НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408
электронный научно-технический журнал

Криптографические хэш-функции, основанные на обобщенных клеточных автоматах

 # 01, январь 2013
DOI: 10.7463/0113.0534640

Ключарёв П. Г.

УДК 519.713; 004.056.55

Россия, МГТУ им. Н.Э. Баумана
pk.iu8@yandex.ru

1. Введение

Криптографические хэш-функции являются одним из важнейших классов криптографических алгоритмов. Они широко используются в задачах обеспечения информационной безопасности. Сейчас существует большое количество разнообразных хэш-функций. Обзор наиболее известных из них можно найти, например, в книге [23], а обзор современных методов построения хэш-функций — в работе [9].

Все возрастающие требования, предъявляемые к производительности, а также необходимость реализации в системах с малыми вычислительными ресурсами, приводят к необходимости разработки новых, высокопроизводительных, криптоалгоритмов. Данная работа посвящена применению подхода, основанного на использовании обобщенных клеточных автоматов, для синтеза криптографических хэш-функций. Использование этого подхода позволяет построить хэш-функции, которые могут быть с большой эффективностью реализованы аппаратно. Впервые он был предложен для создания поточных шифров в работах [7, 8], а затем развит автором в работах [1, 2, 3, 4, 6].

В работе [5] автором было предложено семейство псевдослучайных функций, основанных на обобщенных клеточных автоматов. Эти функции могут быть использованы в качестве основы для криптографических хэш-функций.

2. Постановка задачи

Задачей данной работы является построение семейства криптографических хэш-функций, основанных на обобщенных клеточных автоматах. Напомним, что хэш-функцией называется функция вида

$$H : B^* \to B^s, \qquad (1)$$

являющаяся однонаправленной и устойчивой к коллизиям первого и второго рода (здесь и далее, $B = \{0; 1\}$). За более подробной информацией о хэш-функциях можно рекомендовать обратиться, например, к работе [9].

3. Основные термины и определения

Используемое в качестве основы семейство псевдослучайных функций основано на обобщеных клеточных автоматах. В этом разделе мы приведем основные определения, в основном, следуя работе [5].

Назовем *обобщенным клеточным автоматом* ориентированный мультиграф $A = (V, E)$ (здесь $V = \{v_1, \ldots, v_N\}$ — множество вершин, E — мультимножество ребер). С каждой его вершиной v_i ассоциированы булева переменная m_i, называемая *ячейкой* и булева функция $f_i(x_1, \ldots, x_{d_i})$, называемая локальной функцией связи i-ой вершины. Для произвольной вершины v_i, входящие в нее ребра пронумерованы числами $1 \ldots d_i$.

Обобщенный клеточный автомат работает следующим образом. В начальный момент времени каждая ячейка памяти m_i, $i = 1 \ldots N$, имеет некоторое начальное значение $m_i(0)$. Далее работа осуществляется по шагам. На шаге с номером τ с помощью локальной функции связи вычисляются новые значения ячеек:

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

где $\eta(i, j)$ — номер вершины, из которой исходит ребро, входящее в вершину i и имеющее номер j.

Назовем *однородным обобщенным клеточным автоматом* обобщенный клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f. Степени захода вершин такого клеточного автомата, очевидно, одинаковы и равны d.

Назовем обобщенный клеточный автомат *неориентированным*, если для любого ребра (u, v) в его графе существует и ребро (v, u). Такой граф можно рассматривать как неориентированный, если заменить каждую пару ребер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$. Далее мы будем использовать только неориентированные однородные обобщенные клеточные автоматы, для краткости называя их просто обобщенными клеточными автоматами.

Некоторый набор ячеек клеточного автомата будем называть *выходом*. Ячейки не входящие в этот набор будем называть *скрытыми ячейками*, а соответствующие им вершины графа — *скрытыми вершинами*. Таким образом, длина выхода равна $N - t$ двоичных разрядов, где t — количество скрытых ячеек. *Выходной последовательностью* клеточного автомата A назовем функцию $F_A : B^N \times \mathbb{N} \to B^{N-t}$, аргументами которой является начальное заполнение и номер шага, а значением — значение выхода на этом шаге (здесь и далее $B = \{0; 1\}$).

