Построение псевдослучайных функций на основе обобщенных клеточных автоматов

10, октябрь 2012

DOI: 10.7463/1112.0496381

Ключарёв П. Г.

УДК 519.713+004.056.55

Россия, МГТУ им. Н.Э. Баумана

pk.iu8@yandex.ru

1. Введение

Псевдослучайные функции находят большое применение в криптографии. Во многих случаях они являются основой блочных шифров и хэш-функций. В частности, их можно использовать в качестве S-блоков [18,20]. В настоящее время большинство блочных шифров, хэш-функций, а также ряд поточных шифров, основаны на S-блоках [11, 15]. Зачастую, для построения криптографических алгоритмов требуются достаточно большие S-блоки — с разрядностью входа 32, 64 и более бит. Такие S-блоки, как правило, комбинируют из небольших S-блоков. Например, в алгоритме AES [13] используется S-блок с разрядностью входа 8 бит, а в ГОСТ 28147-89 [1] используются S-блоки с разрядностью входа 4 бита. Такой подход плох тем, что невозможно обеспечить псевдослучайность составного S-блока, кроме того, малые S-блоки возможно подвергнуть различным видам разностного и линейного криптоанализа. Построение больших S-блоков другими способами затруднено, их нельзя задать в виде таблицы, в силу слишком большого ее объема. Поэтому их надо задавать в виде некоторого алгоритма, причем достаточно эффективно реализуемого. Разработке методики построения псевдослучайных функций, на основе которых можно строить S-блоки, и посвящена эта работа.

В этой работе для построения псевдослучайных функций используются обобщенные клеточные автоматы. Алгоритмы, основанные на клеточных автоматах, могут быть эффективно реализованы аппаратно. Впервые обобщенные клеточные автоматы были использованы для построения поточного алгоритма шифрования в работах [8, 7]. Эти подходы были развиты автором в работах [6, 4, 5, 3, 2].

2. Постановка задачи

Основной задачей этой работы является разработка методов построения псевдослучайных функций.

С формальной точки зрения, псевдослучайная функция — это функция вида

$$F: B^k \times B^n \rightarrow B^m, \quad (1)$$

такая, что не существует алгоритма полиномиальной сложности, способного отличить оракул для функции $g: B^n \rightarrow B^m$: $g(x) = F(key, x)$ для случайно выбранного $key \in B^k$ от оракула для случайной функции $h: B^n \rightarrow B^m$. Здесь и далее $B = \{0, 1\}$.

Однако существование функций, отвечающих этому определению не доказано. В то же время, на практике широко используются функции, которые не удастся отличить от случайных с помощью известных методов. Например, все современные блочные шифры являются такими «практически» псевдослучайными функциями. Поэтому, в данной работе мы удовлетворимся практической псевдослучайностью и будем называть псевдослучайными функции вида (1), для которых выполняются следующие условия:

- 1) должен иметь место строгий лавинный эффект (инвертирование одного бита входа должно приводить к тому, что каждый бит выхода инвертируется с вероятностью 0,5);
- 2) нелинейность функции [10] (т.е. расстояние Хемминга до множества аффинных функций) должна быть как можно выше;
- 3) должно быть невозможно отличить функцию от случайной с помощью стандартного набора статистических тестов.

Построение этой функции будет производиться с помощью обобщенных клеточных автоматов.

3. Обобщенные клеточные автоматы

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

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

При этом для вершины v_i , входящие в нее ребра пронумерованы числами $1 \dots d_i$.

Опишем теперь работу обобщенного клеточного автомата. В начальный момент времени каждая ячейка памяти m_i , $i = 1, \dots, N$, имеет некоторое начальное значение $m_i(0)$. Далее автомат работает по шагам. На шаге с номером t с помощью локальной функции связи вычисляются новые значения ячеек:

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

где $\eta(i, j)$ — номер вершины, из которой исходит ребро, входящее в вершину i и имеющее номер j . Заполнением клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \dots, m_N(t))$.

Периодом клеточного автомата будем называть период последовательности его заполнений.

Назовем однородным обобщенным клеточным автоматом обобщенный клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f , т.е. для любого $i \in \{1, \dots, N\}$ выполняется $f_i = f$. Степени захода вершин такого клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \dots = d_N = d$.

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 $\{u, v\}$. Он является регулярным. 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. Выходной последовательностью клеточного автомата A назовем функцию $F_A: B^N \times \mathbb{N} \rightarrow B^N$, аргументами которой является начальное заполнение и номер шага, а значением — значение выхода на этом шаге.

