УДК 621. 3.06

И.Д. ГОРБЕНКО, д-р техн. наук, К.Е. ЛИСИЦКИЙ

О ДИНАМИКЕ ПРИХОДА ШИФРОВ К СЛУЧАЙНОЙ ПОДСТАНОВКЕ ПРИ ИСПОЛЬЗОВАНИИ S-БЛОКОВ С ПОКАЗАТЕЛЯМИ НЕЛИНЕЙНОСТИ БЛИЗКИМИ К ПРЕДЕЛЬНЫМ

Введение

В ряде работ [1, 2 и др.] поднимается вопрос о построении S-блоков с показателями нелинейности близкими к максимально возможным значениям. В частности, считается большим достижением получение случайных S-блоков с показателем нелинейности N_f = 104 (известно, что S-блоки шифра AES, построенные детерминированным способом, имеют показатель нелинейности N_f = 112). Полагается, что применение таких S-блоков может позволить улучшить динамику перехода некоторых шифров, например шифра Калина, к состоянию случайной подстановки.

В этой работе хотим высказать свою позицию к перспективам использования таких S-блоков. Будет показано, что для Rijndael-подобных шифров, к которым относится сам шифр Rijndael, а также шифры Калина, Anubis, ADE. GrandCru и некоторых других, конструкция циклового преобразования для любых S-блоков не позволяет реализовать переход по линейным показателям к случайной подстановке менее чем за три цикла.

Определения, связанные с понятием нелинейности S-блоков

Для изучения свойств S-блоков широко используется аппарат булевых функций. Напомним основные определения, относящиеся к линейным показателям булевых функций f и S-блоков, построенных на их основе. Воспользуемся обобщающим материалом из диссертации Широкова А.В. [3].

Аффинность и нелинейность

Определение 1 [4]. *Аффинной называется функция* f *над* V_n *вида*

$$f = a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus c,$$

где $a_j,\ c \in \mathbf{GF}(2),\ j = 1, 2, \ldots, n,\ V_n$ – n-мерное векторное пространство над полем $\mathbf{GF}(2)$.

Кроме того, функция f называется *линейной*, если $c = 0$ [4]. Последовательность аффинных (или линейных) функций называется *аффинной* (*или линейной*) *последовательностью*.

Определение 2. *Расстоянием Хэмминга* $d(f, g)$ *между последовательностями двух функций* f *и* g *является количество позиций, в которых последовательности этих функций различаются* [4] (*хэмминговый вес таблицы истинности функции* $f(x) \oplus g(x)$, *где* $x = \{x_1, x_2, \ldots, x_n\}$).

В фундаментальной работе Майера и Штаффельбаха [5] минимальное расстояние функции до любой функции с линейной структурой определено как мера нелинейности.

Определение 3 [4, 6]**.** *Нелинейность функции* N_f – *это минимальное расстояние Хэмминга между функцией* f *и всеми аффинными функциями над* $\mathbf{GF}\left(2^n\right)$:

$$N_f = \min_{i=1, 2, \ldots, 2^{n+1}} \left\{ d(f, \varphi_i) \right\},$$

где $\varphi_1, \varphi_2, \ldots, \varphi_{2^{n+1}}$ аффинные функции из V_n.

Установлено [4], что для произвольной функции f нелинейность N_f над $\mathbf{GF}\left(2^n\right)$ может достигать значения:

$$N_f \le 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Для сбалансированной функции f над $\mathbf{GF}\left(2^n\right)$ $(n \ge 3)$ нелинейность N_f может достигать значений [4]:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2, & n = 2k, \\ \left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor, & n = 2k+1, \end{cases}$$

где $\lfloor x \rfloor$ – максимальное четное целое, меньшее либо равное x.

Приведенные определения переносятся на S-блоки следующим образом.

Определение 4. (Критерий нелинейности для S-блоков). В [6] *нелинейность N_S S-блока определяется как худший случай нелинейности булевых функций соответствующих S-блоку:*

$$N_S = \min_f N_f = \min_f \left\{ N_f \,\middle|\, f(x) = c \bullet S(x), c \ne 0 \right\},$$

где минимизация ведется по всем возможным выходным битовым комбинациям $f(x) = \oplus_{i=1}^{m} c_i f_i(x) = c \bullet S(x)$, соответствующим всем ненулевым значениям маскового вектора $c = (c_1, \ldots, c_m)\big|_{1\times m}$, $x \bullet y$ – скалярное произведение векторов x и y.

Нелишним будет и определение 5.

Определение 5. (Линейная аппроксимационная таблица *LAT* для S-блоков). В [6] отмечается, что линейная аппроксимационная таблица (*LAT*) является важным проверочным критерием для измерения безопасности S-блоков против атак линейного криптоанализа, которая была введена Мацуи на Еврокрипте 93 при описании теоретической атаки на DES.

Для данного S-блока $S(x): GF(2^n) \to GF(2^m)$ линейная аппроксимационная таблица, имеющая вход в w-ю строку и c-ю колонку, определяется как

$$LAT(w,c) = \left| x / [c \bullet S(x) = w \bullet x] \right| - 2^{n-1}.$$

где $w \bullet x$ и $c \bullet S(x)$ − скалярные произведения соответствующих векторов (блоков данных на входе и выходе S-блока с масками входа и выхода).

