УДК 621.3.06

ВАРИАЦИИ НА ТЕМУ ШИФРА RIJNDAEL

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, А.В. КАЗИМИРОВ

Рассматривается подход к анализу показателей криптографической стойкости блочных симметричных шифров, строящийся на основе исследования свойств уменьшенных версий этих шифров. С использованием этого подхода оцениваются показатели стойкости к атакам дифференциального криптоанализа нескольких модификаций SPN шифра с 16-битным входом, имеющего структуру общего типа, предложенную в работе Говарда Хейса. Показывается, что существуют решения, превосходящие по показателям стойкости шифр Rijndael.

Ключевые слова: симметричный блочный шифр, криптоанализ, Rijndael.

ВВЕДЕНИЕ

В нашей предыдущей работе [1] мы подняли вопрос о перспективности и новизне решений, использованных при построении шифра Rijndael. Было отмечено, что этот шифр практически повторяет не только общую структуру SPN шифра, рассмотренную в работе Х. Фейстеля 1973 года [2], но и практически по стойкости (при полном наборе цикловых преобразований) оказывается ничуть не лучше своего исторического прототипа. Он представляется выигрышным по сравнению с классической схемой (в 16-битной интерпретации работы [3]) только в динамике выхода на асимптотические показатели стойкости к атакам дифференциального (и линейного) криптоанализа (четыре цикла против семи). Этот выигрыш достигается за счет более эффективного линейного преобразования, примененного в цикловой функции, реализующего стратегию широкого следа (умножения на матрицу МДР кода и циклического сдвига векторов состояний).

В этой работе мы хотим привлечь внимание еще к одному аспекту оценки перспективности решений, заложенных в шифр Rijndael, а именно нас будет интересовать построение преобразования более эффективного, чем реализуется в стандарте 21-го века! Мы приведем примеры таких решений.

1. ОПИСАНИЕ ВАРИАНТОВ РЕАЛИЗАЦИЙ SPN ШИФРОВ

В основе всех последующих рассмотрений будет использована обобщенная структура 16-битного SPN шифра Фейстеля в интерпретации работы [2]. Она приведена на рис. 1. Модификации этой SPN структуры будут состоять в использовании различных вариантов начального и конечного (IT и FT) преобразований.

В частности будут рассмотрены начальные и конечные преобразования двух типов. Первое будет повторять уменьшенные версии начального и конечного преобразований шифра Лабиринт [4]. Мы здесь кратко напомним сущность этих преобразований, описанных в нашей работе [5].

Начальное IT преобразование уменьшенной версии шифра «Лабиринт» (рис. 2) включает сложение по модулю 2^{16} входного 16-битного блока данных с 16-битным подключом. На следующем шаге 16-ть результирующих бит разбиваются на блоки по 4-е бита, которые подаются на нелинейные преобразования, осуществляемые S-блоками. Далее 4-х битные выходы S-блоков объединяются в новые 16-ть бит и опять разбиваются на два полублока, над которыми выполняются циклические сдвиги:левый полублок сдвигается на 4 бита влево, а правый соответственно на четыре бита вправо, и в заключение над полученным 16-битным блоком выполняется операция инволютивного линейного смешивания IMix на 2 бита. Результат предыдущего действия XOR-ится с левыми и правыми 8-ю битами входного слова.

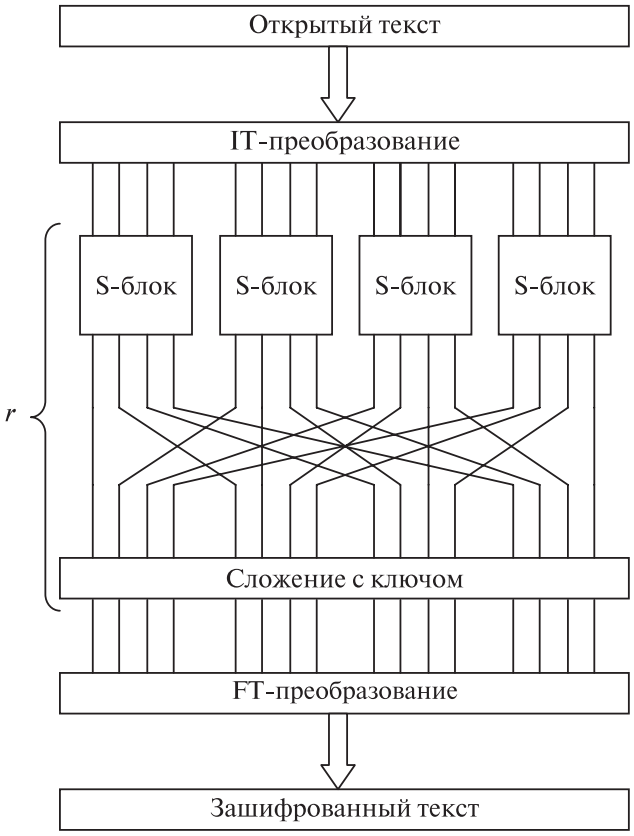

Рис. 1. Общий вид алгоритма Хейса.
На этом рисунке IT – начальное преобразование;
FT – конечное преобразование;
S-блок – подстановка полубайт в полубайт;
r – количество циклов