4. Конструкция псевдослучайной функции

В этом разделе мы предложим способ построения псевдослучайных функций, основанный на обобщенных клеточных автоматах.

Пусть требуется построить псевдослучайную функцию $S: B^k \times B^n \rightarrow B^m$.

Рассмотрим обобщенный клеточный автомат A , содержащий $k + n + t$ вершин, где t — некоторая величина, зависящая от n , которую будем называть количеством скрытых вершин клеточного автомата. Вопрос о выборе числа t будет обсужден ниже.

Построим псевдослучайную функцию следующим образом:

$$S_c^A(key, x) = pr_m(F_A(x \parallel key \parallel c, r)),$$

где $x \parallel y$ — конкатенация x и y ; r — число шагов клеточного автомата; $pr_m: B^* \rightarrow B^m$ — функция, возвращающая младшие m элементов аргумента; $c \in B^t$ — некоторая константа, для веса которой справедливо соотношение

$$|c| = \begin{cases} \frac{t}{2}, & t \text{ — четное;} \\ \frac{t+1}{2}, & t \text{ — нечетное.} \end{cases}$$

Константа c предназначена для того, чтобы обеспечить отсутствие неподвижных точек, а также для улучшения лавинного эффекта.

Число шагов клеточного автомата r и число скрытых вершин t выбираются так, чтобы функцию нельзя было отличить от случайной при помощи статистических тестов.

Ясно, что для того чтобы каждый бит выхода функции зависел от всех битов входа, необходимо, чтобы выполнялось $r \geq D$, где D — диаметр графа. Для того чтобы функция была псевдослучайной, обычно требуется несколько большее число шагов. Более точно на вопрос о числе шагов можно ответить посредством статистического тестирования, проведенного в разделе 7. Основные его результаты отражены ниже (см. табл. 1). Кроме того, проведенные тесты показали, что для того чтобы функция была псевдослучайной, необходимо, чтобы: $t \geq 1,4N$, где N — число вершин в графе.

5. Граф обобщенного клеточного автомата

Граф обобщенного клеточного автомата выберем из следующих соображений:

- граф должен иметь хаотическую структуру;
- диаметр графа должен быть мал;
- граф должен быть регулярным;
- граф не должен иметь петель и кратных ребер;
- граф должен иметь как можно меньшую степень (чтобы снизить коммуникационную сложность клеточного автомата);
- степень графа должна быть не меньше четырех.

Этим требованиям удовлетворяют так называемые графы Рамануджана [12, 14, 17].

Рассмотрим отсортированный по убыванию спектр графа (т.е. совокупность собственных чисел его матрицы смежности): $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. *Графом Рамануджана* называется граф, для которого справедливо неравенство

$$\lambda_2 \leq 2\sqrt{d-1}, \quad (3)$$

где d — степень графа.

Как известно из спектральной теории графов [9], для диаметра графов Рамануджана справедливо соотношение $D = 2 \log_{d-1} n + O(1)$.

Известно два способа построения небольших графов Рамануджана:

- 1) случайная генерация с последующей проверкой значения λ_2 ;
- 2) построение при помощи известного детерминированного алгоритма.

В случае использования первого подхода требуется выработать случайный регулярный граф. Это можно сделать, например, используя метод, изложенный в работе [19], либо более быстрый алгоритм, изложенный в работе [25]. Известно [14], что случайный регулярный граф с большой вероятностью является графом Рамануджана. Тем не менее, необходимо проверить выполнение условия (3), получив значение λ_2 методами линейной алгебры.

Второй способ состоит в том, чтобы воспользоваться каким-либо известным семейством графов Рамануджана. При этом, такой способ должен давать достаточную свободу в выборе

числа вершин графа в достаточно широком диапазоне. По-видимому, наиболее подходящим семейством является так называемое семейство графов Любоцкого — Филиппа — Сарнака $Y^{p,q}$ [17, 16, 21]. Для таких графов доказано, что они являются графами Рамануджана. Построение таких графов производится следующим образом.