Приведем также одну важную для этой работы лемму из работы [6].

Лемма. (Соотношение между нелинейностью S-блока и максимальным значением элемента LAT) *Нелинейность S-блока может быть представлена в терминах максимального значения элемента LAT как*

$$N_s = \min_f N_f = 2^{n-1} - \max_{w,c \in F_2^n} \left| LAT(w,c) \right| \cdot$$

Определение 6 [7]. (Линейная вероятность): *Линейная вероятность LP^f для ключезависимой функции f с n-битным входом x и n-битным выходом y ($x, y \in GF(2^n)$) есть*

$$LP^f(w \to c) = \left(\frac{LAT(w,c)}{2^{n-1}} \right)^2 \cdot$$

Определение 7. ($DP_{\max}^f$ и $LP_{\max}^f$): *Максимальное значение линейной вероятности для ключезависимой функции f определяется как*

$$LP_{\max}^{f} = \max_{w,\, c \neq 0,} LP^{f[k]}(w \to c).$$

Правило вычисления линейных аппроксимационных характеристик определяется накапливающей леммой [8].

Накапливающая лемма. *Пусть* x_i, $i = 1, \ldots, t$ *будут независимыми случайными переменными, каждая из которых принимает значение* 0 *с вероятностью* p_i' *и* 1 *с вероятностью* $1 - p_i'$. *Тогда вероятность того, что* $x_1 \oplus x_2 \oplus, \ldots, \oplus x_t = 0$

$$\frac{1}{2} + 2^{t-1} \cdot \prod_{i=1}^{t} \left(p_i' - \frac{1}{2} \right).$$

В соответствии с этой леммой, если аппроксимация включает в себя L S-блоков $\left(p_i = p_i' - \frac{1}{2} \right)$, то комбинированная вероятность для их суммы

$$p = 2^{L-1} \cdot \prod_{i=1}^{L} p_i \cdot$$

Анализ реальных данных

В табл. 1 представлены результаты расчетов по определению распределения значений максимумов линейных корпусов выборки из байтовых подстановок на основе интегрального закона распределения вероятностей максимумов смещений, полученные в работе [9]:

$$D_{\max}(X) \approx e^{-e^{\frac{32-X}{2}}}. \qquad (1)$$

Таблица 1

Распределения значений максимумов линейных корпусов
на основе интегрального закона распределения вероятностей (1)

k^* (X_1, X_2)	Pr(k *)	Число значений (расчет)	Число значений (эксперимент)
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5{,}6\ 10^{-4} - 3{,}4110^{-7} = 5{,}6\ 10^{-4}$	0,14	0
30 (30,28)	$0{,}064 - 5{,}6\ 10^{-4} = 0{,}0638$	16	10
32 (32,30)	0,368–0,064 = 0,304	78	86
34 (34,32)	0,692 – 0,304 = 0,388	99	98
36 (36,34)	0,874 – 0,692 = 0,181	46	46
38(38,36)	0,9518 – 0,874 = 0,078	19	10
40 (40,38)	0,9821 – 0,9518 = 0,03	8	6
42 (42,40)	0,9933 – 0,9821 = 0,011	3	0
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

Заметим, что по результатам ранее выполненных теоретических и экспериментальных исследований, значения максимума смещения линейной аппроксимационной таблицы случайной подстановки степени 2^8 равно 32 (расчет) и 32 - 34 (эксперимент) [10]. Видно, что результаты экспериментов практически повторяют результаты расчетов.

Отметим, что в соответствии с соотношением (1) вероятность породить случайный S-блок с показателем нелинейности 24 (104) равна $5{,}92 \cdot 10^{-25}$. Для показателя нелинейности 22 (106) уже имеем вероятность $7{,}25 \cdot 10^{-67}$, так что порождение S-блоков с показателем нелинейности $N_f = 104$ является действительно вычислительно непростой задачей.

Выше было отмечено, что S-блоки шифра AES, построенные с использование детерминированных методов, имеют еще меньший показатель нелинейности 16 (112). Но структура этого S-блока, допускающая алгебраическое описание, считается его потенциальной

слабостью [11]. По-видимому, это и побуждает исследователей на поиски подходов, позволяющих строить S-блоки с высокими показателями нелинейности не детерминированными (иными) методами. Покажем, что эта задача во многих практических ситуациях не имеет перспективы.

Идея развиваемого далее подхода изложена в работе [12] для дифференциальных показателей шифров. Она состоит в оценке минимального числа активных (задействованных S-блоков), после прохождения которых шифр становится случайной подстановкой. Это минимальное число определяется дифференциальными и линейными показателями самих S-блоков, применяемых в шифре, конструкциями цикловых линейных преобразований, а также значениями показателей доказуемой стойкости шифра, зависящими от размера его битового входа.

В работе [12] связь между отмеченными показателями определена в виде двух соотношений:

$$IPS_D = (\,DP^{\pi}_{\max}\,)^k,\;\; IPS_L = 2^{k-1}\cdot\left(LP^{\pi}_{\max}\right)^k. \qquad (1)$$

Здесь $DP^{\pi}_{\max}$ и $LP^{\pi}_{\max}$ – максимальные значения дифференциальной и линейной вероятностей подстановочных преобразований $\pi(x)$. IPS_D (Differential Indicator of Provable Security) – дифференциальный показатель доказуемой безопасности и IPS_L (Linear Indicator of Provable Security) – линейный показатель доказуемой безопасности, $k = k_{\min}$ – минимальное число активных S-блоков, участвующих в формировании перехода шифра к случайной подстановке.

