МЕТОД ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ХЭШ-ФУНКЦИЙ НА ОСНОВЕ ИТЕРАЦИЙ ОБОБЩЕННОГО КЛЕТОЧНОГО АВТОМАТА

Ключарёв П.Г.[1]

В статье предлагается новый метод, предназначенный для построения криптографических хэш–функций. Метод основан на использовании обобщенных клеточных автоматов. Работа таких хэш–функций состоит из трех этапов: этапа абсорбирования, этапа дополнительного перемешивания и этапа выжимания. На этапе абсорбирования к заполнению обобщенного клеточного автомата раз в определенное количество шагов подмешивается очередной блок сообщения. На этапе дополнительного перемешивания выполняется определенное количество шагов автомата. А на этапе выжимания происходит съем выходных значений, также через определенное количество шагов. Такую схему можно рассматривать как аналог криптографической губки (Sponge). В качестве графа обобщенного клеточного автомата используются расширяющие графы, в особенности графы Рамануджана, такие как графы Любоцкого–Филипса–Сарнака. Согласно предварительным исследованиями производительности, хэш–функции, построенные с помощью предложенного метода, как и другие криптоалгоритмы, основанные на обобщенных клеточных автоматах, отличаются высокой производительностью при аппаратной реализации, например, на базе программируемых логических интегральных схем. Также уделено внимание вопросам использования хэш–функций, основанных на обобщенных клеточных автоматах, в качестве функций формирования ключа.

Работа выполнена при финансовой поддержке РФФИ (проект № 16–07–00542).

Ключевые слова: *криптография, криптостойкость, криптографическая губка, граф Рамануджана, криптоалгоритмы, программируемые интегральные схемы, информационная безопасность, обобщенный клеточный автомат, локальная функция связи, способ построения криптографических хэш–функций, три этапа вычисления хэш–функции, коллизии в клеточных автоматах.*

DOI: 10.21681/2311-3456-2017-1-45-50

Введение

Во многих задачах управления и обработки информации существует необходимость быстро передавать большие объемы информации, обеспечивая при этом необходимый уровень информационной безопасности. Это приводит к необходимости разработки высокопроизводительных криптографических алгоритмов, в том числе, хэш-функций.

Криптографическим хэш-функциям посвящено большое количество работ. Хороший обзор современного состояния этой области криптографии можно найти в работах [1, 2].

Данная статья является продолжением серии статей (в том числе, [3-9]), посвященных обобщенным клеточным автоматам и методам построения основанных на них криптографических алгоритмов.

Целью статьи является построение нового семейства хэш-функций, в основе которого лежит процесс итераций обобщенного клеточного автомата. Схема построения таких хэш-функций имеет общие черты с концепцией криптографической губки (Sponge), которой посвящен целый ряд работ [10-13]. В частности, хэш-функция Keccak [13], ставшая стандартом США SHA-3, основана на этой схеме.

Автором уже предлагалось использовать обобщенные клеточные автоматы для построения криптографических хэш-функций, при этом использовалась древовидная схема [14]. Предлагаемый в данной статье метод построения хэш-функций обладает, по предварительным оценкам, значительно большей производительностью.

Обобщенные клеточные автоматы

Будем называть *обобщённым клеточным автоматом* ориентированный мультиграф $A(V,E)$, где $V=\{v_1,\ldots,v_N\}$ - множество вершин, а E -мультимножество ребер. С каждой вершиной v_i этого графа ассоциированы:

- булева переменная m_i, которая называется *ячейкой*;
- булева функция $f_i(x_1,\ldots,x_{d_i})$, которая называется локальной функцией связи i-й вершины.

При этом каждой паре (v,e), где v - вершина, а e - инцидентное ей ребро, будет соответствовать номер аргумента локальной функции связи, вычисляемой в вершине v. Мы будем называть его номером ребра e относительно вершины v.

1 Ключарёв Петр Георгиевич, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана, Москва, pk.iu8@yandex.ru

Обобщенный клеточный автомат работает пошагово. Перед началом работы автомата каждая ячейка m_i, $i = 1...N$, имеет начальное значение $m_i(0) \in \{0,1\}$. Далее, значения ячеек на шаге номер t вычисляются по формуле:

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)), \quad (1)$$

где $\eta(i,j)$ – номер вершины, из которой исходит ребро, заходящее в вершину i и имеющее относительно этой вершины номер j. Заполнением клеточного автомата на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \ldots, m_N(t))$.

