УДК 621. 391:519.2:519.7

ОБ УЧАСТИИ S-БЛОКОВ В ФОРМИРОВАНИИ МАКСИМАЛЬНЫХ ЗНАЧЕНИЙ ДИФФЕРЕНЦИАЛЬНЫХ ВЕРОЯТНОСТЕЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

И.В. Лисицкая, А.В. Казимиров

Приводятся аргументы по обоснованию новой точки зрения по вопросу оценки безопасности блочных шифров к атакам дифференциального и линейного криптоанализа, состоящей в том, что максимумы средних вероятностей дифференциалов и линейных корпусов не зависят от свойств S-блоков, используемых в шифрах. Они определяются средними значениями максимумов полных дифференциалов, характерными для случайных подстановок соответствующей степени, т.е. могут быть рассчитаны по формулам.

Наводяться аргументи щодо обґрунтування нової точки зору з питання оцінки безпеки блокових шифрів до атак диференціального й лінійного криптоаналізу, яка полягає у тому, що максимуми середніх ймовірностей диференціалів і лінійних корпусів не залежать від властивостей S-блоків, використаних в шифрах. Вони визначаються середніми значеннями максимумів повних диференціалів, характерними для випадкових підстановок відповідного степеня, тобто можуть бути розраховані за формулами.

Arguments for the justification of a new perspective on the safety assessment of block ciphers to differential attack and linear cryptanalysis, which consists in the fact that the maxima of the average probability of differentials and linear hulls do not depend on the properties of S-blocks used in the cipher. They are defined as the average value of the maximum total differentials characteristic of random permutations to the extent appropriate, i.e. can be calculated according to formulas.

ВВЕДЕНИЕ

Мы здесь приведем сначала в качестве введения краткий обзор публикаций последних лет, приведенный в работе [1].

Речь пойдет о публикациях, в которых обсуждаются подходы к построению (получению) оценок доказуемой безопасности блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа. Представляется небольшая выборка из большого числа публикаций на эту тему.

В [2] Keliher и др. представили новый метод определения верхней границы максимума средней вероятности линейного корпуса (*MALHP*) для SPN шифров – значения, которое позволяет, как считают они, обосновать утверждение о доказуемой безопасности к атакам линейного криптоанализа. Применение этого метода к Rijndael-ю (AES) с 7-ю и более циклами обеспечивает верхнюю границу $UB = 2^{-75}$ и соответствующую нижнюю границу сложности данных $\frac{32}{UB} = 2^{80}$ (для 96,7% отношения успеха). Полученные результаты связываются с дифференциальными и линейными свойствами входящих в шифр S-блоков.

В [3] на основе рассмотрения значений распределения линейных вероятностей для (уникального) S-блока Rijndael-я эта верхняя граница улучшается. Получена верхняя граница для *MALHP*. Для Rijndael-я с 9 циклами приводится значение 2^{-92}, соответствующее нижней границе сложности данных 2^{97} (снова для 96,7% отношения успеха). После про-

ведения 43% вычислений, авторы полагают, что полученное значение уже стабилизировалось.

В [4] изучается подстановочно-перестановочная схема (SPN), на которой строится AES. Вводится AES* – SPN шифр, идентичный AES за исключением того, что фиксированные S-блоки заменены случайными и независимыми перестановками. Доказывается, что эта конструкция сопротивляется линейному и дифференциальному криптоанализу начиная с 4-х внутренних циклов, несмотря на огромный совокупный эффект многопутевых характеристик, которые порождены симметрией AES. Показывается, что дифференциальная и линейная вероятности (*DP* и *LP* условия) обе стремятся к значению $1/(2^{128}-1)$ очень быстро с ростом числа циклов. Подчеркивается, что результат подтверждает предположение других исследователей Keliher-a, Meijer-a, и Tavares-a.

В [5] определены аналитические верхние оценки средних вероятностей дифференциальных и линейных характеристик блочных шифров, построенных по схеме шифра ″Калина-128″, представленного на украинский конкурс по отбору кандидата на национальный стандарт блочного симметричного шифрования. В частности, в работе приводятся такие оценки для отмеченных показателей: $EDP \le 2^{-130}$, $ELP \le 2^{-130}$. Авторы относят эти оценки к показателям практической стойкости шифра.

