотически хорошие скорости выполнения протокола показывают языки C и Java.

Для минимального значения вершин графа берется значение $N = 100$, так как в этом случае число 100! в двоичном виде занимает более 450 бит. Заметим, для сравнения, длина ключа для симметричного блочного шифра «Кузнечик» из ГОСТ Р 34.12-2015 равна 256 бит.

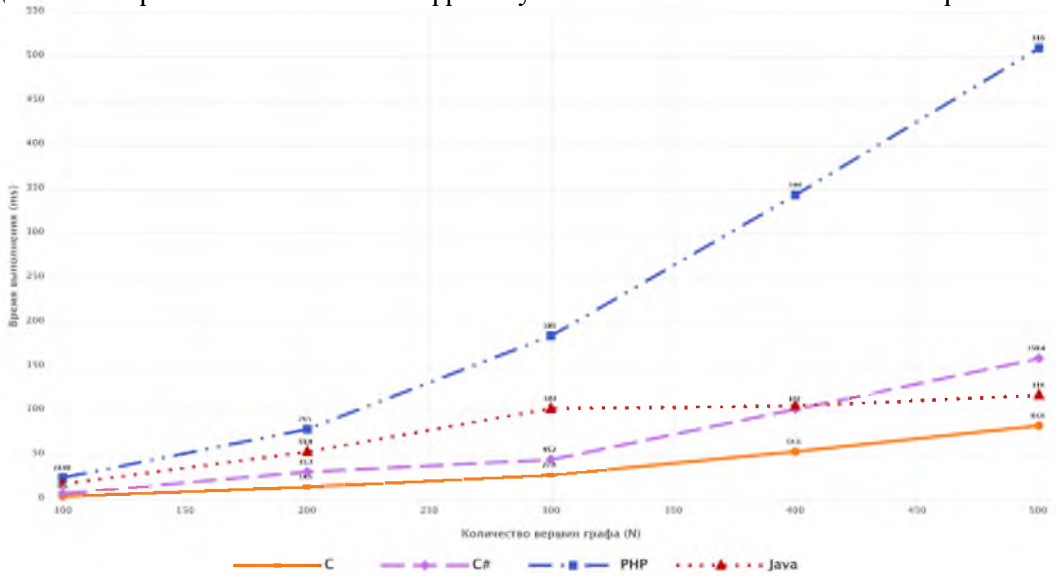

Рис.2. Графики скоростей выполнения протокола на языках Java, C, C#, PHP
Fig.2. Diagrams of speeds of execution of the protocol in the languages Java, C, C#, PHP

При этом, если рассмотреть графики на рис. 2 (до $N = 500$), то на некоторых промежутках реализация на языке C# опережает реализацию на языке Java, но затем (после $N = 500$) начинает значительно терять свои позиции. Не самый лучший результат показала реализация на языке PHP.

2. Применение технологии CUDA для повышения производительности протокола

Хорошо известно, что на современном этапе развития информационных технологий одним из основных факторов увеличения вычислительной мощности является использование графических процессоров. Одними из наиболее эффективно используемых графических процессоров (GPU – graphics processing unit) для выполнения общих вычислений являются видеоускорители компании nVidia с архитектурой CUDA (Compute Unified Device Architecture). Вычислительные задачи, реализованные на CUDA, получают значительное ускорение в таких областях, как молекулярная динамика [Stone, Phillips, Freddolino et al. 2007; Van Meel, Arnold, Frenkel et al. 2008], астрофизика [Zwart, Belleman, Geldof, 2007; Harris, Haines, Staveley-Smith, 2008], медицинская диагностика [Muyan-Ozcelik, Owens, Xia, Samant, 2008] и т.д.

Для протокола аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе в рамках исследования также применялась технология CUDA. На рис. 3 представлены графики зависимости времени выполнения протокола от количества вершин графа G для языков программирования C, Java и технологии CUDA.