Обобщенный клеточный автомат будем называть *однородным*, если для любого $i \in \{1,...,N\}$ выполняется $f_i = f$, то есть локальная функция связи для всех ячеек одинакова. Степени захода вершин такого клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$.

Назовем обобщённый клеточный автомат *неориентированным*, если для любого ребра (u,v) в его графе существует и ребро (v,u). Граф такого автомата можно рассматривать как неориентированный, если заменить каждую пару ориентированных ребер (u,v) и (v,u) на неориентированное ребро $\{u,v\}$.

Здесь мы будем использовать лишь неориентированные однородные обобщённые клеточные автоматы, для краткости называя их просто обобщёнными клеточными автоматами.

Пусть $F_t : \{0,1\}^N \to \{0,1\}^N$ - функция, аргументом которой является начальное заполнение данного обобщенного клеточного автомата, а значением – заполнение этого автомата через *t* шагов.

Хэш-функции

Здесь мы предложим способ построения криптографических хэш-функций. Хэш-функция основана на итерациях обобщенного клеточного автомата. Принцип работы заключается в том, чтобы через определенное количество шагов обобщенного клеточного автомата подмешивать к его заполнению очередной блок хэшируемого сообщения, а затем, опять-таки через определенное количество шагов, снимать выходное значение.

Опишем этот процесс более строго. Пусть k – длина блока хэш-функции. Тогда разделим набор ячеек клеточного автомата на два набора, один – длины k, а другой – длины $N-k$. Соответственно будем записывать преобразование, выполняемое за *t* шагов автомата, в виде: $(x_{i+1}, y_{i+1}) = F_t(x_i, y_i)$.

Пусть $M = (M_1, M_2, \ldots, M_q)$ - разбитое на блоки сообщение, для которого вычисляется хэш. Тогда процесс вычисления хэш-функции состоит из трех этапов:

1. Этап абсорбирования:
$$(x_i, y_i) = F_{t_1}(x_{i-1} \oplus M_i, \mathrm{y}_{i-1}) \quad (2)$$
2. Этап дополнительного перемешивания:
$$(h_1, \mathrm{z}_1) = F_{t_2}(\mathrm{x}_q, \mathrm{y}_q) \quad (3)$$
3. Этап выжимания:
$$(h_{j+1}, \mathrm{z}_{j+1}) = F_{t_3}(h_j, \mathrm{z}_j) \quad (4)$$

При этом значением хэша является конечная последовательность вида $h_1, h_2, \ldots, h_{\lceil s/k \rceil}$, необходимой длины.

Конкретная хэш-функция задается графом обобщенного клеточного автомата, локальной функцией связи, числом ячеек автомата, параметрами t_1, t_2, t_3, длиной блока и длиной хэша. Поэтому можно говорить как о методе построения хэш-функций, так и о семействе хэш-функций, которое порождается этим методом. Будем называть предлагаемое семейство GRACE-H2.

Выбор параметров

Наиболее нетривиальный вопрос – выбор графа обобщенного клеточного автомата и локальной функции связи. Вопрос их выбора для криптографических применений был подробно исследован автором, в частности, в работах [5, 10]. Исследования эти показали, что хорошим выбором графа клеточного автомата являются графы Рамануджана [21-25]. При этом, отношение числа вершин графа к длине блока должно быть не менее 4.

Напомним, что графом Рамануджана называется регулярный граф, для которого справедливо неравенство

$$\lambda_2 \le 2\sqrt{d-1},$$

где λ_2 - второй по величине компонент спектра графа, а *d* – степень графа.

Такие графы имеют большой коэффициент реберного расширения, малый диаметр ($O(\log N)$) и ряд других свойств, делающих такие графы особенно подходящими для клеточных автоматов, применяющихся в криптоалгоритмах. Применение таких графов в криптографических примитивах подробно рассматриваются в работах автора [4, 6, 11]. В частности, там предлагается использовать семейство графов Любоцкого-Филипса-Сарнака (LPS). Кратко опишем здесь строение таких графов.

Выберем простые числа p и q, для которых выполняются условия:

$$\begin{cases} p = 1 \pmod 4 \\ q = 1 \pmod 4 \\ p \neq q \\ \left(\frac{p}{q}\right) = 1, \end{cases} \quad (5)$$

где $\left(\frac{p}{q}\right)$ - символ Лежандра.

