Наука и Образование
МГТУ им. Н.Э. Баумана
Сетевое научное издание
ISSN 1994-0408

Ссылка на статью:
// Наука и Образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 11. С. 142–152.
DOI: **10.7463/1116.0849590**
Представлена в редакцию: 9.11.2016
Исправлена: 24.11.2016

УДК 519.713+004.056.55

Построение алгоритмов выработки имитовставок на основе обобщенных клеточных автоматов

Ключарёв П. Г.[1,*]
[*]pk.iu8@yandex.ru
[1]МГТУ им. Н.Э. Баумана, Москва, Россия

В работе предложен метод построения алгоритмов выработки имитовставок, основанных на обобщенных клеточных автоматах. Такой автомат используется для обработки сообщения. Раз в несколько шагов к внутреннему состоянию автомата подмешивается очередной блок сообщения. Ключ используется в начальном заполнении автомата, а также в начальном заполнении линейного регистра сдвига с обратной связью, выход которого подмешивается к внутреннему состоянию автомата на каждом шаге. После окончания обработки сообщения, клеточный автомат совершает определенное число шагов, после чего с него снимается значение имитовставки. Проведено статистическое тестирование алгоритмов, полученных с помощью разработанного метода.

Ключевые слова: криптография; клеточный автомат; имитовставка

Введение

Важным классом криптографических алгоритмов являются алгоритмы выработки имитовставок (англ. Message Authentication Code, MAC). Такие алгоритмы предназначены для обеспечения целостности сообщений и аутентификации их источника. Для этого к сообщению добавляется вырабатываемая таким алгоритмом имитовставка — двоичный набор, зависящий от сообщения и от секретного ключа.

Алгоритмам выработки имитовставок посвящено большое количество различных источников. Хороший обзор литературы по методам их построения можно найти в работе [1].

Все возрастающие требования к пропускной способности и защищенности систем и сетей связи приводят к необходимости разработки новых криптографических алгоритмов, обладающих высокой производительностью. В связи с этим, большой интерес представляет использование обобщенных клеточных автоматов. Этот подход был исследован автором в ряде работ, в том числе [2, 3, 4, 5] и др. Криптоалгоритмы, основанные на обобщенных клеточных автоматах, показывают очень высокую производительность при аппаратной реализации (например, на программируемых логических интегральных схемах).

1. Постановка задачи

Имитовставка — это вектор $y \in \{0,1\}^q$ фиксированного размера, вычисляемый для сообщения $M \in \{0,1\}^*$ на некотором ключе $key \in \{0,1\}^{|key|}$ (здесь $|key|$ — длина ключа) с помощью эффективного алгоритма: $y = MAC_{key}(M)$. При этом выполняются следующие свойства:

• без знания ключа, вычислительно сложно найти такое $M' \neq M$, что $MAC_{key}(M) = MAC_{key}(M')$;

• по любому числу пар $(y_i, M_i) : y_i = MAC_{key}(M_i)$ вычислительно сложно найти ключ key;

• без знания ключа вычислительно сложно найти имитовставку для данного сообщения.

Основной задачей данной работы является разработка метода синтеза алгоритмов выработки имитовставок, основанных на обобщенных клеточных автоматах.

2. Обобщенные клеточные автоматы

Обобщенные клеточные автоматы — весьма перспективный криптографический примитив. Здесь мы кратко изложим некоторые факты о них из предыдущих работ автора.

Назовем *обобщенным клеточным автоматом* ориентированный мультиграф $A = (V, E)$ (здесь $V = \{v_1, \ldots, v_N\}$ — множество вершин мультиграфа, E — мультимножество ребер мультиграфа). С каждой его вершиной v_i ассоциированы:

• булева переменная m_i, называемая *ячейкой*;

• булева функция $f_i(x_1, \ldots, x_{d_i})$, называемая 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.

Обобщенный клеточный автомат работает следующим образом. Перед началом работы ячейки памяти $m_i, i = 1, \ldots, N$, имеют некоторые начальные значения $m_i(0)$. Далее автомат работает по шагам. На шаге с номером t с помощью локальной функции связи вычисляются новые значения ячеек:

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

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

Заполнением (*внутренним состоянием*) клеточного автомата на шаге t будем называть набор значений ячеек $M(t) = (m_1(t), m_2(t), \ldots, m_N(t))$.

