НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА

НАУКА и ОБРАЗОВАНИЕ

Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408

электронный научно-технический журнал

Исследование стойкости блочных шифров, основанных на обобщенных клеточных автоматах, к линейному криптоанализу

 # 05, май 2013

DOI: 10.7463/0513.0574231

Ключарёв П. Г.

УДК 519.713+004.056.55

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

1. Введение

В работе [2] автором было предложено семейство блочных шифров, основанных на семействе псевдослучайных функций, построенном автором в работе [4] с использованием обобщенных клеточных автоматов. В этой статье мы исследуем достаточно широкий класс блочных шифров, построенных на основе схемы Фейстеля и обобщенных клеточных автоматов, на криптостойкость по отношению к линейному криптоанализу. Основной задачей исследования является получение достаточных условий криптостойкости этого класса шифров по отношению к классическому линейному криптоанализу.

2. Линейный криптоанализ

Линейный криптоанализ является одним из основных методов криптоанализа блочных шифров. Впервые он был предложен в работе [14] для криптоанализа шифра FEAL, затем применен для криптоанализа шифра DES в работе [13]. Систематическое изложение этого метода криптоанализа можно найти в работах [9, 6, 15], а также в книге [11]. Здесь мы ограничимся лишь кратким изложением основных идей этого метода.

Линейный криптоанализ основан на аппроксимации шифра или его части линейным булевым уравнением, которое выполняется с вероятностью, отличающейся от $\frac{1}{2}$ на некоторую величину $\varepsilon \neq 0$, называемую преобладанием. Существует два основных алгоритма такого криптоанализа.

Алгоритм 1. Пусть для шифра с вероятностью $p = \frac{1}{2} + \varepsilon$ выполняется линейное уравнение вида:

$$(x \cdot \alpha) \oplus (y \cdot \beta) = (key \cdot \gamma),$$

где x — блок открытого текста; y — блок шифртекста; key — ключ; α, β, γ — некоторые битовые маски, точкой обозначено скалярное произведение по модулю 2.

Алгоритм 1 состоит в следующем:

1. Пусть имеется N_L пар (x, y), где x — открытый текст, а y — шифртекст. Для каждой такой пары (x, y) вычислить $h = (x \cdot \alpha) \oplus (y \cdot \beta)$. Пусть T_0 — число случаев, когда $h = 0$, а T_1 — число случаев, когда $h = 1$.

2. При $\varepsilon > 0$, если $T_0 > \frac{N_L}{2}$, предположить, что $key \cdot \gamma = 0$, а если $T_0 < \frac{N_L}{2}$, предположить, что $key \cdot \gamma = 1$. При $\varepsilon < 0$ — наоборот, если $T_0 > \frac{N_L}{2}$, предположить, что $key \cdot \gamma = 1$, а если $T_0 < \frac{N_L}{2}$, предположить, что $key \cdot \gamma = 0$.

В работе [13] показано, что вероятность того, что этот алгоритм даст правильный результат, равна

$$\frac{1}{2\pi} \int\limits_{-2\sqrt{N_L}|\varepsilon|}^{\infty} e^{-x^2/2} dx$$

Вероятности, вычисленные с помощью этой формулы, приведены в табл. 1.

Таблица 1

Вероятность успеха Алгоритма 1

N_L	$\lvert\varepsilon\rvert^{-2}/16$	$\lvert\varepsilon\rvert^{-2}/8$	$\lvert\varepsilon\rvert^{-2}/4$	$\lvert\varepsilon\rvert^{-2}/2$	$\lvert\varepsilon\rvert^{-2}$
Вероятность	69%	76%	84%	92%	97%

Алгоритм 2. Пусть шифр состоит из r раундов. Пусть для первых $r - 1$ раундов с вероятностью $p = \frac{1}{2} + \varepsilon$ выполняется линейное уравнение вида:

$$(x \cdot \alpha) \oplus (y_{r-1} \cdot \beta) = (key \cdot \gamma),$$

где x — открытый текст; y_{r-1} — шифртекст на предпоследнем раунде; key — ключ; α, β, γ — некоторые битовые маски, точкой обозначено скалярное произведение по модулю 2.