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

$$p \equiv 1 \pmod{4}; \quad q \equiv 1 \pmod{4}; \quad p \neq q; \quad \left(\frac{p}{q}\right) = 1,$$

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

Мы будем строить неориентированный мультиграф $G = (V, E)$. Множеством вершин мультиграфа V является проективная прямая над конечным полем $\mathbb{F}_q$, другими словами, $V = \mathbb{F}_q \cup \{\infty\}$. Мультимножество ребер E состоит из всех пар (u, v) , для которых

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

для всех четверок $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, таких, что:

- 1) a_0 — нечетное положительное;
- 2) a_1, a_2, a_3 — четные;
- 3) выполняется условие

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p. \quad (5)$$

При этом $i \in \mathbb{F}_q$, такое, что $i^2 + 1 = 0$. Степенью графа является количество решений уравнения (5), равное $p + 1$.

В построенном таким образом графе могут быть кратные ребра (в том случае, когда (4) выполняется и для (u, v) , и для (v, u)) и петли. Как показали статистические тесты, это ухудшает показатели лавинного эффекта. Поэтому необходимо избавиться от кратных ребер и петель, причем так, чтобы граф остался регулярным.

Кратные ребра обработаем следующим способом. 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 ребра (u_1, u_2) и (v_1, v_2) . Таким способом можно обработать все кратные ребра в графе (если количество пар кратных ребер четное, что всегда имеет место для рассматриваемого графа). Эта процедура, очевидно, не нарушит регулярность графа и не уменьшит коэффициенты реберного и вершинного расширения.

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

6. Локальная функция связи

Важным является правильный выбор локальной функции связи обобщенного клеточного автомата. В этом разделе мы сформулируем требования к такой функции.

Будем говорить, что обобщенный клеточный автомат вычисляет булеву функцию $\phi(x_1, \dots, x_M)$, если существуют такие $j_0 \in \{1, \dots, N\}$, $t_0 \in \mathbb{Z}^+$ и набор $(j_1, \dots, j_M) \in \{1, \dots, N\}^M$, элементы которого попарно различны, что выполняется $m_{j_0}(t_0) = \phi(m_{j_1}(0), \dots, m_{j_n}(0))$, где $m_i(t)$ — значение i -й ячейки на шаге t .

Заметим сначала, что если локальная функция связи не имеет слагаемых первой степени в своей АНФ, то АНФ функций, вычисляемых обобщенным клеточным автоматом после двух тактов работы, не будут иметь слагаемых первой и второй степеней. После трех шагов — не имеют слагаемых по третьей степень включительно и т.д. Из этого следует, что если АНФ локальной функции связи обобщенного клеточного автомата не имеет слагаемых первой степени, то функции, вычисляемые обобщенным клеточным автоматом, быстро вырождаются в функцию $x_1 x_2 \dots x_n$.

Если уже по виду локальной функции связи можно определить, что обобщенный клеточный автомат не может вычислить некоторый класс булевых функций, то криптоанализ систем шифрования, основанных на таких автоматах, упрощается. Заметим, что для того, чтобы однородный клеточный автомат мог вычислить произвольную функцию, необходимо, чтобы локальная функция связи являлась шепферовой.

Кроме того, как показано в работе [8], равновесность локальной функции связи является необходимым и достаточным условием для равномерности распределения выходной последовательности обобщенного клеточного автомата.

Наконец, важным свойством является нелинейность криптографического преобразования. Дабы обеспечить большую его нелинейность, потребуем, чтобы локальная функция связи была как можно более нелинейной.

Итак, для локальной функции связи должны выполняться следующие условия:

- 1) функция должна быть равновесной;
- 2) алгебраическая нормальная форма функции должна содержать хотя бы одну переменную в первой степени;
- 3) функция должна быть шепферовой;
- 4) функция должна быть как можно более нелинейной.

Этим условиям удовлетворяют функции из семейства, построенного автором [5]. Так, в случае нечетного числа переменных используется функция

$$g_1(u, x_1, y_1, \dots, x_k, y_k) = \bigoplus_{i=1}^k x_i y_i \oplus s_1(x_1, \dots, x_k) \oplus u,$$

где $s_1(x_1, \dots, x_k)$ — произвольная булева функция, причем $k + t_1 = 1 \pmod{2}$, где t_1 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_1 и при этом свободный член равен 1.