Назовем *однородным обобщенным клеточным автоматом* обобщенный клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f, т.е. для любого $i \in \{1, \ldots, N\}$ выполняется $f_i = f$. В таком автомате степени захода вершин одинаковы: $d_1 = d_2 = \ldots = d_N = d$.

Назовем обобщенный 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 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.

Большое значение имеет выбор графа обобщенного клеточного автомата. В работе [6] показано, что в качестве графа клеточного автомата, применяемого для криптографических целей, хорошо подходят графы Рамануджана [7, 8, 9].

Рассмотрим отсортированный по убыванию спектр графа (т.е. набор собственных чисел его матрицы смежности): $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.

Графом Рамануджана называется граф, для которого справедливо неравенство

$$\lambda_2 \leq 2\sqrt{d-1}, \tag{2}$$

где d — степень графа.

По-видимому, наиболее подходящим семейством графов Рамануджана, является так называемое семейство графов Любоцкого — Филипса — Сарнака Y [9, 10, 11]. Мы не будем подробно здесь останавливаться на синтезе таких графов, однако отметим, что для криптографических применений должно выполняться $d \geq 4$.

Очень важным является правильный выбор локальной функции связи обобщенного клеточного автомата. Требования к такой функции сформулированы автором в работе [4] и [6]:

1) функция должна быть равновесной;

2) алгебраическая нормальная форма функции должна содержать хотя бы одну переменную в первой степени;

3) функция должна быть шефферовой;

4) расстояние между данной функцией и множеством аффинных функций должны быть близким к максимальному.

Методы построения таких функций разработаны автором в работе [4]. Здесь мы не будем на них подробно останавливаться.

Также важна нумерация ребер графа. Этот вопрос исследовался автором в работе [12], где был разработан способ нумерации ребер, обеспечивающий стойкость к коллизиям.

3. Построение алгоритмов выработки имитовставок

В этом разделе предлагается метод построения алгоритмов выработки имитовставок. Метод состоит в использовании следующей схемы построения этих алгоритмов. Итак, пусть вычисляется имитовставка от сообщения M на ключе key. При этом сообщение разбито на блоки длины n. Работа алгоритма состоит из двух этапов:

• этап абсорбции;

• этап вычисления результата.

На этапе абсорбции будем использовать обобщенный клеточный автомат, к внутреннему состоянию которого раз в t_1 шагов (для некоторого t_1) подмешивается очередной блок сообщения. При этом, начальным заполнением автомата является ключ, с которым конкатенирована некоторая константа: $key||c_1$.

Для обеспечения зависимости выхода от всех разрядов ключа используется задающая последовательность, вырабатываемая линейным регистром сдвига с обратной связью, длина которого строго больше длины ключа, а многочлен обратной связи выбран таким образом, чтобы длина периода регистра была максимальной (т.е. $2^L - 1$, где L — длина регистра). В качестве начального заполнения регистра сдвига с обратной связью также используется ключ, конкатенированный с некоторой константой: $key||c_2$.

Обозначим преобразование, выполняемое обобщенным клеточным автоматом над его внутреннем состоянием на одном шаге, как $G : \{0,1\}^N \to \{0,1\}^N$. Тогда внутреннее состояние автомата будет обновляться в соответствии с формулой

$$(m_1(i), m_2(i), \ldots, m_N(i)) =$$

$$= \begin{cases} G(m_1(i-1),\ldots,m_{r-1}(i-1),m_r(i-1)\oplus\xi_i,m_{r+1}(i-1),\ldots \\ \qquad\qquad \ldots,m_N(i-1)), \quad \text{если } i\not\equiv 0 \pmod{t_1}; \\ G(m_1(i-1),\ldots,m_{\mu-1}(i-1),m_\mu(i-1)\oplus M_{\left(\frac{i}{t_1}-1\right)_{n+1}},\ldots \\ \qquad\qquad \ldots,m_{\mu+n-1}(i-1)\oplus M_{\left(\frac{i}{t_1}-1\right)_{n+n}},m_{\mu+n}(i-1),\ldots \\ \qquad \ldots,m_{r-1}(i-1),m_r(i-1)\oplus\xi_i,m_{r+1}(i-1),\ldots,m_N(i-1)), \quad \text{если } i\equiv 0 \pmod{t_1}. \end{cases}$$