Приведем здесь значения минимального числа активных S-блоков 128-битного шифра, обеспечивающих приход шифра к состоянию случайной подстановки, следующие из соотношения (2), полагая при этом, что в активных S-блоках используются наиболее вероятные переходы.

Для показателя нелинейности S-блока 112 (как в шифре Rijndael) максимальная вероятность смещения S-блока равна $(16/128)^2 = 2^{-6}$. Здесь $k_{\min} = 24$ (следует из уравнения $2^{-121} = 2^{k-1}(2^{-6})^k = 2^{5k-1}$), 2^{-121}– показатель доказуемой стойкости 128-битного шифра [11]).

Для показателя нелинейности S-блока 104 (24) соответственно имеем $(24/128)^2 = 2^{-4,83}$ и $k_{\min} = 31{,}59$.

Для показателя нелинейности S-блока 96 (32) получаем $(32/128)^2 = 2^{-4}$, $k_{\min} = 40$.

Для показателя нелинейности S-блока равного 94 (34) имеем $(34/128)^2 = 2^{-3,8}$ и тогда $k_{\min} = 42.85$.

Воспользуемся соображениями, высказанными в работе [12] в отношении динамических показателей прихода шифров к показателям случайной подстановки по дифференциальным показателям. Приведем эти результаты в переложении на линейные показатели шифров

1. Для шифра **Rijndael**, в котором, как отмечено выше, применяются S-блоки с показателем нелинейности 112 (16), результат $LP^{\pi}_{\max} = (16/128)^2 = = 2^{-6}$ совпадает с максимальным значение дифференциальной вероятности $DP^{\pi}_{\max}$. $DP^{\pi}_{\max}$. Здесь $k_{\min} = 24$ (следует из уравнения $2^{-121} = 2^{k-1}(2^{-6})^k = 2^{5k-1}$), $IPS_L = 2^{-121}$ – линейный показатель доказуемой стойкости 128-битного шифра [6]).

Поэтому этот шифр приходит к состоянию случайной подстановки по линейным показателям через четыре цикла ($r_{\min} = 4$).

2. Шифр **Калина**. В [13] показано, что на трех циклах зашифрования в шифре Калина активными становятся минимум 1 + 8 + 16 = 25 S-блоков, чего недостаточно для покрытия минимального числа S-блоков шифра Калина с показателем нелинейности 94 - 96. Для показателя нелинейности S-блока 96 (32) получаем $(32/128)^2 = 2^{-4}$, $k_{\min} = 40$, т.е. в этом случае приходим к результату $r_{\min} = 4$.

Для показателя нелинейности S-блока 104 (24) соответственно имеем $(24/128)^2 = 2^{-4,83}$ и $k_{\min} = 31,59$, т.е. применение S-блоков с показателем нелинейности 104 (24) не позволяет войти в границы минимального числа S-блоков $k_{\min} = 25$ на трех циклах.

3. Шифр **IDEA NXT** (FOX). Для версии шифра FOX-64 (с 64-битными входами и выходами) имеем.

Показатель нелинейности для S-блоков есть $LP^{\pi}_{\max} = (32/128)^2 = 2^{-4}$ [14] и совпадает с дифференциальным показателем $DP^{\pi}_{\max} = \frac{16}{256} = 2^{-4}$.

Функция f32 внутреннего уровня здесь включает в себя два слоя из четверок байтовых S-блоков с промежуточной рассеивающей частью, представляющей собой линейную 4×4-мультиперестановку в поле $GF(2^8)$, и три промежуточных сложения с цикловыми подключами. В результате в первом цикле активизируется минимум пять S-блоков (один S-блок первого слоя и четыре второго). Из уравнения $2^{k-1}(2^{-4})^k = 2^{-27}$ следует $k_{\min} = 8,66$ видно, что одного цикла преобразования f32 недостаточно для прихода f32 к случайной подстановке (2^{-27}– показатель стойкости 32-битного шифра). В следующем цикле будут активизированы все его восемь S-блоков и, здесь на два цикла приходится 13 активных S-блоков. Функция f32 становится случайной подстановкой. Но для 64-битного шифра уравнение (1) имеет вид $2^{k-1}(2^{-4})^k = 2^{-58}$ (здесь 2^{-4} максимальное значение дифференциальной вероятности S-блоков шифра FOX), откуда следует $k_{\min} = 19$. В результате приходим к выводу, что и двух циклов шифра FOX не хватает для покрытия минимального числа активных S-блоков $k_{\min} = 19$, и, следовательно, для шифра FOX-64 следует ожидать $r_{\min} = 3$. В то же время эксперименты с полномасштабным шифром с 16-битными переходами показывают результат $r_{\min} = 2$. Остается заметить, что в этом случае нужно рассматривать уравнение $2^{-12} = 2^{k-1} \cdot (2^{-4})^k \rightarrow k_{\min} = 3,66$ и здесь наличие пяти активных S-блоков первого цикла достаточно для прихода шифра к состоянию случайной подстановки.