Большое значение имеет выбор графа обобщенного клеточного автомата. В работе [5] обосновано, что в качестве графа клеточного автомата, применяемого для криптографических целей, хорошо подходят графы Рамануджана [15, 16, 19].

Рассмотрим отсортированный по убыванию спектр графа (то есть собственные числа его матрицы смежности [12]): $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. *Графом Рамануджана* называется граф, для которого справедливо неравенство $\lambda_2 \leq 2\sqrt{d-1}$, где d — степень графа.

Как и в работе [5], мы будем использовать семейство графов Любоцкого — Филипса — Сарнака $Y^{p,q}$ [18, 19, 22]. Построение графов из этого семейства производится следующим образом.

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

$$\begin{cases} p = 1 \pmod 4; \\ q = 1 \pmod 4; \\ p \neq q; \\ \left(\frac{p}{q}\right) = 1, \end{cases} \tag{3}$$

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

Построим неориентированный мультиграф $G = (V, E)$. Множеством вершин V является проективная прямая над полем $\mathbb{F}_q$, т.е., $V = \mathbb{F}_q \cup \{\infty\}$. Мультимножество ребер E состоит из всех пар (u, v), для которых выполняется

$$v = \begin{cases} \dfrac{(a_0 + ia_1)u + (a_2 + ia_3)}{(-a_2 + ia_3)u + (a_0 - ia_1)}, & (a_2 - ia_3)u \neq a_0 - ia_1, \;\; u \neq \infty; \\ \infty, & (a_2 - ia_3)u = a_0 - ia_1, \;\; u \neq \infty; \\ \dfrac{a_0 + ia_1}{-a_2 + ia_3}, & a_2 \neq ia_3, \;\; u = \infty; \\ \infty, & a_2 = ia_3, \;\; u = \infty, \end{cases} \tag{4}$$

для всех четверок $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, таких, что a_0 нечетное положительное, a_1, a_2, a_3 четные и выполняется условие:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p. \tag{5}$$

При этом, $i \in \mathbb{F}_q$, такое, что $i^2 + 1 = 0$.

Построенный таким образом граф является $(p+1)$-регулярным. В нем существуют кратные ребра и петли, от которых следует избавиться, причем так, чтобы граф остался регулярным. Алгоритмы для этого приведены в работе [5].

Важным является правильный выбор локальной функции связи обобщенного клеточного автомата. Требования к такой функции сформулированы автором в работе [5].

Мы будем использовать функции из семейства, построенного автором в работе [4]. Так, в случае нечетного числа переменных используется функция:

$$g_1(u, x_1, y_1, \ldots, x_\nu, y_\nu) = \bigoplus_{i=1}^{\nu} x_i y_i \oplus s_1(x_1, \ldots, x_\nu) \oplus u, \tag{6}$$

где $s_1(x_1, \ldots, x_\nu)$ — произвольная булева функция, причем $\nu + t_1 = 1 \pmod 2$, где t_1 — число ненулевых коэффициентов алгебраической нормальной формы функции s_1, для которой $s_1(0, \ldots, 0) = 1$.

В случае четного числа переменных используется функция

$$\begin{aligned} g_2(v, u, x_1, y_1, \ldots, x_\nu, y_\nu) = \\ = (1 \oplus v)(\beta_1(x_1, y_1, \ldots, x_\nu, y_\nu) \oplus u) \oplus v(\beta_3(x_1, y_1, \ldots, x_\nu, y_\nu) \oplus u) = \\ = \bigoplus_{i=1}^{\nu} x_i y_i \oplus s_1(x_1, \ldots, x_\nu) \oplus v(s_1(x_1, \ldots, x_\nu) \oplus s_3(x_1, \ldots, x_\nu)) \oplus u, \end{aligned} \quad (7)$$

где $s_1(x_1, \ldots, x_\nu)$ и $s_3(x_1, \ldots, x_\nu)$ — произвольные булевы функции, причем $\nu + t_3 = 1 \pmod 2$, где t_3 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_3 и при этом $s_1(0, \ldots, 0) = 1$.