Здесь:

t_1 — число шагов автомата между примешиванием очередного блока сообщения;

M_j — j-й разряд сообщения;

n — длина блока сообщения;

N — число вершин графа обобщенного клеточного автомата;

$\mu,\ \mu+1,\ \ldots,\ \mu+n-1$ — номера ячеек обобщенного клеточного автомата,
к которым подмешиваются разряды сообщения;

$\{\xi_i\}$ — выходная последовательность линейного регистра сдвига с обратной связью;

r — номер ячейки, к которой прибавляются элементы последовательности $\{\xi_i\}$;

$i = 1,\ 2,\ \ldots$ — номер шага;

$(m_1(i),\ m_2(i),\ \ldots,\ m_N(i))$ — внутреннее состояние обобщенного клеточного автомата на шаге i;

$(m_1(0),\ m_2(0),\ \ldots,\ m_N(0))$ — начальное заполнение обобщенного клеточного автомата.

Линейный регистр сдвига с обратной связью выбирается таким образом, чтобы его характеристический многочлен был примитивным над полем $GF(2)$. Как известно из теории таких регистров [13], это гарантирует максимальный период выходной последовательности.

Параметр r выбирается таким образом, чтобы $r \notin \{\mu,\ \mu+1,\ \ldots,\ \mu+n-1\}$.

После того, как все сообщение будет обработано, этап абсорбирования завершается. Далее начинается этап вычисления результата, на котором клеточный автомат продолжает работать, при этом каждые t_2 шагов с некоторых разрядов его внутреннего состояния (например, разрядов с индексами $\mu, \ldots, \mu+n-1$) снимается необходимое количество двоичных разрядов имитовставки. После того, как будет снято необходимое их количество, работа алгоритма завершается.

Параметр t_1 должен быть не меньше диаметра графа, с тем, чтобы обеспечить зависимость каждой ячейки от каждого разряда всех блоков сообщения. Параметр t_2 должен в несколько раз превосходить параметр t_1, чтобы обеспечить сложный вид зависимости выхода от сообщения. Константы c_1 и c_2 выбираются близкими к равновесным.

В качестве графа обобщенного клеточного автомата используется граф Рамануджана, не содержащий петель и кратных ребер. Выбор именно графа Рамануджана обусловлен в частности тем, что диаметр таких графов равен $O(\log N)$, а также их сложной структурой. Эти свойства позволяют значительно уменьшить параметры t_1 и t_2, необходимые для обеспечения криптостойкости. Более подробно это описано в работе [5].

Как уже упоминалось выше, хорошим выбором графа являются графы Любоцкого-Филипса-Сарнака. Однако они могут содержать кратные ребра и петли. В этом случае такой граф можно модифицировать в соответствии со следующей процедурой. Сначала обработаем кратные ребра следующим образом. Рассмотрим две пары кратных ребер: кратные ребра (u_1, v_1) и кратные ребра (u_2, v_2). Удалим по одному ребру каждой пары из графа и добавим в граф ребра (u_1, u_2) и (v_1, v_2). Таким способом можно обработать все кратные ребра.

Петли обработаем следующим образом. Пусть у вершин u_1, u_2, $\ldots$, u_t имеются петли. Удалим эти петли из графа и добавим в граф ребра (u_1, u_2), (u_2, u_3), $\ldots$, (u_{t-1}, u_t) (если при этом появятся кратные ребра, вершины u_1, u_2, $\ldots$, u_t следует переупорядочить так, чтобы кратных ребер не появлялось). Рассмотренная процедура, очевидно, не нарушит регулярность графа и не уменьшит коэффициенты реберного и вершинного расширения.

Локальная функция связи должна удовлетворять условиям, описанным в предыдущем разделе. Как следует из результатов, полученных в работе [12], для обеспечения устойчивости к коллизиям, при использовании локальной функции связи, линейной по аргументу k, следует, чтобы ребра, имеющие номер k относительно каких-либо вершин вместе с этими вершинами образовывали 2-фактор графа обобщенного клеточного автомата.