Теперь обозначим функцию расшифрования последнего раунда как $F^{-1}(y, key_r)$, где key_r — раундовый ключ последнего раунда.

Алгоритм 2 состоит в следующем:

1. Пусть имеется N_L пар (x, y), где x — открытый текст, а y — шифртекст. Для каждой такой пары (x, y), для каждого возможного значения ключа последнего раунда key_r, вычислить $h = (x \cdot \alpha) \oplus (F^{-1}(y, key_r)$. Пусть T_{0,key_r} — число случаев, когда $h = 0$, а T_{1,key_r} — число случаев, когда $h = 1$ при данном key_r.

2. Среди всех полученных значений T находим максимальное $T_{i,s}$. Предполагаем, что $key_r = s$.

С помощью этого алгоритма можно найти подключ последнего раунда.

В работе [13] выведена формула для вероятности того, что алгоритм 2 даст правильный результат. В связи с тем, что эта формула довольно громоздкая, мы воздержимся от приведения ее здесь. Вероятности, вычисленные с ее помощью указаны в табл. 2.

Таблица 2

Вероятность успеха Алгоритма 2

N_L	$2\|\varepsilon\|^{-2}$	$4\|\varepsilon\|^{-2}$	$8\|\varepsilon\|^{-2}$	$16\|\varepsilon\|^{-2}$
Вероятность	49%	78%	97%	99%

Для использования вышеприведенных алгоритмов необходимо получить линейную аппроксимацию для всего шифра, либо для $r-1$ его раундов, имеющую достаточно большое преобладание. Для решения этой задачи производится поиск линейной аппроксимации для малых частей шифра, для которых ее можно найти перебором. Далее эти аппроксимации объединяются, если это возможно. Для того, чтобы вычислить преобладание полученной аппроксимации всего шифра используется следующая лемма.

Лемма 1 (Мацуи [14]). Пусть $Z_1, \ldots, Z_m$ — независимые случайные булевы переменные, причем, переменная Z_i равна нулю с вероятностью p_i. Тогда выполняется выражение:

$$Pr\left(\bigoplus_{i=1}^{m} Z_i = 0\right) = \frac{1}{2} + 2^{m-1}\prod_{i=1}^{m}\left(p_i - \frac{1}{2}\right).$$

Заметим, что эта лемма работает в том случае, если переменные независимы. Для линейных аппроксимаций шифров, в большинстве случаев, методы основанные на таком предположении работают хорошо.

Метод, используемый в настоящей работе, основан на оценке преобладания линейной аппроксимации шифра. Заметим, что в статье [17] был описан так называемый эффект линейных оболочек, имеющий место в том случае, если связь между одними и теми же разрядами открытого текста и шифртекста может быть аппроксимирована различными линейными выражениями, что может быть использовано в процессе криптоанализа. В последнее время более точные исследования, проведенные в работе [16], показали, что предположения, на которых строилась теория этого эффекта, некорректны и он не влияет на стойкость шифров. Поэтому, в настоящей работе мы этот эффект не рассматриваем.

Очевидно, что проведение атаки методами линейного криптоанализа невозможно, если количество пар (открытый текст, шифртекст), необходимых для атаки, превышает 2^b, где b — длина блока, либо сложность атаки превышает сложность полного перебора ключей.

3. Обобщенные клеточные автоматы

В этом разделе мы кратко опишем методы построения обобщенных клеточных автоматов, являющихся основой для рассматриваемых блочных шифров.

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 для каждой вершины v_i, входящие в нее ребра пронумерованы числами $1, \ldots, d_i$.

В настоящей работе мы будем рассматривать лишь клеточные автоматы, графы которых не имеют кратных ребер.

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 автомат работает по шагам. На шаге с номером t посредством локальной функции связи вычисляются новые значения ячеек:

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

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 $(m_1(t), m_2(t), \ldots, m_N(t))$.

Назовем однородным обобщенным клеточным автоматом обобщенный клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f, то есть 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 регулярный граф, 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.