В [6] расширяется теорема Хонга и др., которая дает верхние границы для максимумов средних вероятностей дифференциалов и линейных корпусов (*MADP* и *MALHP*) SPN блоковых шифров с оптимальными или квазиоптимальными диффузионными слоями для случая вложенных SPN (NSPN) структур. Применение расширенной теоремы для двух NSPN шифров Hierocrypt-3 со 128-битными блоками и Hierocrypt-L1 с 64-битными блоками позволило авторам получить оценки для *MADP* и *MALHP* для 2-х циклового Hierocrypt-3, приводящие к границе 2^{-96}, и для Hierocrypt-L1 с двумя циклами к границе 2^{-48}. Расширенная теорема была применена также для AES и позволила установить, что *MADP* и *MALHP* для 4-х цикловой уменьшенной модели ограничены значением 2^{-96}. Этот результат, отмечают авторы, превосходит лучший предыдущий результат 2^{-92} для 10-ти циклов Keliher-a и др. Результат опять связывается с дифференциальными и линейными свойствами входящих в шифр S-блоков и числом ветвлений.

Можно привести примеры многих других работ, в том числе и известных криптографов К. Нюберг, М. Мацуи и др., посвященных оценке показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа. Все эти работы придерживаются концепции, в соответствии с которой показатели доказуемой стойкости БСШ к атакам дифференциального и линейного криптоанализа непосредственно связаны с дифференциальными и линейными показателями входящих в шифры S-блоковых конструкций.

В этой работе мы хотим привести дополнительные аргументы по обоснованию новой точки зрения для оценки безопасности блочных шифров к отмеченным атакам, пропагандируемой в работе [1], концептуально отличающейся от известных, хотя в конечном итоге речь опять будет идти об определении максимальных значений полных дифференциалов и линейных корпусов (оболочек) БСШ.

Эта точка зрения сложилась на основе развития нового подхода в теории и методах криптоанализа, родившегося на кафедре БИТ ХНУРЭ [7]. Он ориентирован, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – уточнённой в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, новой идеологии определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [1]. Эта новая идеология основывается на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров (DES, ГОСТ, Rijndael, Лабиринт, Мухомор, Калина, ADE, Камелия, FOX и многих других) положении (факте), состоящим в том, что все эти шифры (и большие и малые их версии) через определенное число циклов (для рассмотренных уменьшенных моделей от трех

циклов до семи) независимо от используемых в шифрах S-блоков приобретают свойства случайной подстановки (по комбинаторным показателям (числу инверсий, возрастаний и циклов), а также по законам распределения переходов XOR таблиц дифференциальных разностей (полных дифференциалов) и законам распределения смещений таблиц линейных аппроксимаций (линейных корпусов) они повторяют соответствующие показатели случайной подстановки [8,9,10]). Здесь и далее под случайной подстановкой понимается подстановка, удовлетворяющая установленным критериям близости законов распределения циклов, возрастания и инверсий, а также законов распределения переходов их XOR таблиц и смещений таблиц линейных аппроксимаций соответствующим теоретическим (асимптотическим) законам распределения вероятностей [11].

Мы здесь сразу заметим для того, чтобы не возникали вопросы об адекватности малых моделей большим шифрам, что свойство перехода дифференциальных и линейных показателей шифров после определенного числа циклов зашифрования (для Rijndael-я после четырех) к некоторому установившемуся значению (правда, для S-блоков с предельными (минимально возможными) дифференциальными и линейными показателями) отмечается в ряде публикаций и для больших шифров (например, в [12] для шифра Rijndael).

А это значит, что концепция, разрабатываемая в представленных выше и многих других работах, является не верной**.** На самом деле результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются практически только размером битового входа в шифр и от свойств S-блоков не зависят. Свойства S-блоков сказываются (и то не в существенной степени и не во всех случаях) только на динамике перехода к показателям случайной подстановки. Это факт зафиксирован в работе [1] в виде утверждения.

Утверждение. *Для каждого блочного симметричного шифра* (*из числа известных итеративных БСШ*) *существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Конечно, аккуратнее было бы говорить только об уже проверенных шифрах, но на взгляд авторов работы [1], это свойство должно быть присуще любому сколько-нибудь внушающему доверие шифру.

Дальнейший материал работы будет посвящен изложению более основательных свидетельств справедливости указанного положения.

1. ПОНЯТИЙНЫЙ АППАРАТ ТЕОРИИ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Мы изложим сначала более детально понятийный аппарат и позицию авторов последней из отмеченных выше работ [6].

В работе [6] рассматриваются вложенные SPN структуры, обобщающие метод широкого следа, использованный в шифре Rijndael, для построения доказуемо безопасной цикловой функции. Внимание авторов сосредотачивается, как было уже отмечено выше, на получении оценок для верхних границ максимумов средних вероятностей дифференциалов и линейных корпусов *MADP* и *MALHP* SPN блоковых шифров с оптимальными или квазиоптимальными диффузионными слоями.

