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

Блочные шифры, основанные на обобщенных клеточных автоматах

 # 12, декабрь 2012
DOI: 10.7463/0113.0517543
Ключарёв П. Г.

УДК 519.713+004.056.55

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

1. Введение

Одним из важнейших классов криптографических алгоритмов являются блочные шифры. В настоящее время существует большое количество разнообразных блочных шифров (обзор наиболее известных из них можно найти, например, в книгах [11, 16]), но все возрастающие требования, предъявляемые к производительности, и необходимость реализации в условиях дефицита вычислительных ресурсов, приводят к необходимости разработки новых, высокопроизводительных, криптоалгоритмов. В частности, интерес представляет подход к синтезу блочных шифров, основанный на использовании обобщенных клеточных автоматов, поскольку он позволяет построить шифры, которые могут быть с большой эффективностью реализованы аппаратно. Подобный подход был впервые предложен для создания поточных шифров в работах [7, 8] и развит автором в работах [1–4, 6].

В работе [5] автором было предложено семейство псевдослучайных функций, основанных на обобщенных клеточных автоматов. Такие функции могут использоваться в качестве S-блоков, подходящих для построения блочных шифров. Данная работа посвящена методам построения блочных шифров, основанных на этих функциях.

Существует два основных метода построения блочных шифров: SP-сеть и схема Фейстеля.

Для использования SP-сети необходима обратимость S-блоков, однако рассматриваемые псевдослучайные функции обратимыми не являются. Поэтому в данной работе используется схема Фейстеля.

2. Основные понятия

В этом разделе мы кратко опишем методы построения клеточных автоматов,на основе которых будут построены S-блоки.

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*;

• булева функция $f_i(x_1, \ldots, x_{d_i})$, называемая локальной функцией связи i-й вершины.

При этом входящие в вершину v_i ребра пронумерованы числами $1, \ldots, d_i$.

Опишем теперь работу обобщенного клеточного автомата. В начальный момент времени каждая ячейка памяти m_i, $i = 1, \ldots, N$, 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:

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

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

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 $i \in \{1, \ldots, N\}$ выполняется $f_i = f$. Степени захода вершин такого клеточного автомата, очевидно, 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 $\{u, v\}$. 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 $F_A : \mathbb{N} \to B^N$, аргументами которой является начальное заполнение и номер шага, а значением — значение выхода на этом шаге.

Большое значение имеет выбор графа обобщенного клеточного автомата. В работе [5] показано, что в качестве графа клеточного автомата, применяемого для криптографических целей, хорошо подходят графы Рамануджана [9, 10, 13].

Рассмотрим отсортированный по убыванию спектр графа (т.е. собственные числа 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 $Y^{p,q}$ [12, 13, 15]. Построение таких графов производится следующим образом.

Выберем простые числа p и q, для которых выполняются условия

$$p = 1 (\mathrm{mod}\ 4);$$
$$q = 1 (\mathrm{mod}\ 4);$$
$$p \neq q;$$
$$\left(\frac{p}{q}\right) = 1,$$

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

Построим 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

$$v = \begin{cases} \dfrac{(a_0 + ia_1)u + (a_2 + ia_3)}{(-a_2 + ia_3)u + (a_0 - ia_1)}, & (a_2 - ia_3)u \neq a_0 - ia_1 \ \text{ и } \ u \neq \infty; \\ \infty, & (a_2 - ia_3)u = a_0 - ia_1 \ \text{ и } \ u \neq \infty; \\ \dfrac{a_0 + ia_1}{-a_2 + ia_3}, & a_2 \neq ia_3 \ \text{ и } \ u = \infty; \\ \infty, & a_2 = ia_3 \ \text{ и } \ u = \infty, \end{cases} \tag{3}$$

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

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p. \tag{4}$$

При этом $i \in \mathbb{F}_q$ таково, что $i^2 + 1 = 0$. Степенью графа является количество решений уравнения (4), равное $p + 1$.