4. Статистическое тестирование

Статистическое тестирование проводилось с помощью набора статистических тестов NIST Statistical Test Suite [14, 15]. Для каждого набора параметров генерировалось 300 случайных пар (α, β), где α — начальное значение блока, β — значение ключа. Для каждой пары

вычислялась конкатенация имитовставок: $MAC_\beta(\alpha)||MAC_\beta(\alpha+1)||\ldots||MAC_\beta(\alpha+4095)$. В результате получалось 300 последовательностей длиной 1048576 двоичных разрядов. Они тестировались с помощью NIST Statistical Test Suite. Использовались следующие постоянные параметры:

- длина блока: 256 двоичных разрядов;
- длина имитовставки: 256 двоичных разрядов;
- граф Любоцкого — Филипса — Сарнака: модифицированный;
- число вершин графа: 1022;
- степень графа: 6;
- диаметр графа: 7;
- локальная функция связи:

$$f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_3x_5 \oplus x_3x_4 \oplus x_5x_6 \oplus x_3x_5 \oplus x_1x_5 \oplus x_1 \oplus x_2 \oplus 1. \qquad (3)$$

Использовались все возможные наборы параметров из следующих:

- длина ключа: 128, 256 двоичных разрядов;
- $t_1 = 8,\ 12,\ 16$;
- $t_2 = 16,\ 32,\ 64$.

Итого тесты проводились для 18 наборов параметров.

Локальная функция связи (3) построена как функция из предложенного в работе [4] семейства функций четного числа переменных:

$$g_2(v,u,x_1,y_1,\ldots,x_{\frac{d}{2}-1},y_{\frac{d}{2}-1}) = \\ = \bigoplus_{i=1}^{\frac{d}{2}-1} x_iy_i \oplus s_1(x_1,\ldots,x_{\frac{d}{2}-1}) \oplus v(s_1(x_1,\ldots,x_{\frac{d}{2}-1}) \oplus s_3(x_1,\ldots,x_{\frac{d}{2}-1})) \oplus u,$$

где $s_1(x_1,\ldots,x_{\frac{d}{2}-1})$ и $s_3(x_1,\ldots,x_{\frac{d}{2}-1})$ — произвольные булевы функции, причем выполняется $(\frac{d}{2}-1)+\tau_3 = 1 \pmod 2$, где τ_3 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_3 и, при этом, свободный член АНФ функции s_1 равен 1.

Модификация графа Любоцкого — Филипса — Сарнака заключается в преобразовании его из мультиграфа в обычный граф с помощью метода, приведенного в разделе 3.

При задании линейного регистра сдвига с обратной связью, для длины ключа в 128 двоичных разрядов использовался характеристический многочлен $x^{145}+x^{52}+1$, а для длины ключа в 256 двоичных разрядов использовался характеристический многочлен $x^{297}+x^5+1$. Оба этих многочлена являются примитивными над полем $GF(2)$ [16].

По результатам тестирования, все полученные последовательности для всех протестированных наборов параметров, прошли полный набор статистических тестов из NIST Statistical Test Suite, что подтверждает хорошие статистические свойства криптографических алгоритмов, построенных с помощью предложенного метода.

5. О криптостойкости

Криптографические свойства обобщенных клеточных автоматов исследовались автором в целом ряде работ. Так, в статье [4] показано, что функция, вычисляемая обобщенным клеточным автоматом с правильно выбранными параметрами, за достаточное число шагов, неотличима от псевдослучайной. Свойства обобщенных клеточных автоматов, использование графа Рамануджана с малым диаметром и использование локальной функции связи с высокой нелинейностью дают возможность утверждать, что каждый разряд имитовставки сложным образом нелинейно зависит от всех разрядов сообщения и всех разрядов ключа. Кроме того, как показано в работе [2], в общем случае, задача о восстановлении предыдущего состояния обобщенного клеточного автомата является NP-трудной. На базе обобщенных клеточных автоматов автором был построен ряд криптоалгоритмов, криптоанализ которых не выявил существенных уязвимостей: [5, 6, 17, 18].

Заключение

Таким образом, в статье разработан новый метод построения алгоритмов выработки имитовставок, основанных на обобщенных клеточных автоматах.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №16-07-00542 а.