В основе рассматриваемых SPN структур лежит конструкция, названная авторами *SDS* функцией. Она представлена на рис.1.

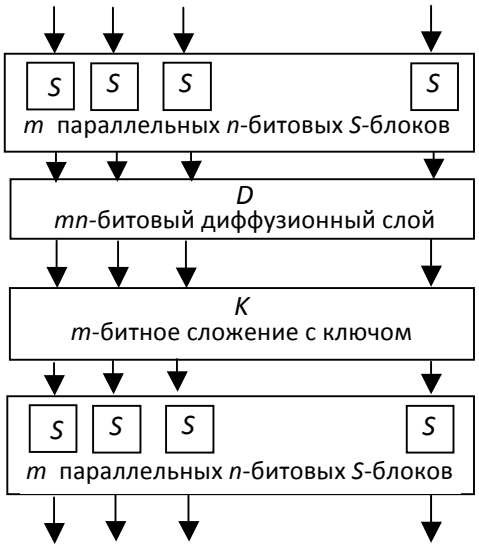

Рис.1 *SDS* функция

В этой конструкции все S-блоки считаются одинаковыми, и их фундаментальные дифференциальные и линейные вероятности p и q (максимальные значения переходов таблиц XOR разностей и смещений таблиц линейных аппроксимаций) соответственно равны

$$p = DP^s_{\max}, \quad q = DL^s_{\max}.$$

Для описания дифференциальных и линейных свойств этого преобразования используется понятие числа ветвлений, с помощью которого определяется эффективность

распространения активизации (лавинного изменения битовых значений) в процессе прохождения диффузионного слоя D. Само линейное преобразование при этом задается с помощью умножения входного блока данных на $mn \times mn$ матрицу линейного преобразования D с элементами из поля $GF(2)$.

Определение 1 (Число ветвлений). *Дифференциальное число ветвлений* $\mathcal{B}_{\mathrm{D}}(D)$ *для диффузионного слоя D определяется так:*

$$\mathcal{B}_{\mathrm{D}}(D) = \min_{\Delta x \neq 0}(Hw(\Delta x) + Hw(D\Delta x)),$$

где Δx *– входная разность.*

Отметим, что понятие Хеммингова веса $Hw(x)$ здесь применяется не для числа ненулевых битов, а сразу для числа m ненулевых n-битных ″характеров″ (m-сегментов из n-битных слов) mn -битного входного блока данных.

Аналогично определяется линейное число ветвлений $\mathcal{B}_{\mathrm{L}}(D)$ для диффузионного слоя D как

$$\mathcal{B}_{\mathrm{L}}(D) = \min_{Гу \neq 0}(Hw(D^* Гу) + Hw(Гу)),$$

где $Гу$ *– выходное масковое значение, а* D^* *есть транспонированная матрица D.*

Практически значения $\mathcal{B}_{\mathrm{D}}(D)$ и $\mathcal{B}_{\mathrm{L}}(D)$ являются нижней границей для числа активных S-блоков для двух смежных циклов дифференциальной и линейной характеристики соответственно.

Нам потребуется еще ряд понятий и определений из работы [6]. Мы их дадим сразу не для отдельного S-блока, а для всего шифрующего преобразования (ключезависимой функции $f = f[k](x)$).

Определение 2 (Дифференциальная и Линейная вероятности): *Дифференциальная вероятность DP^f и линейная вероятность LP^f соответственно для ключезависимой функции f с n-битным входом x и n-битным выходом y ($x, y \in GF(2^n)$) есть*

$$DP^f(\Delta x \to \Delta y) =$$

$$= \frac{\#\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n},$$

$$LP^f(\Gamma y \to \Gamma x) =$$

$$= \left(\frac{\#\{x \in GF(2)^n \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^{n-1}} - 1 \right)^2$$

где Δx и Δy являются входным и выходным различиями (разностями), а Γx и Γy входной и выходной масками; $x \Gamma x$ обозначает результат скалярного произведения x и Γx.

Определение 3 ($DP^f_{\max}$ и $DL^f_{\max}$): *Максимальное значение дифференциальной и линейной вероятности для ключезависимой функции f определяется соответственно как*

$$DP^f_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^f(\Delta x \to \Delta y),$$

$$DL^f_{\max} = \max_{\Gamma x, \Gamma y \neq 0} DL^f(\Gamma x \to \Gamma y).$$

Приведем еще четыре необходимых нам определения из работы [6] для средних вероятностей *ADP*, *ALHP*, *MADP* и *MALHP* ключезависимой функции $f = f[k](x)$, где k и x являются ключом и входом в ключезависимую функцию (шифр) соответственно.