В случае четного числа переменных используется функция:

$$\begin{aligned}
 g_2(v, u, x_1, y_1, \dots, x_k, y_k) &= \\
 &= (1 \oplus v)(\beta_1(x_1, y_1, \dots, x_k, y_k) \oplus u) \oplus v(\beta_3(x_1, y_1, \dots, x_k, y_k) \oplus u) = \\
 &= \bigoplus_{i=1}^k x_i y_i \oplus s_1(x_1, \dots, x_k) \oplus v(s_1(x_1, \dots, x_k) \oplus s_3(x_1, \dots, x_k)) \oplus u,
 \end{aligned}$$

где $s_1(x_1, \dots, x_k)$ и $s_3(x_1, \dots, x_k)$ — произвольные булевы функции, причем $k + t_3 = 1 \pmod{2}$, где t_3 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_3 и при этом свободный член АНФ функции s_1 равен 1.

Примером такой функции может служить:

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1 x_3 x_5 \oplus x_3 x_4 \oplus x_5 x_6 \oplus x_3 x_5 \oplus x_1 x_5 \oplus x_1 \oplus x_2 \oplus 1. \quad (6)$$

7. Статистическое тестирование

С целью эмпирического подтверждения гипотезы о псевдослучайности построенных функций проводилось статистическое тестирование с помощью набора статистических тестов NIST Statistical Test Suit [24, 22]. При этом используется методика, приведенная в [23]. Методика включает в себя тестирование лавинного эффекта по ключу и по аргументу (открытому тексту, по используемой в [23] терминологии), корреляции входа и выхода, итерации функции и др. Тесты были проведены для функций, параметры которых приведены в табл. 1 (во всех случаях использовалась локальная функция связи, заданная формулой (6). В ней же приведено минимальное число шагов, после которого функция является псевдослучайной по результатам тестов.

Таблица 1

Параметры клеточных автоматов, задающих протестированные функции

	Длина входа	Длина ключа	Длина выхода	Число вершин	Степень графа	Диаметр графа	Число шагов
1	64	64	64	282	6	6	7
2	128	128	128	390	6	6	8
3	256	256	256	810	6	6	9

Для всех функций из табл. 1 были пройдены все статистические тесты, что подтверждает гипотезу о том, что функции, построенные с помощью клеточного автомата так, как указано в настоящей статье является псевдослучайными.

8. Заключение

Таким образом, в статье предложена методика построения псевдослучайных функций, основанных на обобщенных клеточных автоматах. Такие функции могут найти широкое

применение в области криптографии, в частности, их можно использовать в качестве S-блоков.

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

Список литературы

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 1990-07-01. М.: Изд-во стандартов, 1996. 28 с.
2. 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 22.11.2012).
3. 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 22.11.2012).
4. 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 22.11.2012).
5. 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 22.11.2012).
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 22.11.2012).
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 Московского государственного технического университета им. Н.Э. Баумана. Сер. Приборостроение.* 2011. № 2. С. 68–76.
9. Chung F. Spectral graph theory. American Mathematical Society, 1997. (CBMS Regional Conference Series in Mathematics, No. 92).
10. Cusick T., Stănică P. Cryptographic Boolean functions and applications. Academic Press, 2009. 232 p.

11. Daemen J., Rijmen V. The design of Rijndael: AES-the advanced encryption standard. Springer, 2002.
12. Davidoff G., Sarnak P., Valette A. Elementary number theory, group theory and Ramanujan graphs. Cambridge University Press, 2003. 144 p. (London Mathematical Society Student Texts, vol. 55.)
13. Federal Information Processing Standard (FIPS) Pub. 197. *Advanced Encryption Standard (AES)*. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL). 2001. 47 p. Available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, accessed 22.11.2012.
14. 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.
15. Knudsen L., Robshaw M. The block cipher companion. Springer, 2011.
16. 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. NY: ACM, 1986. P. 240-246. DOI: 10.1145/12130.12154.
17. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // *Combinatorica*. 1988. Vol. 8, no. 3. P. 261–277.
18. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions // *SIAM Journal on Computing*. 1988. Vol. 17, no. 2. P. 373–386.
19. McKay B., Wormald N. Uniform generation of random regular graphs of moderate degree // *Journal of Algorithms*. 1990. Vol. 11, no. 1. P. 52–67.
20. Mister S., Adams C. Practical s-box design // Workshop on Selected Areas in Cryptography, SAC / Citeseer. 1996. Vol. 96. P. 61–76.
21. Sarnak P. Some applications of modular forms. Cambridge University Press, 1990. Vol. 99.
22. Soto J. Statistical testing of random number generators // Proceedings of the 22nd National Information Systems Security Conference / NIST Gaithersburg, MD. Vol. 10. 1999. P. 12.
23. Randomness testing of the advanced encryption standard finalist candidates: Rep. / DTIC Document; Executor: J. Soto, L. Bassham: 2000.
24. A statistical test suite for random and pseudorandom number generators for cryptographic applications: Rep. / DTIC Document; Executor: A. Rukhin, J. Soto, J. Nechvatal et al.: 2001.
25. Steger A., Wormald N. Generating random regular graphs quickly // *Combinatorics Probability and Computing*. 1999. Vol. 8, no. 4. P. 377–396.