Построим неориентированный мультиграф $G = (V, E)$. В качестве множества V вершин возьмем проективную прямую над полем Галуа F_q, т.е., $V = P^1(\mathsf{F}_q) = \mathsf{F}_q \cup \{\infty\}$. В качестве мультимножества ребер E возьмем мультимножество, состоящее из всех пар (u, v), таких, что выполняется:

$$v = \frac{(a_0 + ia_1)u + (a_2 + ia_3)}{(-a_2 + ia_3)u + (a_0 - ia_1)} \quad (6)$$

для всех таких четверок $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, что a_0 - нечетное положительное число, a_1, a_2, a_3 - четные числа и выполняется равенство $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. Степенью графа является количество таких четверок, очевидно равное $p+1$.

Здесь $i \in \mathsf{F}_q$, такое, что $i^2 = -1$.

В построенном таким образом графе могут быть как кратные ребра, так и петли. От них необходимо избавиться так, чтобы граф оставался регулярным. После этого граф можно считать построенным.

Кроме LPS-графов в качестве графа обобщенного клеточного автомата можно использовать и другие семейства графов Рамануджана. Можно генерировать такие графы и случайно, с последующей проверкой на принадлежность к графам Рамануджана (с помощью стандартных методов линейной алгебры), поскольку случайный регулярный граф является с большой вероятностью графом Рамануджана.

В качестве локальной функции связи следует выбирать равновесную функцию, имеющую достаточно высокую нелинейность (т.е. возможно большее расстояние до множества аффинных функций), являющуюся шефферовой и обладающую некоторыми дополнительными свойствами. Подробно такие функции описаны в работах [9-11].

Параметры t_1, t_2, t_3 имеет смысл выбирать так, чтобы каждый разряд выхода преобразования F_{t_i} зависел от каждого разряда входа и чтобы эти преобразования были неотличимы от псевдослучайных функций. Для того, чтобы обеспечить выполнение этих условий, согласно работе [11], необходимо чтобы выполнялось неравенство $t_i \geq 1.4D$, где D – диаметр графа. Заметим, что диаметр графа Рамануджана равен $O(\log(N))$.

Таким образом, из соображений обеспечения высокой производительности, в качестве значения параметра t_1 имеет смысл выбрать минимальное значение, удовлетворяющее вышеприведенному неравенству, т.е. $1.4D$. При этом, в качестве значений параметров t_2 и t_3 следует взять большие величины, например, не меньшие трехкратного диаметра графа, с тем, чтобы обеспечить хорошее перемешивание информации и реализацию сложных зависимостей значения хэш-функции от ее входа.

Использование в качестве функций формирования ключа

Важное применение хэш-функций – их использование в качестве функций формирования ключа. Такие функции предназначены в первую очередь для выработки ключевой информации из паролей. Они должны обладать дополнительными свойствами, затрудняющими восстановление паролей методом грубой силы, такими как низкая способность к распараллеливанию и относительно высокая вычислительная сложность.

Хэш-функции, основанные на обобщенных клеточных автоматах, прекрасно подходят в качестве таких функций, благодаря тому, что количество ячеек обобщенного клеточного автомата принципиально ничем не ограничено и, следовательно, может быть выбрано достаточно большим с тем, чтобы сделать невозможным эффективное распараллеливание вычислений.

В частности, для того, чтобы сделать невозможным эффективное вычисление выходных значений клеточных автоматов с помощью графических процессоров (технологий OpenCL и CUDA), необходимо выбрать число ячеек большим, чем количество потоков в рабочей группе графического процессора, которое составляет от нескольких сотен до нескольких тысяч, в зависимости от конкретного графического процессора.

Важно также обеспечить противодействие параллельной обработке на программируемых логических интегральных схемах (ПЛИС). Заметим, что для реализации одного клеточного автомата необходимо количество логических элементов, примерно равное количеству ячеек (в случае, если конкретной ПЛИС поддерживаются не менее чем d-местные логические элементы). У современных ПЛИС количество логических элементов

достигает нескольких миллионов. В любом случае, использование клеточных автоматов, состоящих из десятков и сотен тысяч ячеек, существенно ограничивает возможность распараллеливания с использованием ПЛИС, поскольку одновременно на такой ПЛИС можно будет реализовать не более $\lfloor a / N \rfloor$ клеточных автоматов, где a – количество логических элементов ПЛИС, а N – число ячеек клеточного автомата.