Для криптостойкости шифра большое значение имеет выбор графа обобщенного клеточного автомата. Согласно работе [4], хорошим выбором являются графы Рамануджана [8, 10, 12]. Мы не будем подробно останавливаться на этом, поскольку результаты настоящей работы не зависят от выбора семейства графов.

Кроме того, весьма важным является правильный выбор локальной функции связи обобщенного клеточного автомата, требования к которой сформулированы автором в работе [4]. Семейство функций, удовлетворяющих всем необходимым требованиям, построено автором в работе [3]. В настоящей статье ради увеличения общности мы ослабим эти требования и будем считать, что локальная функция связи является равновесной функцией, для нелинейности Λ которой справедливо неравенство $\Lambda \geqslant 2^{d-1} - 2^{\lfloor \frac{d}{2} \rfloor}$. Например, такие функции могут быть получены путем конкатенации бент-функций по следующим формулам [7]:

$$g_1(u, x_1, x_2, \ldots, x_{2k}) = (1 \oplus u)\beta_1(x_1, \ldots, x_{2k}) \oplus u\beta_2(x_1, \ldots, x_{2k}); \tag{2}$$

$$g_2(v, u, x_1, x_2, \ldots, x_{2k}) = (1 \oplus v)\left((1 \oplus u)\beta_1(x_1, \ldots, x_{2k}) \oplus u\beta_2(x_1, \ldots, x_{2k})\right) \oplus \\ \oplus v\left((1 \oplus u)\beta_3(x_1, \ldots, x_{2k}) \oplus u\beta_4(x_1, \ldots, x_{2k})\right), \tag{3}$$

где β_i, $i = 1, 2, 3, 4$ — бент-функции, такие, что $|\beta_1| + |\beta_2| = 2^n$ и $|\beta_3| + |\beta_4| = 2^n$ (здесь $|\beta|$ — вес функции β).

4. Конструкция блочного шифра

Кратко опишем здесь рассматриваемое семейство блочных шифров. Более подробное описание приведено в работе [2]. Семейство основано на обобщенных клеточных автоматах, использованию которых в задачах криптографии посвящен ряд работ, в том числе [5, 1].

В работе [4] 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; $c \in B^s$ — некоторая константа, вес которой приблизительно равен половине длины; s — длина константы c.

В качестве структуры шифров используется схема Фейстеля. В работе [2] использовалась классическая схема Фейстеля, однако результаты, изложенные в настоящей работе, тривиально переносятся на широкий набор вариантов и обобщений схемы Фейстеля.

Итак, шифр основан на следующем раундовом преобразовании:

$$L_i = R_{i-1}; R_i = L_{i-1} \oplus S_{c_i}^A(key_i, R_{i-1}),$$

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.

Алгоритм шифрования состоит из нескольких раундов, причем число раундов должно быть не меньше трех. Из соображений удобства можно рекомендовать четное число раундов. В работе [2] рекомендовалось использовать четыре раунда и рассматривалась простая процедура распределения ключей — ключ разбивался на две равные части $key = (key_1, key_2)$, используемые в качестве раундовых ключей двух первых раундов. Раундовые ключи двух оставшихся раундов определялись по формулам: $key_3 = rol(key_1, m/2)$, $key_4 = rol(key_2, m/2)$, где rol — функция, производящая циклический сдвиг первого операнда влево, на количество разрядов, равное второму аргументу; m — длина подключа, равная половине длины ключа.

Результаты настоящей работы не зависят от процедуры распределения ключей (хотя неудачный выбор таковой процедуры может существенно снизить криптостойкость).

5. Исследование стойкости по отношению к линейному криптоанализу

Мы будем считать, что на основе линейных аппроксимаций локальных функций связи удалось получить аппроксимацию всего шифра. Пусть такая аппроксимация получена из N_A аппроксимаций локальных функций связи для различных ячеек, на различных шагах. Будем также считать, что каждая используемая линейная аппроксимация локальной функции связи существенно зависит не менее чем от $\varkappa$ переменных.