Определение 4 (*ADP*): *Средняя дифференциальная вероятность* (*ADP*) *функции* $f[k](x)$ *есть*

$$ADP^f = \underset{k}{ave}\, DP^{f[k]}(\Delta x \to \Delta y).$$

Определение 5 (*ALHP*): *Средняя вероятность линейного корпуса* (*ALHP*) *функции* $f[k](x)$ *есть*

$$ALHP^f = \underset{k}{ave}\, LP^{f[k]}(\Gamma x \to \Gamma y).$$

Определение 6 (*MADP* и *MALHP*): *Максимум средней дифференциальной вероятности* (*MADP*) *и максимум средней вероятности линейного корпуса* (*MALHP*) *функции* $f[k](x)$ *есть*

$$MADP^f = \max_{\Delta x \neq 0, \Delta y} ADP^f(\Delta x \to \Delta y).$$

$$MALHP^f = \max_{\Gamma y \neq 0, \Gamma x} ALHP^f(\Gamma x \to \Gamma y).$$

Нас в дальнейшем и будут интересовать значения *MADP* и *MALHP* для случаев, когда в качестве функции f выступают цикловые преобразования и последовательности цикловых преобразований итеративных шифров (ключезависимые функции).

Остается теперь изложить теорему Хонга, доказательство которой приведено в [6], которая достаточно полно отражает сущность концепции, о которой идет речь.

Теорема 1. *Если диффузионный слой D есть $m \times m$ матрица, чьи элементы принадлежат полю $GF(2^n)$ и если D есть MDS функция для n-битного слова с числами ветвлений $\mathcal{B}_D = \mathcal{B}_L = M + 1$, то*

$$MADP^{SDS} \leq p^m, \quad MALHP^{SDS} \leq q^m.$$

Для шифра Rijndael (128-битной версии), рассматриваемого как вложенная SPN структура с числами ветвлений нижнего и верхнего уровня равными соответственно $h = m = 4$, для $p = q = 2^{-6}$ авторы рассматриваемой работы предлагают считающейся доказанной оценку:

$$MADP^{\mathrm{NSDS}} \le \left(2^{-6}\right)^{4\times 4} = 2^{-96},$$

$$MALHP^{\mathrm{NSDS}} \le \left(2^{-6}\right)^{4\times 4} = 2^{-96}.$$

2. РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНЫХ ЭКСПЕРИМЕНТОВ

В этой работе мы хотим продемонстрировать результаты оценки влияния на дифференциальные показатели современных шифров (их малых версий) максимальных значений дифференциалов используемых S-блоков (параметра p, фигурирующего в приведенных выше формулах).

Прежде всего, заметим, что проверить экспериментально предлагаемые многими авторами оценки для современных шифров с битовой длиной входного блока $n \ge 128$ вычислительно невозможно. Но это становится возможным, если перейти к шифрам с меньшей битовой длиной входного блока. Именно стремлению обойти вычислительные трудности, связанные с большими шифрами, в качестве альтернативы на кафедре БИТ ХНУРЭ и развивается, как уже было отмечено во введении, подход к криптоанализу основанный на использовании при оценке показателей стойкости больших шифров уменьшенных их моделей. Как показали наши исследования, многие современные шифры допускают масштабирование [13-16 и др.]. В частности это легко удается сделать для шифра Rijndael. Кстати, в интернете можно найти варианты уменьшенных моделей этого шифра [17,18], предлагаемые авторами для учебных целей. Так вот мы уменьшенные модели шифров используем в первую очередь не для учебных целей, а для выполнения исследований показателей стойкости их больших прототипов.

В данном случае предлагаются результаты исследований дифференциальных свойств 16-битных моделей шифров Rijndael-я с различными типами линейных преобразований и простейшего шифра SPN структуры, предложенного еще X. Фейстелем [19]. Для таких размеров входных блоков данных вычислительных ресурсов вполне достаточно, чтобы построить целиком таблицу XOR переходов (полных дифференциалов) сразу для всего шифра.