Увеличение количества ячеек клеточного автомата приводит к некоторому снижению производительности, однако, учитывая, что в случае использования графов Рамануджана необходимое число шагов оценивается как $\Omega(\log N)$, вычислительная сложность растет достаточно медленно, что позволяет использовать такие функции на практике.

Криптостойкость

В работе [11] было обнаружено, что при достаточном числе шагов, преобразование, вычисляемое обобщенным клеточным автоматом, граф которого является графом Рамануджана, в случае правильного выбора локальной функции связи, неотличимо от псевдослучайной функции посредством стандартного набора статистических тестов NIST. Поэтому, как было сказано выше, мы будем считать, что функции F_{t_i} являются псевдослучайными при достаточно большом числе шагов (согласно работе [11] - не меньшим $1.4D$, где D – диаметр графа). Это приводит к возможности тривиального переноса известного из теории конструкции криптографической губки результата о том, что в случае, если функция преобразования криптографической губки является случайной функцией либо случайной подстановкой и используется подходящая процедура дополнения сообщения, то в случае отсутствия внутренних коллизий, все разряды выхода являются независимыми и равномерно распределенными случайными величинами. Применительно к нашему случаю, для этого требуется отсутствие коллизий обобщенного клеточного автомата.

Вопрос коллизий в клеточных автоматах исследовался в работе [13]. Там был получен метод построения обобщенных клеточных автоматов, устойчивых к определенным типам коллизий. В частности, предлагалось использовать локальную функцию связи, линейную по одной из переменных, причем граф клеточного автомата должен быть таким, чтобы ребра, соответствующие переменным, по которым имеется линейная зависимость, вместе с инцидентными им вершинами, образовывали 2-фактор графа.

Отметим, что одной из подходящих процедур дополнения сообщения, как это известно из теории схемы Sponge, является дополнение последовательностью вида 10^*1 до длины кратной длине блока. Такую процедуру мы рекомендуем использовать и в нашем случае.

Реализация

Хэш-функции из предложенного семейства, как и другие криптоалгоритмы, основанные на клеточных автоматах, предназначены, прежде всего, для аппаратной реализации, в частности, на базе программируемых логических интегральных схем (ПЛИС). Поточные и блочные шифры, основанные на клеточных автоматах показали очень высокую производительность при реализации на ПЛИС [12]. В частности, такие поточные шифры показывали производительность до 1.1 Тб/с. Предварительные исследования показывают, что и рассматриваемые в этой статье хэш-функции также демонстрируют весьма высокий уровень производительности, доходящий до сотен гигабит в секунду, однако более подробное выяснение скоростных характеристик требует дополнительных исследований.

Применение

Рассматриваемые хэш-функции могут быть применены в различных приложениях, в частности в системах электронной подписи [15], системах организации доступа к данным [1,3,14] и другим задачам информационной безопасности [2].

Выводы

Таким образом в статье представлен новый метод построения криптографических хэш-функций, основанных на обобщенных клеточных автоматах. Этот метод порождает целое семейство хэш-функций, каждая из которых задается набором параметров. Эти хэш-функции рассчитаны на аппаратную реализацию (например, на базе ПЛИС) и могут найти весьма широкое применение в различных задачах, связанных с обеспечением информационной безопасности.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, v.tsirlov@bmstu.ru*

Работа выполнена при финансовой поддержке РФФИ (проект № 16-07-00542 а).