Пусть локальная функция связи обобщенного клеточного автомата имеет нелинейность $\Lambda(g)$. Напомним, что под нелинейностью $\Lambda(g)$ булевой функции g понимается расстояние Хэмминга между g и множеством аффинных функций (более подробно см. [7]).

Очевидно, что для преобладания $\varepsilon_1(g,d)$ любой линейной аппроксимации d-местной локальной функции связи g выполняется неравенство:

$$|\varepsilon_1(g,d)| \leqslant \frac{1}{2} - \frac{\Lambda(g)}{2^d}.$$

Заметим, что количество линейных аппроксимаций локальных функций связи, входящих в аппроксимацию t шагов обобщенного клеточного автомата можно оценить как $N_A \geqslant \varkappa(t-1)+1$. Действительно, не менее, чем одна аппроксимация входит на последнем шаге и не менее, чем $\varkappa$ — на каждом предыдущем.

С помощью леммы Мацуи мы можем оценить преобладание $\varepsilon_t(g,d)$ линейной аппроксимации, соответствующей t шагам клеточного автомата:

$$|\varepsilon_t(g,d)| = 2^{N_A-1}|\varepsilon_1(g,d)|^{N_A} \leqslant 2^{N_A-1}\left(\frac{1}{2} - \frac{\Lambda(g)}{2^d}\right)^{N_A} \leqslant 2^{\varkappa(t-1)}\left(\frac{1}{2} - \frac{\Lambda(g)}{2^d}\right)^{\varkappa(t-1)+1}.$$

Заметим, что в шифровании участвует константа c. Ее наличие приводит к возможности роста модуля преобладания линейных аппроксимаций на первом шаге. Это обстоятельство может влиять также и на последующие шаги. Для его нивелирования следует добавить дополнительный шаг на каждом раунде и принять меры к тому, чтобы все ячейки клеточного автомата на первом шаге существенно зависели хотя бы от одного разряда подблока или раундового ключа. Для этого ячейки, в которые записываются константы, а также нумерацию ребер, следует выбирать так, чтобы это свойство выполнялось. Вопрос о наиболее подходящей для этих целей локальной функции связи требует отдельных исследований. Мы будем считать, что параметры выбраны таким образом, что этот эффект пренебрежимо мал после первого шага. В связи с изложенным, в дальнейшем мы не будем учитывать первый шаг каждого раунда при оценивании преобладаний.

Теперь, с помощью леммы Мацуи, с учетом вышеизложенного, оценим преобладание $\varepsilon_{t,r}(g,d)$ для линейной аппроксимации r раундов шифра:

$$|\varepsilon_{t,r}(g,d)| = 2^{r-1}|\varepsilon_{t-1}(g,d)|^r \leqslant 2^{\varkappa r(t-2)+r-1}\left(\frac{1}{2} - \frac{\Lambda(g)}{2^d}\right)^{\varkappa r(t-2)+r}. \qquad (4)$$

Будем рассматривать только локальные функции связи, нелинейность которых имеет следующую нижнюю оценку:

$$\Lambda \geqslant 2^{d-1} - 2^{\lfloor \frac{d}{2} \rfloor}, \tag{5}$$

где d — число переменных. В частности, эта оценка справедлива для нелинейности локальных функций связи, построенных по формулам (2), (3).

Из соотношений (4) и (5) получим следующее:

$$|\varepsilon_{t,r}(g,d)| \leqslant 2^{\varkappa r(t-2)+r-1} \left(\frac{2^{\lfloor \frac{d}{2} \rfloor}}{2^d} \right)^{\varkappa r(t-2)+r} = 2^{-\left((\varkappa r(t-2)+r)\left(\lceil \frac{d}{2} \rceil - 1\right)+1\right)}.$$