В таблице 1 представлены зависимости средних значений максимумов полного дифференциала $MADP$ для S-блоков с различными значениями $DP^{s}_{\max} = p$, и различного количества циклов r алгоритма Baby-Rijndael с операцией MixColumns на весь текст: для 16-ти битного вектора B, представляющего собой набор из четырех полубайтовых значений выходов четырех S-блоков $B = (b_0, b_1, b_2, b_3)$, результатом линейного преобразования является 16-ти битный вектор $C = (c_0, c_1, c_2, c_3)$, определяемый с помощью матричного умножения:

$$(c_0, c_1, c_2, c_3) = (b_0, b_1, b_2, b_3) * \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix},$$

где операция матричного умножения выполняется в поле $GF(2^4)$ (элементы матрицы – это элементы поля $GF(2^4)$). В этом случае дополнительного преобразования (перестановки) CtiftRows не требуется.

В экспериментах для каждого шифра рассматривалась выборка из 30 различных ключей зашифрования. Сами варианты использованных S-блоков иллюстрирует таблица 2 (они взяты из работы [20]).

Таблица 1

Значения полного дифференциала для различных S-блоков и количества циклов алгоритма Rijndael с операцией MixColumns на весь текст.

Sbox / *r*	Sbox, Сл *p*4F2	Sbox. *p*4 Лабир.	Sbox AES *p*4	Sbox *p*6F0	Sbox *p*6 F2	Sbox DES *p*8	Sbox *p*8 F0	Sbox *p*12 F0
1	16384,00	16384,00	16384,00	24576,00	24576,00	32768,00	32768,00	49152,00
2	83,87	132,00	132,00	490,87	230,40	1152,00	1536,00	5184,00
3	20,73	**19,47**	**18,80**	25,53	35,27	70,87	139,13	146,13
4	**19,60**	18,73	19,00	**19,20**	**18,93**	**19,27**	**23,93**	**19,07**
5	19,13	19,47	19,47	18,93	19,40	19,00	23,87	19,00

Как следует из представленных результатов во всех случаях, кроме S-блока Sbox *p*8 F0 (7-я колонка таблицы) независимо от максимального значения таблицы дифференциальных разностей *p* S-блоков все шифры приходят к одному и тому же среднему значению максимума полного дифференциала, характерному для случайной подстановки соответствующей степени [9,10].

Таблица 2

Варианты использованных S-блоков с расшифровкой их описаний

Варианты использованных S-блоков	Расшифровка описания S-блоков
SboxAES *p*4 ={A,4,3,B,8,E,2,C,5,7,6,F,0,1,9,D}; SboxDES *p*8 ={E,4,D,1,2,F,B,8,3,A,6,C,5,9,0,7} (первая строка S-блока S_1 шифра DES); Sbox *p*6 F2 = {B,C,5,0,1,3,2,7,8,4,D,F,6,9,E,A}; Sbox *p*6 F0 = {4,6,F,B,E,7,5,D,9,C,1,0,3,8,A,2}; Sbox *p*12 F0 = {8,3,1,9,A,B,E,C,5,D,F,2,0,4,7,6}; Sbox *p*8 F0 = {C,9,4,6,8,E,D,5,3,F,B,0,A,2,1,7}; Sbox, Сл. *p*4F2 = {D,E,B,5,4,2,1,F,0,9,6,A,7,C,8,3}; Sbox. *p*4 Лабир.= {B,8,6,4,A,0,D,2,C,5,1,E,3,F,9,7}.	*p*X – X максимальное значение в дифференциальной таблице S-блока; FY – Y количество фиксированных точек ($S(x) = x$). Отсутствие FY в описании S-блока эквивалентно F0.

Можно также отметить, что S-блок из 7-ой колонки таблицы 1 тоже приходит к асимптотическому значению на четвертом цикле, только оно оказывается несколько больше асимптотического значения для случайной подстановки (≈24). ″Хорошие″ S-блоки с минимальным значением максимума $DP^S_{\max}$ равным 4-ём имеют преимущество перед остальными S-блоками всего лишь на один цикл. Поэтому связь дифференциальных показателей S-блоков $DP^S_{\max}$ с показателями стойкости к дифференциальному (и линейному) криптоанализу всего шифра $MADP$ ($MALHP$), которую считают, что нашли авторы цитируемых работ, становится далеко не очевидной. Мы здесь приводим данные по исследованию дифференциальных свойств уменьшенных моделей, но у нас уже есть данные, что аналогичная ситуация происходит и с линейными показателями.

В таблице 3 приведены результаты экспериментов по определению дифференциальных показателей 16-ти битного SPN шифра (шифра с 16-ти битным входом) из работы проф. Хейса [21], построенного по идеям Х. Фейстеля. Каждая колонка таблицы соответствует использованию S-блоков (одинаковых) со своими значениями параметра *p*.