Примером такой функции может служить функция

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_3x_5 \oplus x_3x_4 \oplus x_5x_6 \oplus x_3x_5 \oplus x_1x_5 \oplus x_1 \oplus x_2 \oplus 1. \quad (8)$$

4. Построение семейства хэш-функций

В этом разделе вводится семейство хэш-функций, которое является основным результатом настоящей работы.

В работе [5] автором предложен метод синтеза псевдослучайных функций вида $S_c : B^k \times B^n \to B^m$. Эти функции основываются на обобщенных клеточных автоматах и могут быть заданы формулой

$$S_c^A(key, x) = \mathrm{pr}_m(F_A(x \parallel key \parallel c, r)), \quad (9)$$

где $x \parallel y$ — конкатенация x и y; r — число шагов клеточного автомата; $\mathrm{pr}_m : B^* \to B^m$ — функция, возвращающая младшие m элементов аргумента; A — обобщенный клеточный автомат; $c \in B^t$ — некоторая константа, вес которой близок к значению $\left[\frac{t}{2}\right]$.

Константа c в формуле (9) необходима для улучшения лавинного эффекта и обеспечения отсутствия неподвижных точек. Число шагов клеточного автомата r и число скрытых вершин t выбираются так, чтобы функцию нельзя было отличить от случайной при помощи статистических тестов.

В работе [5] автором обосновано и подтверждено экспериментально, что такие функции неотличимы от случайных при правильном выборе параметров (числа шагов клеточного автомата r и числа скрытых вершин t).

Известен целый ряд способов, позволяющих построить хэш-функцию из псевдослучайной однонаправленной функции. Например, можно указать схему Меркля — Дамгарда [14, 21], которая часто используется на практике (например, в хэш-функциях MD5 и SHA-1), а также разнообразные ее варианты, такие как Wide pipe, Double pipe [20, 25], 3C [13]

и др. Еще одной известной схемой является так называемая Губка (Sponge) [24], используемая в алгоритме Keccak [17], выигравшим в конкурсе SHA-3 и ставшим новым стандартом США. Эти схемы, по-видимому, можно использовать для создания хэш-функций на основе однонаправленной функции (9). Однако в связи с тем, что вопрос о лавинном эффекте по начальному заполнению в обобщенном клеточном автомате при большом числе итераций является недостаточно исследованным, применение этих схем недостаточно обосновано. Поэтому мы будем использовать схему построения хэш-функций, не связанную с большим количеством итераций — вариант древовидной схемы, являющийся дальнейшим развитием схемы, предложенной в [10] и схемы PMAC для ключевых хэш-функций [11].

Схема, предложенная в [10], описывается формулой

$$\bigodot_{i=1}^{n} h(i \parallel x_i), \tag{10}$$

где h — псевдослучайная функция, x_i — блок сообщения, а $\odot$ — некоторая групповая операция.

Преимуществом такой схемы является возможность получения некоторых теоретических результатов о стойкости. В частности, в работе [10] доказана теорема о стойкости данной схемы при использовании умножения в конечном поле в качестве групповой операции, в предположении о псевдослучайности h и о высокой сложности задачи о дискретном логарифме.

Недостатками этой схемы является то, что далеко не всякая групповая операция подходит — например, при использовании сложения в конечном поле, схема оказывается неустойчивой к коллизиям. Те операции, которые подходят, имеют относительно высокую сложность. При этом, стойкость в такой схеме доказана в предположении высокой сложности задачи о дискретном логарифме, что, вообще говоря, не доказано.

Похожая схема используется и в алгоритме PMAC [11]. Однако этот алгоритм представляет собой ключевую хэш-функцию, для которой свойства однонаправленности и стойкости к коллизиям обеспечиваются только в предположении, что противнику не известен ключ. Поэтому схема, используемая в алгоритме PMAC, напрямую не применима для синтеза хэш-функций.

Мы воспользуемся тем, что функция S_c^A представляет собой семейство однонаправленных псевдослучайных функций и сформируем хэш-функцию следующим образом.