Construction of pseudo-random functions based on generalized cellular automata

10, October 2012

DOI: 10.7463/1112.0496381

Klyucharev P. G.

Russia, Bauman Moscow State Technical University
pk.iu8@yandex.ru

The paper presents a method of constructing pseudo-random functions based on the generalized cellular automata. The graphs of the automata are Ramanujan graphs. The proposed method can be used to construct S-blocks, designed for operation in cryptographic algorithms.

References

1. *GOST 28147-89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritmy kriptograficheskogo preobrazovaniia* [State Standard 28147-89. Information processing system. Cryptographic Security. Cryptographic transformation algorithm]. Moscow, Standards Publishing House, 1996. 28 p.
2. Klyucharev P.G. Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluhainykh 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 22.11.2012.
3. Klyucharev P.G. O vychislitel'noi slozhnosti nekotorykh zadach na obobshchennykh kletochnykh avtomatakh [On the computational complexity of some problems on generalized cellular automata]. *Bezopasnost' informatsionnykh tekhnologii* [Security of information technologies], 2012, no. 1. Available at: http://www.pvti.ru/data/file/bit/2012_1/part_4.pdf, accessed 22.11.2012.
4. Klyucharev P.G. O periode obobshchennykh kletochnykh avtomatov [About the period of generalized cellular automata]. *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 22.11.2012.

5. Kliucharev P.G. Obespechenie kriptograficheskikh svoystv obobshchennykh kletochnykh avtomatov [On cryptographic properties of generalized cellular automata]. *Nauka i obrazovanie 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 22.11.2012.
6. Kliucharev P.G. NP-trudnost' zadachi o vosstanovlenii predydushchego sostoiianiia 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 22.11.2012.
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 svoystvakh 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* [Herald of the Bauman MSTU. Ser. Instrumentation], 2011, no. 2, pp. 68–76.
9. Chung F. *Spectral graph theory*. American Mathematical Society, 1997. (CBMS Regional Conference Series in Mathematics, no. 92).
10. Cusick T., Stănică P. *Cryptographic Boolean functions and applications*. Academic Press, 2009. 232 p.
11. Daemen J., Rijmen V. *The design of Rijndael: AES-the advanced encryption standard*. Springer, 2002.
12. Davidoff G., Sarnak P., Valette A. *Elementary number theory, group theory and Ramanujan graphs*. Cambridge University Press, 2003. 144 p. (London Mathematical Society Student Texts, vol. 55.)
13. *Federal Information Processing Standard (FIPS) Pub. 197. Advanced Encryption Standard (AES)*. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL). 2001. 47 p. Available at: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, accessed 22.11.2012.
14. 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.
15. Knudsen L., Robshaw M. *The block cipher companion*. Springer, 2011.
16. 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.

17. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*. 1988. Vol. 8, no. 3. P. 261–277.
18. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*. 1988. Vol. 17, no. 2. P. 373–386.
19. McKay B., Wormald N. Uniform generation of random regular graphs of moderate degree. *Journal of Algorithms*. 1990. Vol. 11, no. 1. P. 52–67.
20. Mister S., Adams C. Practical s-box design. *Workshop on Selected Areas in Cryptography, SAC*. Citeseer. 1996. Vol. 96. P. 61–76.
21. Sarnak P. *Some applications of modular forms*. Cambridge University Press, 1990. Vol. 99.
22. Soto J. Statistical testing of random number generators. *Proceedings of the 22nd National Information Systems Security Conference*. NIST Gaithersburg, MD. Vol. 10. 1999. P. 12.
23. Randomness testing of the advanced encryption standard finalist candidates: Rep. DTIC Document; Executor: J. Soto, L. Bassham: 2000.
24. A statistical test suite for random and pseudorandom number generators for cryptographic applications: Rep. DTIC Document; Executor: A. Rukhin, J. Soto, J. Nechvatal et al.: 2001.
25. Steger A., Wormald N. Generating random regular graphs quickly. *Combinatorics Probability and Computing*. 1999. Vol. 8, no. 4. P. 377–396.