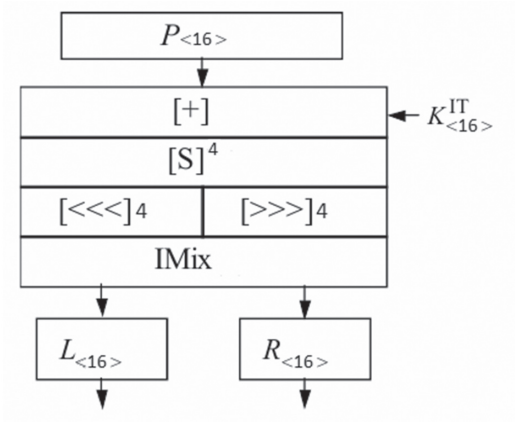

Рис. 2. Начальное преобразование IT

В уменьшенной версии шифра операция IMix реализуется следующим образом: складываются по модулю два левые 8 бит с правыми входных данных, после, результат сдвигается циклически влево.

Конечное FT преобразование (рис. 3) выполняет те же операции, что и начальное, но только в обратном порядке.

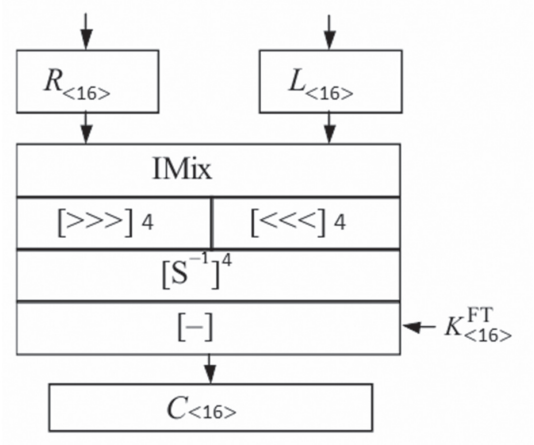

Рис. 3. Конечное преобразование FT

Второй тип начального и конечного преобразований строится на основе идеи, изложенной в нашем патенте «Недетермінований спосіб криптографічного перетворення блоків даних» [6].

Здесь имеется в виду предложение по построению циклового преобразования с управляемыми подстановками, причем управление осуществляется в отличие от известных подходов не с помощью битов циклового подключа, а на основе использования в качестве управляющего воздействия результата нелинейного преобразования предыдущего S-блока. В этом случае в качестве таблиц нелинейной замены (S-блоков) используются сразу целые наборы противоречивых подстановок, называемые в математической литературе латинскими прямоугольниками [7]. Идею предлагаемого способа построения преобразования с управляемыми подстановками (в 16-битной редакции) поясняет рис. 4.

Входной 16-битный блок данных разбивается на 4-х битные подблоки B_0, B_1, B_2, B_3 и осуществляется поочередное преобразование подблоков на основе наборов управляемых подстановок в виде латинских прямоугольников размером $2^4 \times 2^4$.

Одним (″информационным″) входом в латинский прямоугольник является текущий подблок данных B_i, а вторым (″управляющим″) входом является результат (4-х битный блок), полученный на предыдущем шаге преобразования. В качестве инициализирующего подблока выступает вектор инициализации IV_1 (4-х битная константа). Преобразование на основе управляемой подстановки выполняется в обе стороны (двумя слоями). Перед первым слоем осуществляется операция сложения по модулю 2 с подключом. Очевидно, что потребуется вектор инициализации и для второго слоя преобразований. В качестве такового может выступать константа IV_2, либо B_3 или выход последней подстановки предыдущего слоя. На рис. 5 представлена схема реализации второго слоя преобразований с управляемыми подстановками.

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

Далее мы будем интересоваться показателями стойкости шифров к атакам дифференциального крипоанализа в виде максимального значения их полных дифференциалов. Оценим сначала влияние на значения полных дифференциалов оговоренных выше конструкций шифрующих преобразований вида (м.б. моделей) S-блоков (известных и случайно сгенерированных), использованных