Оценим теперь число пар (открытый текст, шифртекст), необходимых для взлома r-рандового шифра с помощью алгоритма 2. Обозначим его N_L. В соответствии с таблицей 2 можно считать, что для того, чтобы взлом оказался успешным с достаточно большой вероятностью, должно выполняться неравенство $N_L \geqslant \frac{1}{\varepsilon^2}$, причем следует использовать аппроксимацию $r-1$ раундов шифра. Отсюда получаем, что для нашего случая, число таких пар $N_{L2}(t,r,d)$ оценивается как

$$N_{L2}(t,r,d) \geqslant \varepsilon_{t,r-1}^{-2}(g,d) \geqslant 2^{2\left((\varkappa(r-1)(t-2)+r-1)\left(\lceil \frac{d}{2} \rceil - 1\right)+1\right)} \tag{6}$$

Кроме того, учитывая, что функция S по целому ряду свойств близка к псевдослучайной и каждый разряд ее выхода зависит от всех разрядов входа, для выполнения алгоритма 2 необходим перебор всех ключей последнего раунда. Пусть $C(t,r,\|key_r\|)$ — количество ключей, которые необходимо опробовать. Оно составляет:

$$C(t,r,\|key_r\|) = 2^{\|key_r\|} N_{L2} \geqslant 2^{\|key_r\|+2\left((\varkappa(r-1)(t-2)+r-1)\left(\lceil \frac{d}{2} \rceil - 1\right)+1\right)}, \tag{7}$$

где $\|key_r\|$ — длина раундового ключа на раунде r.

Кроме использования алгоритма 2, возможно использование алгоритма 1, с помощью которого можно определить некоторые разряды ключа. Для этого требуется линейная аппроксимация всех r раундов шифра. Обозначим количество пар (открытый текст, шифртекст), необходимых для взлома шифра с помощью этого алгоритма, как $N_{L1}(t,r,d)$. В соответствии с таблицей 1, для него справедливо выражение:

$$N_{L1}(t,r,d) \geqslant \varepsilon_{t,r}^{-2}(g,d) \geqslant 2^{2\left((\varkappa r(t-2)+r)\left(\lceil \frac{d}{2} \rceil - 1\right)+1\right)}. \tag{8}$$

Очевидно, что для того, чтобы шифр был стоек к рассматриваемым методам криптоанализа, достаточно, чтобы выполнялось хотя бы одно из условий (9), (10):

$$C(t,r,\|key_r\|) \geqslant 2^{\|key\|}, \tag{9}$$

$$N_{L2} > 2^b, \tag{10}$$

а также, условие

$$N_{L1} > 2^b, \tag{11}$$

где $\|key\|$ — длина ключа шифра, b — длина блока.

Применительно к рассматриваемым шифрам, подставляя в неравенства (9), (10), (11), выражения (7), (6), (8) и производя очевидные преобразования, получим, что для того, чтобы такой шифр был стоек к линейному криптоанализу, достаточно, чтобы выполнялось хотя бы одно из условий (12), (13):

$$\varkappa(r-1)(t-2)+r-1 \geqslant \frac{\|key\|-\|key_r\|-2}{2\left\lceil\frac{d}{2}\right\rceil-2}, \tag{12}$$

$$\varkappa(r-1)(t-2)+r-1 > \frac{b-2}{2\left\lceil\frac{d}{2}\right\rceil-2}, \tag{13}$$

а также, условие

$$\varkappa r(t-2)+r > \frac{b-2}{2\left\lceil\frac{d}{2}\right\rceil-2}, \tag{14}$$

где $\|key\|$ — длина ключа шифра; $\|key_r\|$ — длина ключа последнего раунда; b — длина блока.

Полученные условия являются основным результатом настоящей работы. Следует отметить, что они не зависят от графа клеточного автомата и выполняются при использовании любой локальной функции связи, нелинейность которой удовлетворяет неравенству (5).

Заметим также, что в случае, если граф обобщенного клеточного автомата имеет большой коэффициент реберного расширения, то за счет лучшего перемешивания, криптографические свойства шифров, по-видимому, существенно улучшатся. Этот эффект требует дальнейшего изучения, выходящего за рамки настоящей статьи.