Список литературы

1. Bellare M., Canetti R., Krawczyk H. Keying hash functions for message authentication // Advances in Cryptology — CRYPTO'96. Springer Berlin Heidelberg, 1996. P. 1–15. (Ser: Lecture Notes in Computer Science; vol. 1109). DOI: 10.1007/3-540-68697-5_1
2. 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.neicon.ru/file/505104.html (дата обращения 11.11.2016)ю
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.neicon.ru/doc/340943.html (дата обращения 11.11.2016).
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.neicon.ru/doc/358973.html (дата обращения 11.11.2016).
5. 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.neicon.ru/file/504895.html (дата обращения 11.11.2016).

6. 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
7. Davidoff G., Sarnak P., Valette A. Elementary number theory, group theory and Ramanujan graphs. Cambridge: Cambridge University Press, 2003. 156 p. (Ser. London Mathematical Society Student Texts; vol. 55).
8. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin of the American Mathematical Society. 2006. Vol. 43, no. 4. P. 439–561. Режим доступа: http://www.ams.org/journals/bull/2006-43-04/S0273-0979-06-01126-8/ (дата обращения 11.11.2016).
9. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. 1988. Vol. 8, no. 3. P. 261–277. DOI: 10.1007/BF02126799
10. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the ramanujan conjectures // Proceedings of the 18th annual ACM symposium on Theory of computing. ACM. 1986. P. 240–246.
11. Sarnak P. Some applications of modular forms. Cambridge: Cambridge University Press, 1990. 124 p. (Ser: Cambridge Tracts in Mathematics; vol. 99).
12. Ключарёв П.Г. Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 9. С. 194–202. DOI: 10.7463/0914.0727086
13. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
14. Bassham III L.E., Rukhin A.L., Soto J., Nechvatal J.R., Smid M.E., Barker E.B., Leigh S.D., Levenson M., Vangel M., Banks D.L., Heckert N.A., Dray J.F., Vo S. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Gaithersburg: NIST, 2010. 163 p. Режим доступа: http://dl.acm.org/citation.cfm?id=2206233 (дата обращения 11.11.2016).
15. Soto J. Statistical testing of random number generators // Proceedings of the 22nd National Information Systems Security Conference. Gaithersburg: NIST, 1999. Vol. 10. 12 p.
16. Živković M. A table of primitive binary polynomials // Mathematics of Computation. 1994. Vol. 62, no. 205. P. 385–386.
17. Ключарёв П.Г. Блочные шифры, основанные на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 12. DOI: 10.7463/0113.0517543
18. Ключарёв П. Г. Криптографические хэш-функции, основанные на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 1. DOI: 10.7463/0113.0534640

Science & Education of the Bauman MSTU
Electronic journal
ISSN 1994-0408

Science and Education of the Bauman MSTU, 2016, no. 11, pp. 142–152.
DOI: **10.7463/1116.0849590**
Received: 9.11.2016
Revised: 24.11.2016

Algorithms for Message Authentication Codes Based on Generalized Cellular Automata

Klyucharev P. G.[1,*]

[*]pk.iu8@yandex.ru

[1]Bauman Moscow State Technical University, Russia

Keywords: cryptography, cellular automata, MAC

An important class of cryptographic algorithms is Message Authentication Code (MAC) algorithms. These algorithms are designed to provide integrity of messages and authentication of their source.

The main objective of the paper is to develop a method for synthesis of MAC algorithms based on generalized cellular automata.

The paper proposes the method of MAC algorithm development that uses the following pattern. Let the MAC to be calculated from the message at a certain key. The algorithm execution comprises two phases: a phase of absorption and a phase of calculation result.

The phase of absorption uses the generalized cellular automata to the internal state of which the next block of message is added in several steps. To ensure the dependence of the output on all the key bits is used a driving sequence, produced by the linear shift register with a feedback. Initial filling of cellular automata and the initial filling of the shift register are based on the key. Once the cellular automata have processed the entire message, the absorbing phase is completed. Then a phase of calculation result begins. During this phase the cellular automata continue running and at the same time, once in the certain number of steps, the required number of MAC bits are taken off some bits of its internal state. After the required number of bits has been received the algorithm is terminated.

As a graph of the cellular automata are used the Ramanujan graphs, i.e. graphs of Lubotzky — Phillips — Sarnak. A local communication function is selected in a special way.

The paper presents the requirements for a local communication function, focuses on the structure of a cellular automata graph and on the crypto-strength issues.