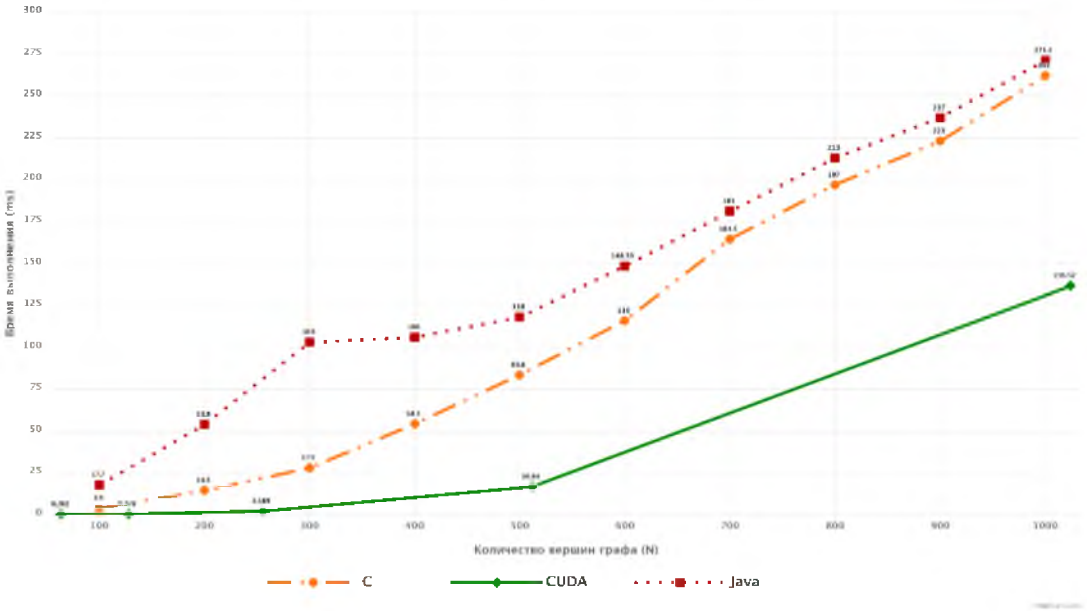

Рис. 3. Графики скоростей выполнения протокола на Java, C, CUDA
Fig.3. Diagrams of speeds of execution of the protocol on Java, C, CUDA

Из рис. 3 видно, что технология CUDA имеет очень высокую скорость выполнения по сравнению с самой быстрой (из рассматриваемых выше реализаций) на языке C.

3. Применение протоколов привязки к биту и эллиптических кривых в протоколах аутентификации с нулевым разглашением

В работах [Bellare, Micali, Ostrovsky, 1990; Введение в криптографию, 2012] рассмотрен способ повышения эффективности доказательств с нулевым разглашением на примере протокола на основе задачи изоморфизма графов. Здесь мы приведем аналог этого метода для протокола аутентификации с нулевым разглашением на основе задачи

поиска гамильтонова цикла в графе. При этом в приведенном здесь протоколе будут фигурировать эллиптические кривые, что повысит его криптографическую стойкость.

Сам принцип функционирования криптосистем на эллиптических кривых подробно изложен в [Hankerson, Menezes, Vanstone, 2004]. Безопасность криптосистем на эллиптических кривых ECC (Elliptic Curve Cryptography), как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой [Hankerson, Menezes, Vanstone, 2004]. Исследования показывают, что в классе криптосистем с открытым ключом, криптосистемы на эллиптических кривых превосходят классические криптосистемы на основе модулярной арифметики, как минимум, по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при аппаратной и программной реализациях [An Elliptic Curve … 2004].

В рассмотренном выше протоколе аутентификации на основе поиска гамильтонова цикла в графе главная проблема – большое количество раундов t. Достаточно естественная идея – выполнить все эти последовательные раунды параллельно. На первом шаге A выбирает m случайных перестановок $\sigma_1,\ldots, \sigma_m$, вычисляет $H_1=\sigma_1(G),\ldots, H_m=\sigma_m(G)$ и посылает все эти m графов проверяющей стороне B. На втором шаге B выбирает m случайных битов $a_1,\ldots, a_m$ и посылает их A, а на третьем A формирует все m требуемых перестановок и посылает их B. Но этот протокол будет являться трехпроходным, а как показывает результат работы [Goldreich, Micali, Wigderson, 1991], трехпроходных доказательств с нулевым разглашением, скорее всего, не существует. Проверяющая сторона B формирует свои запросы $a_1,\ldots, a_m$, уже получив от A все графы $H_1,\ldots, H_m$, и может выбирать их (запросы) зависящими достаточно сложным образом от всех этих графов.

Зависимость $a_1,\ldots, a_m$ от $H_1,\ldots, H_m$ можно предотвратить, используя протокол привязки к биту. Протокол привязки к биту – один из основных типов примитивных криптографических протоколов. Он находит многочисленные применения в криптографии. Проверяющий B выбирает свои запросы в самом начале выполнения протокола, еще до того, как увидит $H_1,\ldots, H_m$. Каждый бит a_i упаковывается в значение (блоб) r_i и B посылает все (блобы) $r_1,\ldots, r_m$ доказывающему A. Только после этого A посылает B все графы $H_1,\ldots, H_m$. В ответ B открывает $a_1,\ldots, a_m$, а доказывающий A, получив $a_1,\ldots, a_m$, формирует требуемые перестановки и посылает их B.

Для протокола привязки к биту используем эллиптические кривые. Пусть q – некоторый (достаточно большой) простой делитель числа $|E_p(a,b)|$, где $E_p(a,b)$ – эллиптическая кривая над полем $\mathbf{Z}_p$ вида $E_p(a,b): y^2 = x^3 + ax + b \,(\mathrm{mod}\ p)$.