Результаты и этого эксперимента свидетельствуют, что все варианты шифра (отличающиеся S-блоками) приходят через определенное число циклов опять к установившемуся значению, характерному для случайной подстановки, правда, Sbox *p*8 F0 снова

″пошел своей дорогой″. Причину такого поведения шифров с S-блоком Sbox *p*8 F0 предстоит еще выяснить.

Таблица 3

Значения полного дифференциала для различных S-блоков и количества циклов алгоритма Хейса

Sbox / *r*	Sbox, Сл ***p*4** F2	Sbox. ***p*4** Лабир.	Sbox AES ***p*4**	Sbox, Сл ***p*6** F0	Sbox ***p*6** F2	Sbox DES ***p*8**	Sbox ***p*8**F0	Sbox ***p*12**F0
1	16384,00	16384,00	16384,00	24576,00	24576,00	32768,00	32768,00	49152,00
2	4096,00	4096,00	4096,00	6144,00	6144,00	12288,00	8192,00	15552,00
3	443,87	1616,00	2036,27	1920,00	2802,40	2303,33	3432,00	1587,20
4	54,60	362,87	596,00	601,20	649,33	222,27	1184,47	613,13
5	25,07	88,47	190,33	148,93	292,93	64,13	457,07	265,73
6	**19,00**	24,93	77,47	50,00	71,47	24,80	178,40	104,87
7	19,33	**19,53**	35,87	22,00	32,00	**18,80**	87,33	46,87
8	19,20	18,93	21,07	**19,07**	19,67	18,80	39,93	23,87
9	18,97	19,27	**19,27**	18,87	**18,93**	19,00	**24,60**	**19,13**
10	19,45	19,02	19,33	19,27	19,33	18,93	24,27	19,00

Далее мы приводим результаты экспериментов применения при построении версий шифра Baby-Rijndael других вариантов линейных преобразований. Так, в таблице 4 представлены поцикловые значения полных дифференциалов для SPN шифров с линейным преобразованием MixColumn и ShiftRow GF(2^4): для 16-ти битного вектора B, представляющего набор из четырех полубайтовых значений выходов четырех S-блоков $B = (b_0, b_1, b_2, b_3)$, результатом линейного преобразования является 16-ти битный вектор $C = (c_0, c_1, c_2, c_3)$, определяемый с помощью матричного умножения

$$\begin{pmatrix} c_0 & c_2 \\ c_1 & c_3 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} * \begin{pmatrix} b_0 & b_2 \\ b_1 & b_3 \end{pmatrix} \text{ GF}(2^4),$$

где операция матричного умножения выполняется в поле GF(2^4). В этом случае для дополнительного перемешивания результатов матричного произведения используется операция ShiftRow.

Применение менее эффективного линейного преобразования не изменяет картину. Опять через определенное число циклов (четыре или пять) независимо от варианта используемых подстановок наблюдается выход к установившемуся (асимптотическому) значению (Sbox *p*8F0 снова дает индивидуальный результат, повторяющий по характеру предыдущий).

Таблица 4

SPN шифр с линейным преобразованием MixColumn и ShiftRow GF(2^4)

Sbox / *r*	Sbox AES ***p*4**	Sbox. ***p*4** Лабир.	Sbox, Сл ***p*4** F2	Sbox, Сл ***p*6** F0	Sbox DES ***p*8**	Sbox ***p*8**F0	Sbox, Сл ***p*12** F0
1	16384,00	16384,00	16384,00	24576,00	32768,00	32768,00	49152,00
2	2952,53	3515,73	3072,00	4625,07	4744,53	8192,00	10240,00
3	282,67	318,93	373,33	612,27	748,80	1382, 40	768,00
4	**19,33**	**19.27**	**19,20**	22,60	26,87	53,87	41,67
5	19,33	19,07	19,27	**18,73**	**19,00**	**24,13**	**18,80**
6	19,00	19,40	19,00	19,00	19,00	23,80	19.27

В последнем из экспериментов мы взяли уменьшенную модель шифра Rijndael с линейным преобразованием MixColumn и ShiftRow GF(2^8): для 16-ти битного вектора B', представляющего набор из двух байтовых значений выходов четырех S-блоков

$B' = (b'_0, b'_1)$ ($b'_0 = (b_0, b_1)$, $b'_1 = (b_3, b_4)$) результатом линейного преобразования является 16-ти битный вектор $C' = (c'_0, c'_1) = (c_0, c_1, c_2, c_3)$, определяемый с помощью матричного умножения:

$$\begin{pmatrix} c'_0 \\ c'_1 \end{pmatrix} = \begin{pmatrix} 01 & 03 \\ 03 & 01 \end{pmatrix} * \begin{pmatrix} b'_0 \\ b'_1 \end{pmatrix} \mathrm{GF}(2^8),$$

где операция матричного умножения выполняется в поле $\mathrm{GF}(2^8)$ (элементы матрицы – это элементы поля $\mathrm{GF}(2^8)$). В этом случае для дополнительного перемешивания (перестановки) результатов матричного произведения используется также операция StiftRows (в данном случае байты c_0 и c_1 просто меняются местами). Таблица 5 иллюстрирует результаты этого эксперимента.