4. В 128-битном шифре **FOX** применяется матричное умножение на МДР матрицу 8×8 и опять двухслойное нелинейное преобразование. Поэтому на первом цикле имеем 9 активных S-блоков. На двух циклах их будет уже 9 +16 = 25, и, следовательно, для прихода шифра к состоянию случайной подстановки в этом случае нужен еще один цикл: $r_{\min} = 3$ (здесь $k_{\min} = 40$).

5. Для конструкция **функции усложнения M-64 шифра Мухомор-128** имеем уравнение $2^{k-1}(2^{-4,16})^k = 2^{-58}$ (показатель нелинейности для S-блоков шифра Мухомор равен 30), откуда $k_{\min} = 18,03$. Выше было отмечено, что схема включения SL преобразований обеспечивает активизацию всех 12-ти S-блоков первого цикла. В этом случае для прихода M-64 к состоянию случайной подстановки потребуется $r_{\min.} = 2$ цикла.

Последующее преобразование схемы Лея - Месси верхнего уровня переносит эффект перемешивания битов входа на весь 128-битный блок данных (обеспечивает зависимость битов выхода от всех битов входа). Однако для покрытия минимального числа активных S-блоков $k_{\min} = 38,29$ потребуется $r_{\min.} = 4$ цикла.

Заметим, что при зашифровании в режиме использования 16-битных сегментов входа и выхода для этого шифра приходим к результату $r_{\min.} = 1$ ($2^{-12} = 2^{k-1} \cdot (2^{-4})^k \rightarrow k_{\min} = 3,66$).

6. Конструкция **функции усложнения M-128 шифра Мухомор-256** (вход в шифр 256 битов) состоит из восьми SL преобразований. Если считать, что на первом цикле задействованными являются минимум 29 S-блоков, формирующих все выходные байты цикла активными, то итеративный шифр, построенный с использованием цикловой функции в виде функции усложнения M-128, будет становиться случайной подстановкой за два цикла ($k_{\min} = 38$) и с большими показателями нелинейности S-блоков.

Шифры с фейстель подобной структурой.

7. Шифр **Лабиринт**, использующий для построения цикловых преобразований вложенные фейстель-подобные структуры, тоже демонстрирует линейные показатели, повторяющие

динамику шифра Мухомор (в экспериментах он тоже становится случайной подстановкой с первого цикла [14]). Но как отмечено выше, в этом шифре использованы мощные доцикловые и послецикловые преобразования, построенные с применением слоев S-блоков, которые вполне могут рассматриваться как дополнительные специфические циклы. Поэтому и в этом случае мы полагаем, что в результатах экспериментов [14] начальные данные для шифра Лабиринт соответствуют сразу трем циклам (все S-блоки третьего цикла активны). Здесь первый цикл с начальным IT и заключительным FT преобразованиями содержит 48 S-блоков.

В табл. 2 для сравнения приводим поцикловые значения максимумов смещений таблиц линейных аппроксимаций для ряда шифров из работы [14] (для 16-битных сегментов). Здесь приводятся данные для 128-битного шифра AES, а также данные для шифров, представленных на украинский конкурс.

Таблица 2

Поцикловые значения максимумов смещений таблиц линейных аппроксимаций шифров со значениями среднеквадратических отклонений

Число циклов	Калина 30 ключей	Мухомор 30 ключей	Лабиринт 1 ключ	AES 1 ключ
1	11008,392± 1785,34	824,742± 20,1286	– 790*	4096
2	817,271± 27,6348	818,621± 25,9742	839*	9216
3	817,718± 21,3851	827,431± 21,2352	-816	826
4	814,19± 26,7792	824,193± 17,8115	832	808
5	837,349± 28,2712	831,753± 25,7731	885	812
6	810,733± 29,3801	814,155± 28,9121	810	834
7	820,384± 20,752	820,975± 20,2673	– 834	828
8	837,917± 23,2539	823,024± 18,853	835	822
9	809,273± 22,186	810,196± 22,9352	– 809	826
10	821,755± 25,5737	821,316± 25,849	– 806	802

Видно, что линейные показатели (на уровне 16-битных сегментов) по динамике прихода к случайной подстановке практически повторяют дифференциальные.

8. Шифр **ГОСТ 28147-89** практически по линейным показателям повторяет дифференциальные. Он приходит к состоянию случайной подстановки на 9 - 10-м циклах.

9. Для **белорусского шифра**, как отмечено выше, цикловое преобразование включает 28 байтовых S-блоков, из которых на первом цикле активизируются минимум 13 (активизируется одна из четырех ветвей входа). Следовательно, и в случае рассмотрения линейных показателей шифру для прихода к случайной подстановке потребуется $r_{\min.}= 2$ цикла. Одновременно становится понятным, что и в этом случае есть запас для использования S-блоков и не с минимальными линейными показателями.