6. Примеры

В качестве примеров рассмотрим шифры с длиной блока 128 бит и длиной ключа — 128 и 256 бит. В качестве локальной функции связи выберем функцию, приведенную в качестве примера в работе [2]:

$$f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_3x_5 \oplus x_3x_4 \oplus x_5x_6 \oplus x_3x_5 \oplus x_1x_5 \oplus x_1 \oplus x_2 \oplus 1. \tag{15}$$

Эта функция не имеет линейных аппроксимаций, существенно зависящих лишь от одной входной переменной, но имеет аппроксимацию, существенно зависящую от двух входных переменных и равную $x_2 \oplus x_3$, с преобладанием равным $\frac{1}{4}$. Таким образом, для этой функции $\varkappa = 2$.

Итак, качестве примера, рассмотрим шифр со следующими параметрами:

- степень графа $d = 6$;
- $\varkappa = 2$;
- длина блока $b = 128$;
- длина ключа $\|key\| = 128$;
- длина подключа на последнем раунде $\|key_r\| = 64$;
- число раундов $r = 4$.

Оценим число t шагов клеточного автомата в каждом раунде:

• из неравенства (12) получаем, что $t \geqslant 5$;

• из неравенства (13) получаем, что $t \geqslant 7$;

• из неравенства (14) получаем, что $t \geqslant 6$.

Таким образом, для данных параметров должно выполняться $t \geqslant 7$.

Другой пример:

• степень графа $d = 6$;

• $\varkappa = 2$;

• длина блока $b = 128$;

• длина ключа $\|key\| = 256$;

• длина подключа на последнем раунде $\|key_r\| = 128$;

• число раундов $r = 4$.

Оценим значение t:

• Из неравенства (12) получаем, что $t \geqslant 7$.

• Из неравенства (13) получаем, что $t \geqslant 7$.

• Из неравенства (14) получаем, что $t \geqslant 6$.

Таким образом, для данных параметров должно выполняться $t \geqslant 7$.

7. Заключение

Таким образом, в статье получены условия, при выполнении которых обеспечивается стойкость блочных шифров, основанных на обобщенных клеточных автоматах к классическому линейному криптоанализу. Следует заметить, что эти условия получены для худшего случая. Конкретный шифр из этого семейства может обладать более высокой криптостойкостью. Результаты статьи обладают достаточной общностью, поскольку не зависят от графа клеточного автомата и остаются справедливыми при использовании различных вариантов схемы Фейстеля. В то же время, результаты относятся только к классическому методу линейного криптоанализа.

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

В заключение автор хотел бы выразить благодарность Д.А. Жукову и А.Е. Жукову за ценное обсуждение.

Список литературы

1. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10. Режим доступа: http://technomag.edu.ru/doc/241308.html (дата обращения 30.04.2013).
2. Ключарев П.Г. Блочные шифры, основанные на обобщенных клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2012. № 12. DOI: 10.7463/0113.0517543.

3. Ключарев П.Г. Обеспечение криптографических свойств обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 3. Режим доступа: http://technomag.edu.ru/doc/358973.html (дата обращения 30.04.2013).
4. Ключарев П.Г. Построение псевдослучайных функций на основе обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 10. DOI: 10.7463/1112.0496381.
5. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34–41.
6. Biryukov A., Cannière C.D. Linear cryptanalysis for block ciphers // Encyclopedia of Cryptography and Security / Tilborg Henk C.A., Jajodia Sushil (Eds.). 2nd ed. Springer US, 2011. P. 722–725. DOI: 10.1007/978-1-4419-5906-5_589.
7. Cusick T., Stănică P. Cryptographic Boolean functions and applications. Academic Press, 2009. 232 p.
8. 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.)
9. Heys H.M. A tutorial on linear and differential cryptanalysis // Cryptologia. 2002. Vol. 26, no. 3. P. 189–221. DOI: 10.1080/0161-110291890885
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. DOI: 10.1090/S0273-0979-06-01126-8ю
11. Knudsen L., Robshaw M. The block cipher companion. Springer, 2011. 267 p. DOI: 10.1007/978-3-642-17342-4.
12. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. 1988. Vol. 8, no. 3. P. 261–277. DOI: 10.1007/BF02126799.
13. Matsui M. Linear cryptanalysis method for des cipher // Advances in Cryptology — EUROCRYPT'93. Springer, 1994. P. 386–397. DOI: 10.1007/3-540-48285-7_33.
14. Matsui M., Yamagishi A. A new method for known plaintext attack of FEAL cipher // Advances in Cryptology — Eurocrypt'92. Springer, 1993. P. 81–91. DOI: 10.1007/3-540-47555-9_7.
15. Mirza F. Block ciphers and cryptanalysis. 1998. Available at: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.4708, accessed 30.04.2013.
16. Murphy S. The effectiveness of the linear hull effect // Rapport technique RHUL-MA-2009-17. Royal Holloway. 2009. Vol. 4, no. 1. P. 4–5.
17. Nyberg K. Linear approximation of block ciphers // Advances in Cryptology — EUROCRYPT'94. Springer, 1995. P. 439–444. DOI: 10.1007/BFb0053460.