В построенном таким образом графе существуют кратные ребра 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. Алгоритмы для этого описаны 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:

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

где $s_1(x_1, \ldots, x_k)$ — произвольная булева функция, причем $k + t_1 = 1 (\mathrm{mod}\ 2)$, 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

$$g_2(v, u, x_1, y_1, \ldots, x_k, y_k) =$$

$$= (1 \oplus v)(\beta_1(x_1, y_1, \ldots, x_k, y_k) \oplus u) \oplus v(\beta_3(x_1, y_1, \ldots, x_k, y_k) \oplus u) =$$

$$= \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k)) \oplus u,$$

где $s_1(x_1, \ldots, x_k)$ и $s_3(x_1, \ldots, x_k)$ — произвольные булевы функции, причем $k + t_3 = 1 (\mathrm{mod}\ 2)$, 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:

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_3x_5 \oplus x_3x_4 \oplus x_5x_6 \oplus x_3x_5 \oplus x_1x_5 \oplus x_1 \oplus x_2 \oplus 1. \quad (5)$$

3. Конструкция блочного шифра

В этом разделе предлагается метод построения блочных шифров, являющийся основным результатом настоящей работы.

В работе [5] автором предложен способ построения псевдослучайных функций вида $S_c : B^k \times B^n \to B^m$. Такие функции основаны на обобщенных клеточных автоматах и задаются выражением

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

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

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

Константа c предназначена для обеспечения отсутствия 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. Например, можно рекомендовать, чтобы выполнялось: $t \geqslant 0.4(k+n)$.

Автором обосновано и подтверждено экспериментально [5], что такие функции неотличимы от случайных при правильном выборе параметров.

Как было указано выше, в качестве структуры шифров используется схема Фейстеля. Заметим, что, несмотря на существование различных ее вариантов и обобщений, оптимальным является использование классической схемы Фейстеля. Такое утверждение можно сделать, поскольку число шагов клеточного автомата, необходимое для того, чтобы реализуемая им функция была псевдослучайной, пропорциональна диаметру его графа, который для графов Рамануджана растет как логарифм числа вершин. Следовательно, больший размер клеточного автомата приводит к увеличению производительности. Мы будем использовать вариант классической схемы Фейстеля, в котором смешивания данных с раундовым ключом осуществляется с помощью S-блока.

Воспользуемся тем, что, как показано в работе [14], из псевдослучайной функции можно построить блочный шифр с помощью схемы Фейстеля, причем для того, чтобы этот шифр являлся псевдослучайной подстановкой, достаточно трех раундов.

Итак, для построения блочного шифра определим следующее раундовое преобразование:

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus S^A_{c_i}(key_i, R_{i-1}),$$

где i — номер раунда; L_0 — левая половина блока открытого текста; R_0 — правая половина блока открытого текста; L_i — левая половина блока после i-го раунда; R_i — правая половина блока после i-го раунда; key_i — раундовый ключ; c_i — константа.

При расшифровании выполняется преобразование, обратное данному.

Для того чтобы каждое раундовое преобразование было различным, константы c_i должны попарно различаться. При этом, чтобы отличия между раундами проявлялись как можно быстрее, расстояние Хемминга между каждой парой констант должно быть близко к половине длины константы.

Как обычно, алгоритм шифрования состоит из нескольких раундов. Выше указывалось, что число раундов должно быть не меньше трех. Из соображений удобства можно рекомендовать четное число раундов. Статистические тесты показали, что при четырех раундах подстановка, реализуемая шифром, неотличима от случайной. Процедура распределения ключей использовалась простая — ключ разбивался на две равные части: $key = (key_1, key_2)$. Таким образом, определяются ключи первых двух раундов. Раундовые ключи двух оставшихся раундов определяются следующим образом: $key_3 = rol(key_1, m/2)$, $key_4 = rol(key_2, m/2)$, где rol — функция, осуществляющая циклический сдвиг первого операнда влево, на количество разрядов, равное второму операнду; m — длина подключа, равная половине длины ключа.

4. Статистическое тестирование

Статистическое тестирование проводилось с помощью набора статистических тестов NIST Statistical Test Suite [17, 19]. При этом используется методика, приведенная в [18] и включающая в себя тестирование лавинного эффекта по ключу и по открытому тексту, корреляции входа с выходом и др. Эта методика применялась NIST для тестирования криптоалгоритмов, представленных на конкурс AES. Тесты были проведены для шифров, параметры которых приведены в табл. 1 (во всех случаях использовалась локальная функция связи, заданная формулой 5).

Таблица 1

Протестированные шифры

	Длина ключа	Длина блока	Число вершин	Степень графа	Число шагов (теор.)	Число шагов (экспер.)
1	128	128	182	6	6	6
2	256	128	282	6	7	7

Всеми вариантами шифра из таблицы 1 были пройдены все статистические тесты. Число шагов клеточных автоматов, начиная с которого все тесты были пройдены приведено в столбце «Число шагов (экспер.)». Число шагов, для которого используемые S-блоки неотличимы от псевдослучайных функций, согласно работе [5], приведено в столбце «Число шагов (теор.)».