10. Для **шифра Хейса** в лучшем случае для полубайтовых S-блоков с показателем нелинейности, равным 4, уравнение зашифрования, как уже было показано ранее, имеет вид $(18\div20)/2^{16} = 2^{k-1}\ (2^{-2})^k$ (показатель нелинейности полубайтовых S-блоков равен 4). Для S-блоков с показателем нелинейности, равным 4, имеем $k_{\min}= 11$. Если считать, что при побитном линейном преобразовании с полубайтовыми S-блоками реализуется коэффициент ветвления равный 3 (полубайтовый S-блок имеет в среднем на выходе два единичных бита), то приходим к выводу, что этот шифр должен выходить к состоянию случайной подстановки за четыре цикла (первый цикл – один активный S-блок, второй – два, третий – четыре – на три цикла получается семь активных S-блоков).

В табл. 3 приведены поцикловые распределения максимумов таблиц линейных аппроксимаций для полубайтовых S-блоков шифра СЕРПЕНТ и золотых S-блоков из работы [14].

Таблица 3

Поцикловые значения максимумов смещений линейных корпусов шифра Хейса с различными наборами S-блоков

Подстановки		Циклы					
Шифр СЕРПЕНТ		1	2	3	4	5	6
1	3,8,f,1,a,6,5,b,e,d,4,2,7,0,9,c	16384	2048	872	878	808	862
2	f,c,2,7,9,0,5,a,1,b,e,8,6,d,3,4	16384	2048	816	792	786	882
3	8,6,7,9,3,c,a,f,d,1,e,4,0,b,5,2	16384	2048	880	820	816	844
4	0,f,b,8,c,9,6,3,d,1,2,4,a,7,5,e	16384	2048	800	844	856	844
5	1,f,8,3,c,0,b,6,2,5,4,a,9,e,7,d	16384	2048	840	864	838	798
6	f,5,2,b,4,a,9,c,0,3,e,8,d,6,7,1	16384	2048	808	846	820	822
7	7,2,c,5,8,4,6,b,e,9,1,f,d,3,a,0	16384	2048	808	866	830	826
8	1,d,f,0,e,8,2,b,7,4,c,a,9,3,5,6	16384	2048	872	820	826	792
Золотые подстановки							
1	0,3,5,8,6,9,c,7,d,a,e,4,1,f,b,2	16384	2048	800	814	844	786
2	0,3,5,8,6,a,f,4,e,d,9,2,1,7,c,b	16384	2048	824	794	804	868
3	0,3,5,8,6,c,b,7,9,e,a,d,f,2,1,4	16384	1792	808	812	846	782
4	0,3,5,8,6,c,b,7,a,4,9,e,f,1,2,d	16384	1792	864	824	786	794

11. 128-битный шифр **Serpent.** Анализ показывает, что за счет начальной битовой перестановки на первом цикле активизируется в среднем два S-блока. На втором цикле тогда активизируется 32 S-блока (за два цикла получается, что активизируется 2+32 = 34 S-блока). С другой стороны, $2^{-121} = 2^{k-1}\,(2^{-2})^k \rightarrow k_{\min} = 120$. Таким образом, шифр Serpent приходит к состоянию случайной подстановки по линейным показателям за пять циклов ($r_{\min} = 5$). По результатам экспериментов с 16-битными переходами [14] шифр Serpent показывает $r_{\min} = 2$ цикла ($2^{-12} = 2^{k-1}\,(2^{-2})^k \rightarrow k_{\min} = 11$, и для двух циклов получаем $k = 2 + 4$ активных S-блока). Напомним, что авторы разработки заявляли, что три цикла являются для шифра минимально необходимыми для обеспечения зависимости каждого бита выхода от каждого бита входа.

Разберемся теперь с шифрами с не максимально достижимыми значениями нелинейности и δ-равномерности.

Как мы поняли значения минимального числа циклов выхода шифра к состоянию случайной подстановки непосредственно связано с дифференциальными и линейными свойствами S-блоков.

Обратим теперь внимание на то, что в наших расчетах мы ориентировались на значения вероятностей максимумов переходов, близкие к предельно достижимым значениям. В то же время, как показывает анализ, распределение максимумов переходов S-блоков существенно зависит от значений достигаемых максимумов. В табл. 4 представлены результаты, иллюстрирующие зависимость числа максимумов, встречающихся у S-блоков, с разными значениями максимумов.

Из представленных данных следует, что для S-блоков с предельными линейными и дифференциальными показателями (S-блоки шифров ADE, AES, GrandCru, Лабиринт) число значений максимумов получается большим (достаточным для построения дифференциальной и линейной характеристик из максимально вероятных переходов). В то же время для других шифров (S-блоки шифров Iseberg, Khazad, Мухомор и случайные подстановки) со значениями дифференциальных и линейных переходов S-блоков, имеющих максимумы переходов, превышающие предельно достижимые (минимальные) значения, числа этих максимумов выражаются десятками, а то и единицами (их получается мало).

Таблица 4

Зависимость числа максимумов от значений максимумов
для таблиц подстановок различных шифров.

S-блоки шифров	Max ДТ	Число максимумов	Max ЛАТ	Число максимумов
ADE, AES, GrandCru, Лабиринт	4	255	112	1275
FOX	16	125	96	219
Мухомор	8	90	98	8
Iseberg, Khazad	8	80	98	6
Случайные	10	12	96	3
	12	1	94	1

Это означает, что при построении дифференциальных и линейных характеристик с такими S-блоками в большинстве случаев будут использоваться переходы и не с максимально вероятными значениями (максимальных значений очень мало). Поэтому реальные значения дифференциальных и линейных характеристик будут меньшими по сравнению со случаем характеристик с максимально вероятными переходами.