Таблица 5

Значения полного дифференциала для SPN шифра с линейным преобразованием MixColumn и ShiftRow $\mathrm{GF}(2^8)$ с различными S-блоками.

Sbox / *r*	SboxAES ***p*4**	Sbox. ***p*4** Лабир.	Sbox, Сл. ***p*6**	Sbox, Сл. ***p*6**	Sbox DES, ***p*8**	Sbox ***p*8**F0	Sbox, Сл ***p*12** F0
1	16384,00	16384,00	24576,00	24576,00	32768,00	32768,00	49152,00
2	4983,47	1024,00	5102,93	4522,67	3635,20	6144,00	3072,00
3	647,47	32,73	530,13	833,07	542,93	301,47	166,73
4	42,40	**19,33**	34,00	66,53	22,13	25,00	**19,07**
5	20,67	18,67	**19,60**	40,93	**19,07**	**19,00**	18,87
6	**19,20**	19,00	19,33	**19,27**	19,27	19,27	19,00
7	19,13	18,00	19,20	19,20	19,00	19.13	19,13

Интересно отметить, что S-блок Sbox*p*8 F0 в этом случае тоже дал асимптотическое значение, соответствующее случайной подстановке.

Приведенные результаты свидетельствуют, что концепция оценки доказуемой стойкости, развиваемая в приведенных во введении и многих других работах, все же ошибочна! Может быть, это звучит и через чур резко, и получающиеся результаты иногда оказываются весьма близкими к действительным, но сама идея привязки показателей стойкости шифров к свойствам S-блоков оказывается явно не конструктивной.

Во всех рассмотренных примерах показатели стойкости шифров не зависят от подстановок, использованных при их построении, а зависят только от битового размера входа в шифр. Подстановки влияют лишь на динамику перехода к асимптотическому значению. Конечно же, этот результат, следующий из большого числа экспериментов со случайными подстановками и малыми моделями шифров, будет сохраняться и для больших версий шифров (и не только для шифров с SPN структурой!).

ЗАКЛЮЧЕНИЕ

Общий вывод работы состоит в том, что итоговые показатели стойкости шифров к атакам дифференциального и линейного криптоанализа определяются тем, что асимптотически шифры ведут себя как случайные подстановки (от свойств S-блоков, использованных при построении шифров, не зависят). А раз так, то интересующие нас показатели доказуемой стойкости (безопасности) шифров к атакам дифференциального и линейного криптоанализа могут быть определены расчетным путем из соответствующих формул для теоретических законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени [9,10].

Для этого достаточно воспользоваться упрощенными расчетными соотношениями, приведенными в работе [1]. Мы здесь напомним итоговые результаты для 128-битного шифра Rijndael.

Для среднего значения максимума дифференциальной вероятности ($MADP$) для 128-битного шифра получена оценка $MADP^R = \frac{128+3}{2^{128}} \approx 2^{-113}$ (аппроксимация точного выражения в виде $MADP = \frac{n+3}{2^n}$, предложенная в [10] на основе анализа результатов вычислений, выполненных для различных значений n).

Заметим, что оценка, полученная авторами работы [6] для шифра Rijndael $MADP^R \leq 2^{-96}$, отличается от нашей в 2^{17} раз. Она действительно может рассматриваться как грубая оценка сверху, но это скорее случайность (не лишенная, может быть, интуитивных предчувствий), чем строго доказанное правило. По методике [6] для шифров с подстановками, имеющими большие значения максимумов p и q, результаты должны заметно измениться в худшую сторону, чего на самом деле не происходит.

Среднее значение максимального смещения таблицы линейных аппроксимаций (линейных каркасов (оболочек, корпусов)) для шифров с n-битным значением размера входного блока данных аппроксимируется соотношением $\left(\frac{3}{2}\right)^n$. Для среднего значения максимума вероятности линейного корпуса ($MALHP$) 128-битного шифра приходим к результату $MALHP^R = \left(\frac{\left(\frac{3}{2}\right)^{128}}{2^{127}}\right)^2 = 2^{-104}$. Реальное значение может отличаться от приведенного, по нашим предположениям, менее чем в два раза.