Литература

1. Al-Kuwari S., Davenport J.H., Bradford R.J. Cryptographic hash functions: recent design trends and security notions // 2010. URL: http://eprint.iacr.org/2011/565
2. Preneel B. The first 30 years of cryptographic hash functions and the NIST SHA-3 competition // Topics in Cryptology-CT-RSA 2010. 2010. — С. 1-14.
3. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10. URL: http://technomag.neicon.ru/doc/241308.html
4. Ключарев П.Г. Криптографические свойства клеточных автоматов, основанных на графах Любоцкого-Филипса-Сарнака // Безопасные информационные технологии. – М.: НИИ радиоэлектроники и лазерной техники. 2011. — С. 163-173.
5. Ключарев П.Г. Построение псевдослучайных функций на основе обобщённых клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 10. DOI: 10.7463/1112.0496381
6. Ключарев П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2012. № 12. DOI: 10.7463/0113.0517543
7. Ключарев П.Г. Обеспечение криптографических свойств обобщённых клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 3. URL: http://technomag.neicon.ru/doc/358973.html
8. Ключарев П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. Электронное научно-техническое издание. 2012. № 1. URL: http://technomag.neicon.ru/doc/312834.html
9. Ключарев П.Г. О периоде обобщённых клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 2. URL: http://technomag.neicon.ru/doc/340943.html
10. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge functions. : Citeseer, 2007.
11. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak sponge function family main document. 2009. — 30 p.
12. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge-based pseudo-random number generators. : Springer, 2010. — P. 33-47.
13. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak. : Springer, 2013. — P. 313-314.
14. Ключарев П.Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2013. № 1. DOI: 10.7463/0113.0534640
15. Charles D.X., Goren E.Z., Lauter K.E. Families of Ramanujan graphs and quaternion algebras // Groups and symmetries: from Neolithic Scots to John McKay. 2009. Т. 47. — С. P. 53-63.
16. Davidoff G.P., Sarnak P., Valette A. Elementary number theory, group theory, and Ramanujan graphs. — New York : Cambridge University Press, 2003. — 144 p.
17. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. 1988. — P. 261-277.
18. Sarnak P. Some applications of modular forms. — Cambridge ; New York : Cambridge University Press, 1990. — 111 p.
19. Ключарёв П.Г. Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий // Наука и образование. Электронное научно-техническое издание. 2014. № 9. — С. 194-202. DOI: 10.7463/0914.0727086
20. Ключарев П.Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных атоматах // Наука и образование. Электронное научно-техническое издание. 2013. № 10. — С. 299-314. DOI: 1013.0624722
21. Лебедев А.Н. Электронная подпись: новый этап // Вестник Московско-го городского педагогического университета: серия Экономика. 2013. № 1. — С. 43-51.
22. Лебедев А.Н. Способ рассылки защищенных данных с регулировани-ем доступа к отдельным их разделам // Вопросы кибербезопасности. 2015. № 5. — С. 70-72.
23. Быков А.Ю. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Наука и образование. Электронное научно-техническое издание. 2015. № 9. — С. 160-187. DOI: 10.7463/0915.0812283
24. Быков А.Ю., Панфилов Ф.А., Ховрина А.В. Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Наука и образование. Электронное научно-техническое издание. 2016. Т. 1. — С. 90-107. DOI: 10.7463/0116.0830972
25. Быков А.Ю., Артамонова А.Ю. Модификация метода вектора спада для оптимизационно-имитационного подхода к задачам проектирования систем защиты информации // Наука и образование. Электронное научно-техническое издание. 2015. № 1. — С. 158-175. DOI: 10.7463/0115.0754845

METHODS OF DESIGNING CRYPTOGRAPHIC HASH-FUNCTIONS BASED ON ITERATION OF THE UNIFORM CELLULAR AUTOMAT

***P. Klyucharev*[2]**

Abstract. *The article suggests a new method of designing cryptographic hash–functions. The method is based on the use of uniform cellular automata. The work of such hash–functions consists of three stages: absorption stage, additional hashing stage and extraction stage. At the absorption stage, another message block is added to the fill of the uniform cellular automaton once in a certain number of steps. A certain number of*

2 Petr Klyucharev, Ph.D., Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

the automaton steps is accomplished at the additional hashing stage. At the extraction stage, the output values are removed, also in a certain number of steps. Such scheme can be viewed as an analogue of cryptographic sponge (Sponge). The graph of the uniform cellular automaton in use is represented by the expander graphs, especially Ramanujan graphs, such as Lubotzky–Phillips–Sarnak graphs. Subject to the preliminary performance studies, hash–functions are built with the help of the suggested method, just like other encryption algorithms based on uniform cellular automata, which have high performance in hardware implementation, for instance, on the basis of programmable integrated logic circuits. The article also covers the issue of the use of hash–functions based on uniform cellular automata as the key generation function.

Keywords: *cryptography, cryptographic, cryptographic sponge, Ramanujan graph, cryptographic algorithms, programmable integrated circuits, information security, generalized cellular automaton, a local communication function, a method for constructing cryptographic hash functions, three steps of calculating hash collisions in cellular automat.*