Разберемся теперь со случайными подстановками при использовании их в полномасштабных шифрах.

В работе [14] показано, что случайными байтовыми S-блоками следует считать S-блоки, имеющие значения максимумов таблиц XOR разностей, равные 10 - 12, и значения максимумов смещений таблиц линейных аппроксимаций, близкие к 34.

Далее и будем ориентироваться на S-блоки с такими показателями. Главной особенностью таких S-блоков следует считать тот факт, что числа этих максимумов выражаются десятками, а то и единицами (их получается мало). Как мы убедимся в дальнейшем, отмеченная особенность приводи к тому, что при формировании переходов шифров с такими S-блоками к состоянию случайной подстановки в активных S-блоках используются далеко не максимально вероятные переходы. Это приводит к тому, что шифры с такими S-блоками практически приводятся к шифрам с эквивалентными значениями вероятности переходов XOR таблиц и смещений таблиц линейных аппроксимаций существенно меньшими, чем максимальные значения дифференциальных и линейных показателей применяемых S-блоков.

Оценка перспектив применения случайных S-блоков

Дело в том, что цикловые преобразования шифров содержат операцию введения подключа, а это значит, что входы в S-блоки следующего цикла независимо от свойств линейного преобразования и свойств S-блоков предыдущего цикла следует считать случайными. Даже если в шифре используются одни и те же S-блоки, результат прохождения активных S-блоков будет определяться максимальными значениями строк таблицы линейных аппроксимаций (дифференциальных таблиц) случайно взятых входов активных S-блоков. Для S-блоков одного и того же типа задача приводится к оценке вероятностей переходов из набора его случайно взятых строк.

Нас интересуют значения максимумов и их числа при активизации 35 строк линейной таблицы случайной подстановки.

Вспомним для этого закон распределения переходов ЛАТ таблицы случайной байтовой подстановки [14]. Приведем соответствующий результат (см. табл. 5).

Здесь приведено распределение переходов для всей таблицы. В общее число переходов здесь входят и положительные и отрицательные смещения.

Таблица 5

Распределение переходов для LAT таблицы подстановки степени 2^8 (считаются вместе положительные и отрицательные смещения)

$\|2k\|$	Число ячеек	Вероятность
0	6466	0,09944
2	12538	0,192815
4	11424	0,1756848
6	9982	0,1504416
8	7872	0,1210626
10	5952	0,0915406
12	4228	0,0650312
14	2822	0,0433972
16	1768	0,0271986
18	1040	0,01600576
20	574	0,00884176
22	298	0,00458356
24	146	0,0022291
26	66	0,001016608
28	28	0,000434614
30	10	0,000174096
32	4	0,0000653134
34	2	0,0000305176

При проходе S-блока будет использоваться лишь одно из значений смещения – положительное или отрицательное. Если нас интересует строка таблицы, то распределение переходов отдельно взятой строки можно получить из половинных значений второй колонки этой таблицы делением результатов на число строк в таблице (256). В результате получим (см. табл. 6).

Таблица 6

Расчет числа переходов разного типа в 25 строках ЛАТ

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 24 случайно взятых строках таблицы ЛАТ
±32	4	0,0156	0,376 0,546 0,3276
±30	10	0,0392	0,9408 1,372 0,8232
±28	28	0,1098	2,63 3,843 2,3058
±26	66	0,2588	6,21 9,058 5,4348
±24	146	0,572	13,728 20,02 12,012
±22	298	1,1686	28,047 40,901 24,54
±20	574	2,25098	54,0235 78.7843 47,27
±18	1040	4,078	97,88 142.73 85,638

В таблице представлены результаты оценки числа переходов и их значений в 35 случайно взятых строках таблицы ЛАТ. Из представленных результатов следует, что для 35 активных S-блоков при выборе в них максимально вероятных переходов можно ожидать при случайных входах в S-блоки:

-один переход со значением 32;

-один переход со значением 30;

- четыре перехода со значением 28;
- девять переходов со значением 26;
- двадцать переходов со значением 24;

Всего 35 переходов (активных S-блоков). Самый первый (один) S-блок взят с максимально возможным значением перехода.

Полагая далее, что строки в S-блоке выбираются из всего множества 256 строк равновероятно, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем выполнить оценку вероятности прихода шифра к состоянию случайной подстановки.

Вычисления для значения $k = 35$ приводят к результату

$$2^{34}\times\left(\frac{34}{128}\right)^2\times\left(\frac{30}{128}\right)^2\times\left(\left(\frac{28}{128}\right)^2\right)^4\times\left(\left(\frac{26}{128}\right)^2\right)^9\times\left(\left(\frac{24}{128}\right)^2\right)^{20}=2^{-129}.$$

и, следовательно, 35 активных S-блоков позволяют осуществить переход шифра к случайной подстановке. Получается, что для шифра Калина со случайными S-блоками переход к случайной подстановке может быть осуществлен за четыре цикла.

Заметим, что эти же четыре цикла получаются и для S-блоков с показателем нелинейности 104 (24).