Результаты работы позволяют также прийти к еще одному важному выводу. Одним из весомых аргументов для серьезных возражений использованию уменьшенных моделей в рамках развиваемого подхода в теории криптоанализа является вопрос адекватности моделей оригиналам, а также вопрос о правомерности переноса оценок показателей стойкости малых моделей на большие шифры.

В отношении адекватности моделей малых шифров. Мы представили здесь несколько моделей шифра baby-Rijndael, отличающиеся конструкциями основного (принципиального) преобразования шифра Rijndael – линейного преобразования. Была поставлена задача выбрать наиболее подходящую (более полно повторяющую свойства оригинальной версии) конструкцию модели. Результаты, однако, свидетельствуют о том, что различные в данном случае варианты реализации МДР преобразования приводят к шифрам с весьма близкими дифференциальными показателями. Мы полагаем, что эта инвариантность к точному повторению в модели отдельных операций прототипа будет сохраняться и по отношению к другим показателям.

Ну а в отношении сохранения в большом шифре свойств уменьшенной модели можно лишь отметить, что мы говорим о сохранении свойств и показателей случайной подстановки. При увеличении битового размера входа в шифр (с увеличением степени подстановки) ее соответствие асимптотическим законам распределения вероятностей (по инверсиям, возрастаниям и циклам), а также законам распределения вероятностей переходов таблиц полных дифференциалов и таблиц линейных корпусов будет только повышаться. Об этом свидетельствую и последние результаты исследования дифференциальных характеристик больших шифров, о которых будет идти речь в следующих наших публикациях.

Литература

1. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И.Д., Долгов В.И.,

Лисицкая И.В., Олейников Р.В.//Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320.
2. L. Keliher, H. Meier, and S. Tavares. New method for upper bounding the maximum average linear hull probability for SPNs, Advances in Cryptology – EUROCRYPT 2001, LNCS 2045, Springer-Verlag, pp. 420-436, 2001.
3. L. Keliher, H. Meijer, and S. Tavares, Improving the upper bound on the maximum average linear hull probability for Rijndael, Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112-128, Springer-Verlag, 2001.
4. Thomas Baignoires and Serge Vaudenay Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch. 2004. p. 16.
5. Алексийчук А.Н. Оценки практической стойкости блочного шифра ″Калина″ относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах / Алексийчук А.Н., Ковальчук Л.В., Скрыпник Е.В., Шевцов А.С. // Прикладная радиоэлектроника. – 2008. – Т.7. – №3. – С. 203-209.
6. F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis/ IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37-46.
7. Долгов В.И. Подход к криптоанализу современных шифров /Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй международной конференции ″Современные информационные системы. Проблемы и тенденции развития″, Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436.
8. Lysytska I.V. The selection criteria of random substitution tables for symmetric enciphering algorithms / Lysytska I.V., Koriak A.S., Golovashich S.A., Oleshko O.I., Oleinik R.V // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. – P. 204.
9. Олейников Р.В. Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333.
10. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340.
11. Долгов В.И. Случайные подстановки в криптографии / Долгов В.И., Лисицкая И.В., Лисицкий К.Е. // Радіоелектронні та комп'ютерні системи, 2010, № 5 (46), С. 79-84.
12. K. Ohkuma Security Assessment of Hierocrypt and Rijndael against the Differential and Linear Cryptanalysis/ K. Ohkuma, H. Shimizu, F. Sano, S. Kawamura//, In Proceedings of the 2nd NESSIE workshop (2001).
13. Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И. // Прикладная радиоэлектроника – 2009. – Т.8, № 3 – С. 252-257.
14. Долгов В.И. Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л. // Прикладная радиоэлектроника. – 2008. – Т.7 – № 3. С. 215-224.
15. Долгов В.И. Криптографические свойства уменьшенной версии шифра ″Калина″/ Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев А.В., Дробатько Е.В. // Прикладная радиоэлектроника , 2010. – Т.9. – № 3. – С. 349–354.
16. Долгов В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.// Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2009. – Т. 8 − № 3, С. 283-295.
17. A Description of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003.

18. Raphael Chung-Wei Phan, Mini Advanced Encryption Standard (Mini-AES): A Tested for Cryptanalysis Students, Cryptology, XXVI (4), 2002.
19. H. Feistel, Cryptography and computer privacy. Scientific American, 228(5): 15-23,1973.
20. Долгов В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / Долгов В.И., Кузнецов А.А., Лисицкая И.В., Сергиенко Р.В., Олешко О.И. // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2009. – Т. 8 − № 3, С. 268-277.
21. H. M. Heys. A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p 189-221.