Разобьем сообщение X на блоки длины n: $X = (x_1, x_2, \ldots, x_\eta)$ (если сообщение не кратно дине блока, дополним его до длины блока нулями). Хэш, имеющий длину s, будем вычислять по формуле:

$$H(X) = \mathrm{pr}_s\left(S_{c_2}^A\left(c_3, \bigoplus_{i=1}^{\eta} S_{c_1}^A(i, x_i)\right)\right), \tag{11}$$

где $c_1, c_2 \in B^t$ — различные константы, вес которых близок к значению $[t/2]$; $c_3 \in B^k$ — константа, вес которой близок к значению $[k/2]$; t — число скрытых вершин графа.

Обобщенный клеточный автомат A должен иметь граф, построенный в соответствии с приведенными выше соображениями. Число скрытых вершин графа должно удовлетворять условию: $t \geq \frac{n+k}{2}$. Значение параметра k следует выбирать таким, чтобы максимальный номер блока помещался в k разрядов. Например, можно рекомендовать $k = 64$. Значение параметра m функции (9) должен быть не меньше длины хэша s.

Такая схема отличается от схемы, описанной в [10] тем, что в качестве комбинирующей функции используется функция $S^A_{c_2}$ от поразрядной суммы по модулю два, а не некоторая групповая операция. От алгоритма PMAC схема отличается тем, что вместо функции зашифрования симметричного шифра используется функция S^A_c, а с каждым блоком конкатенируется его номер (в PMAC используется сложение с некоторой функцией, зависящей от номера блока). Эти различия, очевидно, приводят к тому, что предложенная схема имеет существенно меньшие схемную сложность и глубину. Учитывая, что функция S^A_c, является псевдослучайной, можно утверждать, что такая схема безопасна.

Отметим, что выражением (11) задано целое семейство хэш-функций. Конкретная хэш-функция определяется набором следующих параметров:

- число вершин графа;
- степень графа;
- локальная функция связи;
- константы c_1, c_2 и c_3;
- число скрытых вершин графа t;
- длина блока n;
- параметр m;
- число шагов клеточного автомата r;
- длина хэша s.

Все эти параметры должны выбираться в соответствии с вышеприведенными условиями, такими как (3), (6), (7) и др.

Преимуществом предложенного семейства хэш-функций является возможность параллельного вычисления функции $S^A_{c_1}$ от различных блоков, что, в сочетании с эффективностью аппаратной реализации обобщенных клеточных автоматов, делает возможной весьма эффективную аппаратную реализацию хэш-функции.

5. Криптографическая стойкость

Согласно [5], функция S^A_c является псевдослучайной. Также она имеет высокую нелинейность, а каждый двоичный разряд ее выхода зависит от всех разрядов входа. Кроме того, как показано автором в работе [6], задача о восстановлении предыдущего состояния обобщенного клеточного автомата, в общем случае, является NP-полной. Все это позволяет рассматривать эту функцию как однонаправленную и устойчивую к коллизиям.

Предложенная хэш-функция использует древовидную схему, основанную на функции S_c^A. Каждый разряд выхода хэш-функции сложным образом нелинейно зависит от всех разрядов сообщения. Различные виды криптоанализа, которые могут быть использованы для обращения хэш-функции или построения коллизий, применить затруднительно, в связи с большой длиной входа функции S. Исходя из вышесказанного можно утверждать, что предложенная хэш-функция является криптостойкой.

Кроме того, стойкость предложенной хэш-функции может быть усилена методом, аналогичным известному [21] методу усиления схемы Меркля — Дамгарда, который заключается в том, что сообщение конкатенируют с дополнительной информацией, включающей в себя длину сообщения.

6. Заключение

В статье предложено новое семейство криптографических хэш-функций, основанное на использовании обобщенных клеточных автоматов. Дальнейшие исследования направлены, в частности, на анализ предложенного семейства и дальнейшее обоснование его криптографической стойкости.

Работа выполнена при финансовой поддержке РФФИ (грант № 12-07-31012).