References

1. Al-Kuwari S., Davenport J.H., Bradford R.J. Cryptographic hash functions: recent design trends and security notions,2010. URL: http://eprint.iacr.org/2011/565
2. Preneel B. The first 30 years of cryptographic hash functions and the NIST SHA-3 competition,Topics in Cryptology-CT-RSA 2010. 2010. — C. 1-14.
3. Klyucharev P.G. Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluchaynykh posledovatel'nostey,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2011, No 10. URL: http://technomag.neicon.ru/doc/241308.html
4. Klyucharev P.G. Kriptograficheskie svoystva kletochnykh avtomatov, osnovannykh na grafakh Lyubotskogo-Filipsa-Sarnaka,Bezopasnye informatsionnye tekhnologii. – M.: NII radioelektroniki i lazernoy tekhniki. 2011. — C. 163-173.
5. Klyucharev P.G. Postroenie psevdosluchaynykh funktsiy na osnove obobshchennykh kletochnykh avtomatov,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2012, No 10. DOI: 10.7463/1112.0496381
6. Klyucharev P.G. Blochnye shifry, osnovannye na obobshchennykh kletochnykh avtomatakh,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2012, No 12. DOI: 10.7463/0113.0517543
7. Klyucharev P.G. Obespechenie kriptograficheskikh svoystv obobshchennykh kletochnykh avtomatov,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2012, No 3. URL: http://technomag.neicon.ru/doc/358973.html
8. Klyucharev P.G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostoyaniya obobshchennogo kletochnogo avtomata,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2012, No 1. URL: http://technomag.neicon.ru/doc/312834.html
9. Klyucharev P.G. O periode obobshchennykh kletochnykh avtomatov,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2012, No 2. URL: http://technomag.neicon.ru/doc/340943.html
10. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge functions. : Citeseer, 2007.
11. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak sponge function family main document. 2009. — 30 p.
12. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge-based pseudo-random number generators. : Springer, 2010. — P. 33-47.
13. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak. : Springer, 2013. — P. 313-314.
14. Klyucharev P.G. Kriptograficheskie khesh-funktsii, osnovannye na obobshchennykh kletochnykh avtomatakh,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2013, No 1. DOI: 10.7463/0113.0534640
15. Charles D.X., Goren E.Z., Lauter K.E. Families of Ramanujan graphs and quaternion algebras,Groups and symmetries: from Neolithic Scots to John McKay. 2009. T. 47. — C. P. 53-63.
16. Davidoff G.P., Sarnak P., Valette A. Elementary number theory, group theory, and Ramanujan graphs. — New York : Cambridge University Press, 2003. — 144 p.
17. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. 1988. — P. 261-277.
18. Sarnak P. Some applications of modular forms. — Cambridge ; New York : Cambridge University Press, 1990. — 111 p.
19. Klyucharev P.G. Ob ustoychivosti obobshchennykh kletochnykh avtomatov k nekotorym tipam kolliziy,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2014, No 9. — C. 194-202. DOI: 10.7463/0914.0727086
20. Klyucharev P.G. Proizvoditel'nost' i effektivnost' apparatnoy realizatsii potochnykh shifrov, osnovannykh na obobshchennykh kletochnykh atomatakh,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2013, No 10. — C. 299-314. DOI: 1013.0624722
21. Lebedev A.H. Elektronnaya podpis': novyy etap,Vestnik Moskovsko-go gorodskogo pedagogicheskogo universiteta: seriya Ekonomika. 2013, No 1. — C. 43-51.
22. Lebedev A.H. Sposob rassylki zashchishchennykh dannykh s regulirovani-em dostupa k otdel'nym ikh razdelam, Voprosy kiberbezopasnosti, 2015, No 5, pp. 70-72.
23. Bykov A.Yu. Algoritmy raspredeleniya resursov dlya zashchity informatsii mezhdu ob"ektami informatsionnoy sistemy na osnove igrovoy modeli i printsipa ravnoy zashchishchennosti ob"ektov,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2015, No 9. — C. 160-187. DOI: 10.7463/0915.0812283
24. Bykov A.Yu., Panfilov F.A., Khovrina A.V. Algoritm vybora klassov zashchishchennosti dlya ob"ektov raspredelennoy informatsionnoy sistemy i razmeshcheniya dannykh po ob"ektam na osnove privedeniya optimizatsionnoy zadachi k zadache teorii igr s neprotivopolozhnymi interesami,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2016. T. 1. — C. 90-107. DOI: 10.7463/0116.0830972
25. Bykov A.Yu., Artamonova A.Yu. Modifikatsiya metoda vektora spada dlya optimizatsionno-imitatsionnogo podkhoda k zadacham proektirovaniya sistem zashchity informatsii,Nauka i obrazovanie. Elektronnoe nauchno-tekhnicheskoe izdanie. 2015, No 1. — C. 158-175. DOI: 10.7463/0115.0754845