Для 21-го S-блока получаем:
- один переход со значением 32;
- один переход со значением 30;
- два перехода со значением 28;
- пять переходов со значением 26;
- двенадцать переходов со значением 24.

Для 21-го S-блока (с первым максимально вероятным) получаем:

$$2^{20}\times\left(\frac{34}{128}\right)^2\times\left(\frac{30}{128}\right)^2\times\left(\left(\frac{28}{128}\right)^2\right)^2\times\left(\left(\frac{26}{128}\right)^2\right)^5\times\left(\left(\frac{24}{128}\right)^2\right)^{12}=2^{-77},$$

и, следовательно, для шифра Rijndael случайные S-блоки не проходят.

Приведем здесь также соответсвующие результаты, определяющие перспективы использования случайных S-блоков при реализации высокой динамики дифференциальных показателей (см. табл. 7).

Таблица 7

Расчет числа переходов разного типа в 25 строках дифференциальной таблицы случайной подстановки

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 25 строках
12	1	0,003906	0,09765
10	10	0,039065	0,9766
8	104	0,40625	10,156
6	830	3,24218	81,0545

Из представленных результатов следует, что для 25 активных S-блоков при выборе максимально вероятных переходов можно ожидать при случайных входах в S-блоки:
- один переход со значением 10;
- десять перехода со значением 8;
- четырнадцать переходов со значением 6.

Всего 25 переходов (активных S-блоков). Самый первый (25-й S-блок) S-блок и здесь может быть взят с максимально возможным значением перехода. Вычисления в этом случае приводят к результатам:

$$\frac{10}{256}\times\left(\frac{8}{256}\right)^{10}\times\left(\frac{6}{256}\right)^{14}=2^{-130}.$$

Для 21-го S-блока получаем вероятность, равную 2^{-108}, и, следовательно, для шифра Rijndael случайные S-блоки не проходят, но они проходят для шифра Калины.

Случайные S-блоки могут конкурировать с любыми другими S-блоками для шифров, у которых минимальное число активных S-блоков для прихода шифров к состоянию случайной подстановки по дифференциальным показателям больше 25, а по линейным показателям больше 35.

В последнее время появилась информация о разработке российскими учеными нового шифра **"Кузнечик",** который предлагается вместо российского стандарта ГОСТ [15]. Судя по представленной информации, этот шифр стал продолжением серии Rijndael-подобных шифров, появившихся в последнее время, таких как Калина, ADE, Anubis, GrangCru и ряда других.

Основное отличие шифра Кузнечик от шифра Rijndael состоит в том, что вместо операции MixColumns, примененной в шифре Rijndael к четверкам S-блоков (с использованием матрицы МДР кода (8,4,5)), в шифре Кузнечик применяется линейное преобразование с использованием рекурсивного МДР кода (32,16,17), т.е. выполняется операция MixColumns сразу над всем входным текстом (коэффициент ветвления равен 17). Естественно, что в этом случае преобразование ShiftRows оказывается лишним. В результате в этом 128-битном шифре при активизации на первом цикле одного S-блока линейное преобразование делает активными все 16 байтов выхода первого цикла, так что на двух циклах становятся активными 17 S-блоков (активизируется сразу все 16 S-блоков второго цикла). Третий цикл добавляет еще 16 активных S-блоков. На трех циклах имеем 33-и активных S-блока, но этого мало, так что шифр Кузнечик приходит к состоянию случайной подстановки на четвертом цикле независимо от дифференциальных и линейных показателей используемых в нем S-блоков. Общий итог – шифр Кузнечик (со случайными S-блоками) повторяет криптографические показатели стойкости (к атакам дифференциального и линейного криптоанализа) и динамические показатели прихода шифра к случайной подстановке, реализованные в отмеченных выше шифрах. Можно сделать общее заключение, что все Rijndael-подобные шифры (и шифр Калина с S-блоками с показателем нелинейности 104) по линейным показателям реализуют минимальное значение числа циклов прихода к случайной подстановке (по линейным показателям) равное 4 и никакие ухищрения с S-блоками не позволят уменьшить это число – оно является характеристикой циклового преобразования, реализованного в этой серии шифров.

Все эти шифры используют одну и ту же конструкцию циклового преобразования и поэтому имеют одни и те же криптографические свойства.

По сравнению с линейкой Rijndael-подобных шифров, например, белорусский шифр является более продвинутой конструкцией, так как цикловое преобразование белорусского шифра содержит 28 S-блоков и обеспечивает приход к состоянию случайной подстановки за два цикла, что на один цикл быстрее, чем у отмеченных выше шифров.

В табл. 8 приведены обобщенные результаты по оценке минимального число циклов для выхода шифров к стационарному состоянию случайной подстановки по линейным показателям.

Сравнение результатов, приведенных в этой таблице с результатами, приведенными в работе [12] иллюстрирует, что по линейным показателям число циклов необходимых для прихода шифра к случайной подстановке получается на один цикл большим, чем для прихода шифра к состоянию случайной подстановки по дифференциальным показателям.

По линейным показателям прихода к состоянию случайной подстановки белорусский шифр оказывается лидером среди остальных конструкций.