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

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

electronic scientific and technical journal

Investigation of strength of block ciphers based on generalized cellular automata against linear cryptanalysis

 # 05, May 2013

DOI: 10.7463/0513.0574231

Klyucharev P. G.

Bauman Moscow State Technical University
105005, Moscow, Russian Federation
pk.iu8@yandex.ru

In this paper the strength of the block ciphers, based on the generalized cellular automata, against classical linear cryptanalysis was investigated. A linear cryptanalysis is one of the main standard techniques for cracking block ciphers. Sufficient condition for the strength of this family of ciphers against linear cryptanalysis is the main result of this paper. This condition was used to demonstrate that with arbitrary graph of a cellular automaton in case of the right selection of local connecting function and other parameters in order to create ciphers with the key length of 128 and 256 bits and block length of 128 bits which couldn't be cracked by linear cryptanalysis when using 4 rounds and 7 steps of a cellular automaton per round.

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 30.04.2013.
2. Kliucharev P.G. Blochnye shifry, osnovannye na obobshchennykh kletochnykh avtomatakh [Construction of pseudo-random functions based on generalized cellular automata]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 12. DOI: 10.7463/0113.0517543.
3. Kliucharev P.G. Obespechenie kriptograficheskikh svoistv obobshchennykh kletochnykh avtomatov [On cryptographic properties of generalized cellular automatons]. *Nauka i obrazo-*

vanie 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 30.04.2013.

4. 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.
5. 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.
6. Biryukov A., Cannière C.D. Linear cryptanalysis for block ciphers. In: Tilborg Henk C.A., Jajodia Sushil (Eds.) *Encyclopedia of Cryptography and Security*. 2nd ed. Springer US, 2011, pp. 722–725. DOI: 10.1007/978-1-4419-5906-5_589.
7. Cusick T., Stănică P. *Cryptographic Boolean functions and applications*. Academic Press, 2009. 232 p.
8. 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.)
9. Heys H. M. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 2002, vol. 26, no. 3, pp. 189–221. DOI: 10.1080/0161-110291890885.
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. DOI: 10.1090/S0273-0979-06-01126-8.
11. Knudsen L., Robshaw M. *The block cipher companion*. Springer, 2011. 267 p. DOI: 10.1007/978-3-642-17342-4.
12. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277. DOI: 10.1007/BF02126799.
13. Matsui M. Linear cryptanalysis method for des cipher. *Advances in Cryptology — EUROCRYPT'93*. Springer, 1994, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.
14. Matsui M., Yamagishi A. A new method for known plaintext attack of FEAL cipher. *Advances in Cryptology — Eurocrypt'92*. Springer, 1993, pp. 81–91. DOI: 10.1007/3-540-47555-9_7.
15. Mirza F. *Block ciphers and cryptanalysis*. 1998. Available at: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.4708, accessed 30.04.2013.
16. Murphy S. The effectiveness of the linear hull effect. *Rapport technique RHUL-MA-2009-19*. Royal Holloway, 2009, vol. 4, no. 1, pp. 4–5.
17. Nyberg K. Linear approximation of block ciphers. *Advances in Cryptology — EUROCRYPT'94*. Springer, 1995, pp. 439–444. DOI: 10.1007/BFb0053460.