Список литературы

1. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // *Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн.* 2011. № 10. Режим доступа: http://technomag.edu.ru/doc/241308.html (дата обращения 19.12.2012).
2. Ключарёв П.Г. О вычислительной сложности некоторых задач на обобщенных клеточных автоматах // *Безопасность информационных технологий*. 2012. № 1. Режим доступа: http://www.pvti.ru/data/file/bit/2012_1/part_4.pdf (дата обращения 19.12.2012).
3. Ключарёв П.Г. О периоде обобщенных клеточных автоматов // *Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн.* 2012. № 2. Режим доступа: http://technomag.edu.ru/doc/340943.html (дата обращения 19.12.2012).
4. Ключарёв П. Г. Обеспечение криптографических свойств обобщенных клеточных автоматов // *Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн.* 2012. № 3.Режим доступа: http://technomag.edu.ru/doc/358973.html (дата обращения 19.12.2012).
5. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщенных клеточных автоматов // *Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн.* 2012. № 10. DOI: 10.7463/1112.0496381.
6. Ключарёв П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // *Наука и образование. МГТУ им. Н.Э. Баумана. Электрон.*

журн. 2012. № 1. Режим доступа: http://technomag.edu.ru/doc/312834.html (дата обращения 19.12.2012).

7. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // *Прикладная дискретная математика*. 2010. № 2. С. 34–41.
8. Сухинин Б.М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // *Вестник МГТУ им. Н.Э. Баумана. Серия: Приборостроение*. 2011. № 2. С. 68–76.
9. Al-Kuwari S., Davenport J., Bradford R. Cryptographic hash functions: recent design trends and security notions. The University of Bath, 2010. Available at: http://opus.bath.ac.uk/20815, accessed 10.01.2013.
10. Bellare M., Micciancio D. A new paradigm for collision-free hashing: Incrementality at reduced cost // *Advances in Cryptology – EUROCRYPT'97*. Springer Berlin Heidelberg, 1997. P. 163–192. DOI: 10.1007/3-540-69053-0_13 (Lecture Notes in Computer Science; vol. 1233).
11. Black J., Rogaway P. A block-cipher mode of operation for parallelizable message authentication // *Advances in Cryptology – EUROCRYPT 2002*. Springer Berlin Heidelberg. 2002. P. 384–397. DOI: 10.1007/3-540-46035-7_25 (Lecture Notes in Computer Science; vol. 2332).
12. Chung F. Spectral graph theory. American Mathematical Society, 1997. 207 p. (CBMS Regional Conference Series in Mathematics; No. 92).
13. Constructing secure hash functions by enhancing merkle-damgård construction / P. Gauravaram, W. Millan, E. Dawson, K. Viswanathan // Information Security and Privacy. Springer Berlin Heidelberg. 2006. P. 407–420. DOI: 10.1007/11780656_34 (Lecture Notes in Computer Science; vol. 1233).
14. Damgård I. A design principle for hash functions // *Advances in Cryptology – CRYPTO'89 Proceedings*. Springer New York. 1990. P. 416–427. DOI: 10.1007/0-387-34805-0_39 (Lecture Notes in Computer Science; vol. 435).
15. Davidoff G., Sarnak P., Valette A. Elementary number theory, group theory and Ramanujan graphs. Cambridge: Cambridge University Press, 2003. 154 p. (London Mathematical Society Student Texts; vol. 55).
16. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // *Bulletin of the American Mathematical Society*. 2006. Vol. 43, no. 4. P. 439–562.
17. Bertoni G., Daemen J., Peeters M., Van Assche G. Keccak specifications. Submission to NIST (Round 2). 2009. Available at: http://keccak.noekeon.org/Keccak-specifications-2.pdf, accessed 19.12.2012.

18. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the Ramanujan conjectures // STOC′86 Proceedings of the eighteenth annual ACM symposium on Theory of computing. New York, NY, ACM, 1986. P. 240–246. DOI: 10.1145/12130.12154.

19. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // *Combinatorica*. 1988. Vol. 8, no. 3. P. 261–277. DOI: 10.1007/BF02126799.