Таблица 8

Минимальное число циклов для выхода шифра
по линейным показателям
к стационарному состоянию случайной подстановки

Шифр	$r_{\min}$
Rijndael-128	4
Калина-128	4-5
FOX-64	3-4
FOX-128	4
ГОСТ 28147-89	9
Хейс-16	4
Мухомор-128	4
Белорусский шифр	2
Serpent	5
Лабиринт	≥ 3
Шифр с цикловой функцией М-64	2
Шифр с цикловой функцией М-128	2

Заключение

Показано, что для Rijndael-подобных шифров, к которым относится сам шифр Rijndael, а также шифры Калина, Anubis, ADE. GrandCru и некоторых других, конструкция циклового преобразования для любых S-блоков не позволяет реализовать переход к случайной подстановке по линейным показателям менее чем за четыре цикла.

Представленные результаты свидетельствуют о том, что вывод, сделанный в работе [16] о том, что задача поиска S-блоков с улучшенными криптографическими показателями потеряла перспективу, оказывается не совсем верным.

Имеются шифры, у которых цикловые преобразования построены так, что линейные и дифференциальные показатели входящих в них S-блоков влияют (в пределах одного-двух циклов) на динамические показатели прихода шифров к состоянию случайной подстановки. Это шифры с относительно малым числом активизируемых S-блоков на первых циклах (например, Rijndael). В таких шифрах необходимое число активных S-блоков находится на границе обеспечения числа цикловых преобразований, обозначающих минимум, необходимый для прихода шифра к состоянию случайной подстановки. И поэтому изменение дифференциальных или линейных показателей S-блоков может влиять на минимально необходимое число цикловых преобразований для прихода шифра к случайной подстановке. А это означает, что случайные S-блоки могут оказаться не совсем оптимальными для применения в таких шифрах (проигрывающие один цикл другим отмеченным конструкциям). В этих случаях можно ставить и решать задачи оптимизации S-блоков по линейным и дифференциальным показателям. Но это скорее локальные задачи, которые уже практически решены, и поэтому не имеющие перспективных продолжений.

Список литературы: 1. *Kazymyrov, O.A.* Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent / V. Kazymyrova, O. Kazymyrov, R. Oliynykov // Second workshop on Current Trends in Cryptology (CTCrypt 2013), Ekaterenburg, Russian, June 23-24, 2013. – Ekaterenburg, 2013. – P. 107-115. 2. *Казимиров, А.В.* Метод построения нелинейных узлов замены на основе градиентного спуска / А.В. Казимиров, Р.В. Олейников // Радиотехника. – 2013. – Вып. 172. – С. 104-108. 3. *Широков, А. В.* Методы формирования S-блоковых конструкций случайного типа с улучшенными криптографическими показателями (для блочных симметричных шифров с доказуемой безопасностью) : дис. … канд. техн. наук: 05.13.21 / Широков Алексей Викторович. – Харьков, 2010. – 265 с. 4. *J. Seberry, X. S. Zhang and Y. Zheng*. Relationships among nonlinearity criteria. Presented at EUROCRYPT-94, 1994. 5. *W.*

Saier, O. Staffelbach. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Cosputer Science, Springer-Verlag, pp.549-562, 1990. 6. *M.D. Yücel*. IAM501-Introduction to Cryptography. Institute of Applied Mathematics METU, Ankara, Turkey (9700501), 2002, p. 1-28. 7. *M. Matsui*. On a Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. IEICE Trans/ FundaMENTALS, vol. E82-A, NO. 1 January 1999, pp. 117-122. 8. *Matsui, M.:* Linear cryptanalysis method for DES cipher. In Advances in Cryptology.- EUROCRYPT'93 (1994) vol. 765. Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 386-397. 9. *Lisitskiy, K.E*. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers / K.E. Lisitskiy // I.J. Computer Network and Information Security, 2014, 1, 11-18 Published Online November 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.01.02. 10. *Лисицкая, И.В.* Сравнение по эффективности суперблоков некоторых современных шифров // Радіоелектроніка. Інформатика. Управління. Запоріжжя 1(26)'. – 2012. – С. 37- 43. 11. *Лисицкая, И.В.* О новой методике оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа // Системы обработки информации / Харьковский университет Противоздушных Сил имени Ивана Кожедуба. – 2011. – Вып. 4(94). – С. 167-173. 12. *Gorbenko I.D.* On Ciphers Coming to a Stationary State of Random Substitution / I.D. Gorbenko, K.E. Lisitskiy, D.S. Denisov // Copyright © 2013 Horizon Research Publishing. 13. *Горбенко, И.Д.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація. / І.Д. Горбенко, В.І. Долгов, Р.В. Олейніков и др. // Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195-208. 14. *Долгов, В.И.* Блочные симметричные шифры. Методология оценки стойкости к атакам дифференциального и линейного криптоанализа / В.И. Долгов, И.В. Лисицкая. – Харьков : Форт, 2013. – 420 с. 15. *Шишкин, В.* Принципы синтеза перспективного алгоритма симметричного шифрования с длиной блока 128 бит. / В. Шишкин // Рус Крипто'2013. 28 марта 2013 г. 16. *Lisitskaya, I.V., Melnychuk, E.D., Lisitskiy, K.E.* Importance of S-Blocks in Modern Block Ciphers I.J. Computer Network and Information Security, 2012, 10, 1-12 ISSN: 2074-9104 .

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.12.2013