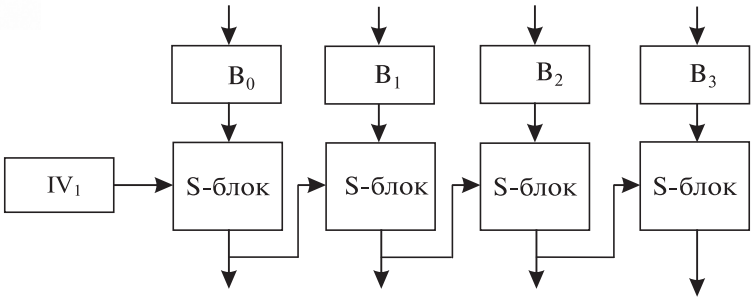

Рис. 4. Слой преобразования с управляемыми подстановками (16-битный вариант)

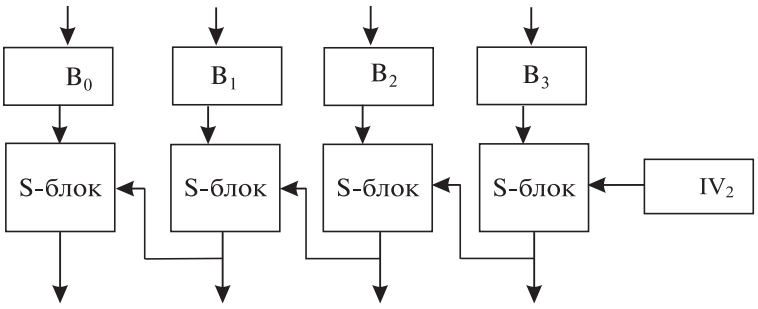

Рис. 5. Второй слой преобразований с управляемыми подстановками

при реализации каждой из конструкций. Список S-блоков, примененных в вычислительных экспериментах, приведен ниже в табл. 1.

Таблица 1

Варианты использованных S-блоков с расшифровкой их описаний

Варианты использованных S-блоков	Расшифровка описания S-блоков
SboxAESD4 ={A,4,3,B,8,E,2, C,5,7,6,F,0,1,9,D}; SboxHEYS D8 ={E,4,D,1,2,F, B,8,3,A,6,C,5,9,0,7}; SboxD6F2 = {B,C,5,0,1,3,2,7,8, 4,D,F,6,9,E,A}; SboxD6F0 = {4,6,F,B,E,7,5, D,9,C,1,0,3,8,A,2}; SboxD12F0 = {8,3,1,9,A,B,E, C,5,D,F,2,0,4,7,6}; SboxD8F0 = {C,9,4,6,8,E,D,5, 3,F,B,0,A,2,1,7}.	DX – X максимальное значение в дифференциальной таблице S-блока; FY – Y количество фиксированных точек ($S(x)=x$). Отсутствие FY в описании S-блока эквивалентно F0.

В их числе представлены S-блок мини версии шифра AES [8], S-блок шифра из работы [3] (первая строка S-блока шифра DES), остальные S-блоки сгенерированы случайным образом (выбраны из случайно сгенерированных S-блоков). Во всех вариантах рассматриваемых в дальнейшем конструкций шифров будут использоваться одни и те же (одинаковые) наборы S-блоки.

Первая серия экспериментов была проведена с 16-битным SPN шифром в том виде, в котором он представлен в работе проф. Хейса, где в качестве начального и конечного преобразований используется простое побитное сложение с цикловыми 16-битными подключами (начальное преобразование в виде $M = P \oplus K_0$ и конечное в виде $C = M' \oplus K_{r+1}$). Полученные значения полного дифференциала для различных вариантов S-блоков в зависимости от числа циклов преобразования представлены в табл. 2.

Анализ результатов показывает, что все варианты S-блоков, кроме последнего, выходят на асимптотическое значение максимума полного дифференциала в пределах первых девяти циклов итеративных преобразований. В то же время нашелся S-блок, который не достиг асимптотического значения на тринадцати циклах, однако это скорее исключение, чем правило (этот S-блок выходит за рамки случайного и по числу инверсий – 75 и не укладывается в границы случайного по критерию 4: он имеет 5 максимальных значений равных 8). Правда, не укладывается в рамки случайного и S-блок шифра мини AES (это одноцикловая подстановка с минимальным значением максимума XOR таблицы равным 4 и таких значений в таблице 15), а также не проходят критерий инверсий S-блоки SboxD6F0 и SboxD12F0.

Интересно отметить, что для S-блока SboxHEYSD8 асимптотическое значение 19 при нахождении полного дифференциала достигается на два цикла быстрее, чем для S-блока SboxAESD4 (S-блока, построенного по идеям разработчиков Rijndael).

Во второй серии экспериментов рассматривалась модель SPN шифра рис 1, в которой в качестве начального преобразования вместо операции XOR использовалось IT-преобразование вида $M = (P + K_0) \bmod 2^{16}$, при этом конечное преобразование FT не менялось, т.е. оно имело вид $C = M' \oplus K_{r+1}$. Соответствующие результаты расчётов представлены в табл. 3.