Проведенные тесты подтверждают хорошие статистические свойства построенных криптографических алгоритмов.

5. Стойкость по отношению к основным методам криптоанализа

Учитывая то, что S-блоки неотличимы от случайных функций, а также то, что локальная функция связи клеточного автомата является нелинейной и шефферовой [4], можно утверждать, что каждый разряд выхода S-блока сложным образом нелинейно зависит от всех входов S-блока (т.е. от соответствующей половины блока и раундового подключа). В работе [6] показано, что в общем случае, задача о восстановлении предыдущего состояния обобщенного клеточного автомата является NP-полной. Это обстоятельство является аргументом в пользу криптостойкости рассматриваемого семейство шифров.

Стойкость к разностному криптоанализу обусловлена тем, что S-блоки имеют очень большой размер (например, 128×64, в случае, если длина ключа равна 128), что не позволяет построить разностные характеристики.

Стойкость к линейному криптоанализу обусловлена высокой нелинейностью S-блоков, которая достигается тем, что локальная функция связи клеточных автоматов имеет максимальную нелинейность для равновесной функции. Кроме того, эту функцию весьма затруднительно описать явно, ввиду крайней громоздкости формулы, а ее таблица истинности имеет очень большой размер. Все это не позволяет использовать существующие методики применения линейного криптоанализа.

Таким образом, шифры, синтезированные посредством предложенного метода, обладают стойкостью по отношению к основным методам криптоанализа.

6. Заключение

Таким образом, в статье разработан новый метод построения блочных шифров, основанный на использовании обобщенных клеточных автоматов.

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. 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.)

10. 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.

11. Knudsen L., Robshaw M. The block cipher companion. Springer, 2011.

12. 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.

13. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // *Combinatorica*. 1988. Vol. 8, no. 3. P. 261–277.

14. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions // *SIAM Journal on Computing*. 1988. Vol. 17, no. 2. P. 373–386.

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

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

17. Soto J. Statistical testing of random number generators // Proceedings of the 22nd National Information Systems Security Conference / NIST Gaithersburg, MD. 1999. Vol. 10. P. 12.

18. Soto J., Bassham L. Randomness testing of the advanced encryption standard finalist candidates: Rep. / DTIC Document, 2000.

19. Rukhin A., Soto J., Nechvatal J., et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications: Rep. DTIC Document, 2001.

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

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

electronic scientific and technical journal

Block ciphers based on generalized cellular automata

 # 12, December 2012

DOI: 10.7463/0113.0517543

Klyucharev P. G.

Russia, Bauman Moscow State Technical University

pk.iu8@yandex.ru

In the paper we present a method of constructing block ciphers, based on the generalized cellular automata. We use the Feistel network as the structure of the ciphers. The round function construction is based on generalized cellular automata which graph is a Ramanujan graph. Statistical properties of the ciphers were studied by means the NIST Statistical Test Suit. We got an empirical evidence that the ciphers have all necessary statistical properties and indistinguishable from pseudorandom permutations. There are a number of practical applications in the field of information security where ciphers constructed by means the method developed can be used.

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. 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 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 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 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* [Herald of the Bauman MSTU. Ser. Instrument Engineering], 2011, no. 2, pp. 68–76.
9. 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.)

10. 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.
11. Knudsen L., Robshaw M. *The block cipher companion*. Springer, 2011.
12. 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, pp. 240–246. DOI: 10.1145/12130.12154.
13. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277.
14. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 1988, vol. 17, no. 2, pp. 373–386.
15. Sarnak P. *Some applications of modular forms*. Cambridge: Cambridge University Press, 1990. (*Cambridge Tracts in Mathematics*, vol. 99.)
16. Schneier B., Sutherland P. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., 1995.
17. Soto J. Statistical testing of random number generators. *Proceedings of the 22nd National Information Systems Security Conference*. Gaithersburg, MD, 1999, vol. 10, p. 12.
18. Soto J., Bassham L. *Randomness testing of the advanced encryption standard finalist candidates*: Rep. DTIC Document, 2000.
19. Rukhin A., Soto J., Nechvatal J., et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*: Rep. DTIC Document, 2001.