Statistical tests of algorithms for different sets of parameters were carried out using a NIST Statistical Test Suite complex of statistical tests. All the tests have been successfully completed.

Thus, the paper offers a new method to develop algorithms based on generalized cellular automata.

The work was conducted under support of the Russian Federal Property Fund within the framework of research project 16-07-00542.

References

1. Bellare M., Canetti R., Krawczyk H. Keying hash functions for message authentication. *Advances in Cryptology — CRYPTO'96*. Springer Berlin Heidelberg, 1996, pp. 1–15. (Ser: Lecture Notes in Computer Science; vol. 1109). DOI: 10.1007/3-540-68697-5_1
2. Kliucharev P.G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostoianiia obobshchennogo kletochnogo avtomata. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2012, no. 1. Available at: http://technomag.neicon.ru/file/505104.html, accessed 11.11.2016. [In Russian]
3. Kliucharev P.G. O periode obobshchennykh kletochnykh avtomatov. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2012, no. 2. Available at: http://technomag.neicon.ru/doc/340943.html, accessed 11.11.2016. [In Russian]
4. Kliucharev P.G. Obespechenie kriptograficheskikh svoistv obobshchennykh kletochnykh avtomatov. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2012, no. 3. Available at: http://technomag.neicon.ru/doc/358973.html, accessed 11.11.2016. [In Russian]
5. Kliucharev P.G. Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluchainykh posledovatel'nostei. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2011, no. 10. Available at: http://technomag.neicon.ru/file/504895.html accessed 11.11.2016. [In Russian]
6. Kliucharev P.G. Postroenie psevdosluchainykh funktsii na osnove obobshchennykh kletochnykh avtomatov. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2012, no. 10. DOI: 10.7463/1112.0496381 [In Russian]
7. Davidoff G., Sarnak P., Valette A. *Elementary number theory, group theory and Ramanujan graphs*. Cambridge, Cambridge University Press, 2003. 156 p. (Ser. London Mathematical Society Student Texts; vol. 55).
8. Hoory S., Linial N., Wigderson A. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 2006, vol. 43, no. 4, pp. 439–561. Available at: http://www.ams.org/journals/bull/2006-43-04/S0273-0979-06-01126-8/, accessed 11.11.2016.
9. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277. DOI: 10.1007/BF02126799
10. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the ramanujan conjectures. *Proceedings of the 18th annual ACM symposium on Theory of computing*. ACM, 1986, pp. 240–246.

11. Sarnak P. *Some applications of modular forms*. Cambridge, Cambridge University Press, 1990, 124 p. (Ser: Cambridge Tracts in Mathematics; vol. 99).

12. Kliucharev P.G. Ob ustoichivosti obobshchennykh kletochnykh avtomatov k nekotorym tipam kollizii. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2014, no. 9, pp. 194–202. DOI: 10.7463/0914.0727086 [In Russian]

13. Alferov A.P., Zubov A.Iu., Kuz'min A.C., Cheremushkin A.V. *Osnovy kriptografii* [Basics of cryptography]. Moscow, Gelios APB, 2002, 480 p. [In Russian]

14. Bassham III L.E., Rukhin A.L., Soto J., Nechvatal J.R., Smid M.E., Barker E.B., Leigh S.D., Levenson M., Vangel M., Banks D.L., Heckert N.A., Dray J.F., Vo S. *SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Gaithersburg, NIST, 2010, 163 p. Available at: http://dl.acm.org/citation.cfm?id=2206233, accessed 11.11.2016.

15. Soto J. Statistical testing of random number generators // Proceedings of the 22nd National Information Systems Security Conference. Gaithersburg, NIST, 1999, vol. 10, 12 p.

16. Živković M. A table of primitive binary polynomials. *Mathematics of Computation*, 1994, vol. 62, no. 205, pp. 385–386.

17. Kliucharev P.G. Blochnye shifry, osnovannye na obobshchennykh kletochnykh avtomatakh. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2012, no. 12. DOI: 10.7463/0113.0517543 [In Russian]

18. Kliucharev P.G. Kriptograficheskie khesh-funktsii, osnovannye na obobshchennykh kletochnykh avtomatakh. *Nauka i obrazovanie = Science and education of the Bauman MSTU*, 2013, no. 1. DOI: 10.7463/0113.0534640 [In Russian]