20. Lucks S. A failure-friendly design principle for hash functions // *Advances in Cryptology – ASIACRYPT 2005*. Springer Berlin Heidelberg. 2005. P. 474–494. DOI: 10.1007/11593447_26 (Lecture Notes in Computer Science; vol. 3788).

21. Merkle R. One way hash functions and DES // *Advances in Cryptology – CRYPTO′89 Proceedings*. Springer New York. 1990. P. 428–446. DOI: 10.1007/0-387-34805-0_40 (Lecture Notes in Computer Science; vol. 435).

22. Sarnak P. Some applications of modular forms. Cambridge: Cambridge University Press, 1990. (Cambridge Tracts in Mathematics; vol. 99).

23. Schneier B., Sutherland P. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, Inc., 1995.

24. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge functions // ECRYPT Hash Workshop 2007. May 2007.

25. Yasuda K. A double-piped mode of operation for macs, prfs and pros: Security beyond the birthday barrier // *Advances in Cryptology – EUROCRYPT 2009*. Springer Berlin Heidelberg. 2009. P. 242–259. DOI: 10.1007/978-3-642-01001-9_14 (Lecture Notes in Computer Science; vol. 5479).

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

EL № FS77 - 48211. №0421200025. ISSN 1994-0408

electronic scientific and technical journal

Cryptographic hash functions based on generalized cellular automata

 # 01, January 2013

DOI: 10.7463/0113.0534640

Klyucharev P. G.

Russia, Bauman Moscow State Technical University

pk.iu8@yandex.ru

In this paper the author introduces a family of cryptographic hash functions based on using generalized cellular automata. The structure of the proposed functions is a dendrogram which includes a one-way pseudorandom function built with the use of a generalized cellular automaton whose graph is a Ramanujan graph. The local link function of the cellular automata is a balanced function with large nonlinearity and some additional properties. The family of proposed hash functions may find practical application in a number of information security tasks, including authentication, integrity, digital signature, etc.

References

1. Kliucharev P.G. Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluchainykh posledovatel'nostei [Cellular automations based on Ramanujan graphs in the field of the generation of pseudorandom sequences]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2011, no. 10. Available at: http://technomag.edu.ru/doc/241308.html, accessed 19.12.2012.
2. Kliucharev P.G. O vychislitel'noi slozhnosti nekotorykh zadach na obobshchennykh kletochnykh avtomatakh [On the computational complexity of some problems on generalized cellular automata]. *Bezopasnost' informatsionnykhtekhnologii* [Security of information technologies], 2012, no. 1. Available at: http://www.pvti.ru/data/file/bit/2012_1/part_4.pdf, accessed 19.12.2012.
3. Kliucharev P.G. O periode obobshchennykh kletochnykh avtomatov [About the period of generalized cellular automatons]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 2. Available at: http://technomag.edu.ru/doc/340943.html, accessed 19.12.2012.