Пусть некоторая точка $G \in E_p(a,b)$ имеет порядок q, т.е. образует циклическую подгруппу порядка q в аддитивной абелевой группе $(E_p(a,b),+)$: $<G>=\{G,[2]G,\ldots,[q]G=\mathsf{O}\}$. Абонент A выбирает случайное число x, $1\le x\le q-1$, и вычисляет значение открытого ключа $Y=[x]G$, которое размещается в открытом справочнике или передается проверяющей стороне B. Четырехроходный протокол аутентифкации с нулевым разглашением примет следующий вид.

1. Абонент B генерирует случайные числа k_i, $1\le k_i\le q-1$, битовую строку $(a_1,\ldots,a_m)\in\{0,1\}^m$, вычисляет точки эллиптической кривой $R_i=[k_i]G+[a_i]Y$, $i=1,\ldots,m$, и передает набор $R_1,\ldots, R_m$ абоненту A.

2. Абонент A случайно выбирает перестановки $\sigma_i \in S_n$ и применяет их к номерам вершин графа G, получив при этом графы $H_i = \sigma_i(G)$, $i = 1,\ldots,m$, которые передаются абоненту B.

3. Абонент B, получив графы $H_1,\ldots, H_m$, передает абоненту A значения $k_1,\ldots, k_m$, $a_1,\ldots, a_m$.

4. При $a_i = 0$ абонент A фиксирует перестановку σ_i, при $a_i = 1$ – перестановку, являющуюся гамильтоновом циклом графа H_i, $i = 1,\ldots,m$. Данные перестановки передаются абоненту B.

5. Абонент B проверяет, что в случае $a_i = 0$ предъявленная перестановка σ_i действительно переводит граф G в граф H_i, а в случае $a_i = 1$ проверяет гамильтонов цикл графа H_i, $i = 1,\ldots,m$.

Выводы

Использование протокола привязки к биту обеспечивает безусловную безопасность отправителя. Даже если абонент A обладает неограниченными вычислительными возможностями, он не может извлечь из блобов $R_1,\ldots, R_m$ никакой информации о запросах $a_1,\ldots, a_m$ до тех пор, пока на третьем шаге абонент B сам их не раскроет. Также, как и многораундовый протокол аутентификации на основе поиска гамильтонова цикла в графе, данный протокол остается протоколом с абсолютно нулевым разглашением.

Заметим, что нулевое разглашение играет похожую роль, что и свойство совершенности для шифров и кодов аутентификации [Рацеев, 2015; Рацеев, Череватенко, 2014а; Рацеев, Панов, 2014; Рацеев, 2013; Рацеев, 2014; Рацеев, 2014; Рацеев, Рацеев, 2016; Рацеев, Череватенко, 2014б; Рацеев, 2013; Рацеев, Череватенко, 2017]. Понятие совершенного шифра ввел К. Шеннон в 40-х годах XX века. Такие шифры обеспечивают наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченного шифрованного сообщения. Так как длины ключей шифров замены с неограниченным ключом шифров не меньше длин передаваемых сообщений, то совершенные шифры целесообразно использовать в исключительно важных случаях.

Список литературы
References

1. Stone J.E.E., Phillips J.C.C., Freddolino P.L.L. et al. 2007. Acelerating molecular modeling applications with graphics processors. J. Comput. Chem. 28(16): 2618-2640.

2. Van Meel J.A., Arnold A., Frenkel D. et al. 2008. Harvesting graphics power for MD simulations. Mol. Simulat. 34(3): 259-266.

3. Zwart S.F.P., Bel leman R.G., Geldof P.M. 2007. High-performance direct gravitational Nbody simulations on graphics processing units. New Astronomy. 12(8): 641-650.

4. Harris C., Haines K., Staveley-Smith L. 2008. GPU accelerated radio astronomy signal convolution. Exp. Astron. 22(1): 129-141.

5. Muyan-Ozcelik P., Owens J.D., Xia J., Samant S.S. 2008. Fast deformable registration on the GPU: A CUDA implementation of demons. Computational Science and its Applications: Intern. Conf.: 223-233.

6. Bellare M., Micali S., Ostrovsky R. 1990. Perfect zero-knowledge in constant rounds. Proc. 22nd Annu. ACM Symp. on Theory of Computing: 482-493.

7. Введение в криптографию. 2012. Под общ. ред. В.В. Ященко. 4-е изд., доп. М., МЦНМО, 348.

Introduction to cryptography. 2012. Under a general editionof V.V. Yashchenko. 4prod., additional M., MTsNMO, 348. (in Russian)

8. Hankerson D., Menezes A., Vanstone S. 2004. Guide to Elliptic Curve Cryptography.

Springer-Verlag, New York, 358.

9. An Elliptic Curve Cryptography (ECC). Primer why ECC is the next generation of public key cryptography. The Certicom 'Catch the Curve' White Paper Series, June 2004, 24.

10. Goldreich O., Micali S., Wigderson A. 1991. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. J. ACM. 38(3): 691-729.

11. Рацеев С.М. 2015. Некоторые обобщения теории Шеннона о совершенных шифрах. Вестник Южно-Уральского государственного университета. Серия Математическое моделирование и программирование. 8(1): 111-127.

Ratseev S.M. 2015. Some generalizations of Shannon's theory of perfect ciphers. Vestnik YuUrGU. Ser. Mat. Model. Progr. [Bulletin of the South Ural State University, Series: Mathematical Modelling, Programming and Computer Software]. 8(1): 111-127. (in Russian)

12. Рацеев С.М., Череватенко О.И. 2014а. О совершенных шифрах на основе ортогональных таблиц. Вестник Южно-Уральского государственного университета. Серия Математическое моделирование и программирование. 7(2): 66-73.

Ratseev S.M., Cherevatenko O.I. 2014a. On perfect ciphers based on orthogonal tables. Vestnik YuUrGU. Ser. Mat. Model. Progr. [Bulletin of the South Ural State University, Series: Mathematical Modelling, Programming and Computer Software]. 7(2): 66-73. (in Russian)

13. Рацеев С.М., Панов Н.П. 2014. О построении совершенных шифров замены с неограниченным ключом. Научные ведомости БелГУ. Математика. Физика. 7(183): 84-91.

Ratseev S.M., Panov N.P. 2014. On constructions of perfect ciphers of substitution with unbounded key. Nauchnye vedomosti BelGU. Ser. Matematika. Fizika [Belgorod State University Scientific Bulletin. Mathematics & Physics]. 7(183): 84-91. (in Russian)

14. Рацеев С.М. 2013. О совершенных имитостойких шифрах замены с неограниченным ключом. Вестник Самарского государственного университета. Естественнонаучная серия. Т. 110, № 9/1: 42-48.

Ratseev S.M. 2013. On perfect imitation resistant ciphers of substitution with unbounded key. Vestnik SamGU. Estestvenno-Nauchnaya Ser. [Vestnik of Samara State University. Natural Science Series]. Vol. 110, № 9/1: 42-48. (in Russian)

15. Рацеев С.М. 2014. О теоретически стойких шифрах. Системы и средства информатики. 24(1): 61-72.

Ratseev S.M. 2014. On theoretic perfect ciphers. Sistemy i Sredstva Informatiki [Systems and Means of Informatics]. 24(1): 61-72. (in Russian)

16. Рацеев С.М. 2014. О построении совершенных шифров. Вестник Самарского государственного технического университета. Серия Физ.-мат. науки. 34(1): С. 192-199.

Ratseev S.M. 2014. On construction of perfect ciphers. Vestnik Samarskogo Gosudarstvennogo Tekhnicheskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki [Vestnik of Samara State Technical University, Ser. Physical and Mathematical Sciences]. 34(1): С. 192-199. (in Russian)

17. Рацеев С.М., Рацеев В.М. 2016. Построение совершенных имитостойких шифров на основе комбинаторных объектов. Вестник Самарского университета. Естественнонаучная серия. № 1-2: 46-50.

Ratseev S.M., Ratseev V.M. 2016. On perfect imitation resistant ciphers based on combinatorial objects. Vestnik SamGU. Estestvenno-Nauchnaya Ser. [Vestnik of Samara University. Natural Science Series]. № 1-2: 46-50. (in Russian)

18. Рацеев С.М., Череватенко О.И. 2014б. О кодах аутентификации на основе ортогональных таблиц. Вестник Самарского государственного технического университета. Серия Физ.-мат. науки. 37(4): 178-186.

Ratseev S.M., Cherevatenko O.I. 2014b. On authentication codes based on orthogonal tables. Vestnik Samarskogo Gosudarstvennogo Tekhnicheskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki [Vestnik of Samara State Technical University, Ser. Physical and Mathematical Sciences] 37(4): 178-186. (in Russian)

19. Рацеев С.М. 2013. Об оптимальных кодах аутентификации. Системы и средства информатики. 23(1): 53-57.

Ratseev S.M. 2013.On optimal authentication code. Sistemy i Sredstva Informatiki [Systems and Means of Informatics]. 23(1): 53-57. (in Russian)

20. Рацеев С.М., Череватенко О.И. 2017. Об оптимальных кодах аутентификации на основе конечных полей. Научные ведомости БелГУ. Математика. Физика. 13(262): 38-41.

Ratseev S.M., Cherevatenko O.I. 2017. On authentication codes based on finite fields. Nauchnyye vedomosti BelGU. Matematika. Fizika [Belgorod State University Scientific Bulletin. Mathematics & Physics]. 13(262): 38-41. (in Russian)