4. Kliucharev P.G. Obespechenie kriptograficheskikh svoistv obobshchennykh kletochnykh avtomatov [On cryptographic properties of generalized cellular automatons]. *Nauka i brazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 3. Available at: http://technomag.edu.ru/doc/358973.html, accessed 19.12.2012.
5. Kliucharev P.G. Postroenie psevdosluchainykh funktsii na osnove obobshchennykh kletochnykh avtomatov [Construction of pseudorandom functions based on generalized cellular automata]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 10. DOI: 10.7463/1112.0496381.
6. Kliucharev P.G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostoianiia obobshchennogo kletochnogo avtomata [NP-hard of step backward problem in generalized cellular automaton]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 1. Available at: http://technomag.edu.ru/doc/312834.html, accessed 19.12.2012.
7. Sukhinin B.M. Vysokoskorostnye generatory psevdosluchainykh posledovatel'nostei na osnove kletochnykh avtomatov [High-speed generators of pseudorandom sequences based on cellular automata]. *Prikladnaia diskretnaia matematika*, 2010, no. 2, pp. 34–41.
8. Sukhinin B.M. O nekotorykh svoistvakh kletochnykh avtomatov i ikh primenenii v strukture generatorov psevdosluchainykh posledovatel'nostei [Some properties of cellular automata and their application in the structure of pseudorandom sequences generators]. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie* [Bulletin of the Bauman MSTU. Ser. Instrument Engineering], 2011, no. 2, pp. 68–76.
9. Al-Kuwari S., Davenport J., Bradford R. *Cryptographic hash functions: recent design trends and security notions*. The University of Bath, 2010. Available at: http://opus.bath.ac.uk/20815, accessed 10.01.2013.
10. Bellare M., Micciancio D. A new paradigm for collision-free hashing: Incrementality at reduced cost. *Advances in Cryptology – EUROCRYPT'97*. Springer Berlin Heidelberg, 1997, pp. 163-192. DOI:10.1007/3-540-69053-0_13 (*Lecture Notes in Computer Science*, vol. 1233).
11. Black J., Rogaway P. A block-cipher mode of operation for parallelizable message authentication. *Advances in Cryptology – EUROCRYPT 2002*. Springer Berlin Heidelberg, 2002, pp. 384-397. DOI: 10.1007/3-540-46035-7_25 (*Lecture Notes in Computer Science*, vol. 2332).
12. Chung F. *Spectral graph theory*. American Mathematical Society, 1997. 207 p. (*CBMS Regional Conference Series in Mathematics*, no. 92).
13. Gauravaram P., Millan W., Dawson E., Viswanathan K. Constructing secure hash functions by enhancing Merkle-Damgård construction. *Information Security and Privacy*. Springer Berlin Heidelberg, 2006, pp. 407–420. DOI: 10.1007/11780656_34 (*Lecture Notes in Computer Science*, vol. 1233).

14. Damgård I. A design principle for hash functions. *Advances in Cryptology – CRYPTO' 89 Proceedings*. Springer New York, 1990, pp. 416–427. DOI: 10.1007/0-387-34805-0_39 (*Lecture Notes in Computer Science*, vol. 435).

15. Davidoff G., Sarnak P., Valette A. *Elementary number theory, group theory and Ramanujan graphs*. Cambridge, Cambridge University Press, 2003. 154 p. (*London Mathematical Society Student Texts*, vol. 55).

16. Hoory S., Linial N., Wigderson A. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 2006, vol. 43, no. 4, pp. 439–562.

17. Bertoni G., Daemen J., Peeters M., Van Assche G. *Keccak specifications*. Submission to NIST (Round 2). 2009. Available at: http://keccak.noekeon.org/Keccak-specifications-2.pdf, accessed 19.12.2012.

18. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the ramanujan conjectures. *STOC '86 Proceedings of the eighteenth annual ACM symposiumon Theory of computing*. New York, NY, ACM, 1986, pp. 240-246. DOI: 10.1145/12130.12154.

19. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277. DOI: 10.1007/BF02126799.

20. Lucks S. A failure-friendly design principle for hash functions. *Advances in Cryptology – ASIACRYPT 2005*. Springer Berlin Heidelberg, 2005, pp. 474–494. DOI: 10.1007/11593447_26 (*Lecture Notes in Computer Science*, vol. 3788).

21. Merkle R. One way hash functions and DES. *Advances in Cryptology – CRYPTO' 89 Proceedings*. Springer New York, 1990, pp. 428–446. DOI: 10.1007/0-387-34805-0_40 (*Lecture Notes in Computer Science*, vol. 435).

22. Sarnak P. *Some applications of modular forms*. Cambridge, Cambridge University Press, 1990. (*Cambridge Tracts in Mathematics*, vol. 99).

23. Schneier B., Sutherland P. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., 1995.

24. Bertoni G., Daemen J., Peeters M., Van Assche G. Sponge functions. *ECRYPT Hash Workshop 2007*. May 2007.

25. Yasuda K. A double-piped mode of operation for macs, prfs and pros: Security beyond the birthday barrier. *Advances in Cryptology – EUROCRYPT 2009*. Springer Berlin Heidelberg, 2009, pp. 242–259. DOI: 10.1007/978-3-642-01001-9_14 (*Lecture Notes in Computer Science*, vol. 5479).