Сравнивая полученные результаты с таблицей 1, можно сделать вывод, что применение сложения по модулю 2^{16} в качестве начального преобразования существенных улучшений (более быстрого достижения асимптотического значения 19) не даёт).

Но в случае применения S-блоков SboxHEYSD8 заметно уменьшение значений полного дифференциала при числе циклов меньшем 7.

Далее было исследовано поведение значения полного дифференциала в случае, когда:

– начальное преобразование аналогично IT-преобразованию шифра «Лабиринт»;

– конечное преобразование имеет вид $C = M' \oplus K_{r+1}$.

Таблица 2

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

Sbox / r	SboxAESD4	SboxHEYSD8	SboxD6F2	SboxD6F0	SboxD12F0	SboxD8F0
1	16384,00	32768,00	24576,00	24576,00	49152,00	32768,00
2	4096,00	12288,00	6144,00	6144,00	15552,00	8192,00
3	2036,27	2303,33	2802,40	1920,00	1587,20	3432,00
4	596,00	222,27	649,33	601,20	613,13	1184,47
5	190,33	64,13	292,93	148,93	265,73	457,07
6	77,47	24,80	71,47	50,00	104,87	178,40
7	35,87	**18,80**	32,00	22,00	46,87	87,33
8	21,07	18,80	19,67	**19,07**	23,87	39,93
9	**19,27**	19,00	**18,93**	18,87	19,13	24,60
10	19,33	18,93	19,33	19,27	19,00	24,27
11	18,87	19,27	18,93	19,20	19,13	23,80
12	19,27	18,93	19,00	18,73	18,93	23,93
13	19,20	18,87	18,87	19,20	19,33	24,07

Таблица 3

Алгоритм Хейса с начальным сложением блоков данных с цикловым подключом (первичным забеливанием) по модулю 2^{16}

Sbox / №	SboxAESD4	SboxHEYSD8
1	16330,13	26016,60
2	3903,00	7403,60
3	1637,73	964,47
4	485,07	128,27
5	150,40	47,53
6	65,87	20,27
7	31,20	**19,07**
8	19,80	19,00
9	**19,07**	19,27
10	18,93	18,93
11	19,07	19,00
12	19,47	18,93
13	18,93	18,87

В этом эксперименте значение полного дифференциала при различном числе циклов преобразования имеет вид, представленный в табл. 4.

Таблица 4

Алгоритм Хейса с начальным IT-преобразованием шифра «Лабиринт»

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	10068,87	7141,73	1234,13
2	1982,60	2229,20	313,07
3	549,73	296,33	127,67
4	220,80	37,93	47,67
5	94,00	**19,07**	22,80
6	42,33	19,33	**19,07**
7	22,47	19,20	19,40
8	**19,47**	19,20	19,40
9	19,27	19,07	19,00
10	19,53	18,87	19,00
11	19,47	19,27	19,00
12	19,67	19,00	19,33
13	19,47	19,27	19,47

Из таблицы видно, что использование IT-преобразования резко уменьшает количество циклов, необходимое для достижения значения 19. Даже при использовании S-блока SboxD8F0, который в первой серии экспериментов не достигал необходимого значения, теперь оно приходит к значению 19 при 8 циклах.

В табл. 5 представлены значения полного дифференциала, для случая, когда начальное и конечное преобразования эквивалентны преобразованиям IT и FT в шифре «Лабиринт».

Результаты таблицы 5 свидетельствуют, что применение IT и FT преобразований значительно уменьшает количество циклов, необходимых для достижения значения 19 по сравнению с оригинальными начальными и конечными преобразованиями, использованными в SPN шифре Хейса.

Таблица 5

Алгоритм Хейса с начальным IT-преобразованием и FT-преобразованием шифра «Лабиринт»

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	733,13	517,13	517,20
2	132,93	76,87	40,67
3	25,67	23,93	20,20
4	20,07	**19,27**	**19,33**
5	**19,20**	19,27	18,93
6	18,67	19,27	19,53
7	19,27	18,93	19,07
8	19,07	18,93	19,07
9	19,00	19,13	19,13
10	19,53	19,33	19,20
11	19,00	19,07	18,93
12	19,13	19,00	18,87
13	19,40	19,00	18,93

Наконец, была проведена серия экспериментов, в которых было исследовано влияние на значения полного дифференциала применения в качестве IT и FT преобразований в структуре SPN шифра рис.1 управляемых подстановок в виде латинских прямоугольников. Результаты этих экспериментов иллюстрирует табл. 6.

Таблица 6

Алгоритм Хейса с преобразованиями, использующими латинский прямоугольник

Sbox / №	Sbox-D8F0	SboxHEYSD8	SboxAESD4
1	156,67	88	100,80
2	34,53	**18,87**	35,87
3	21,20	18,93	19,80
4	**19,13**	18,87	**19,07**
5	19,20	19,27	19,60
6	18,73	19,13	18,93
7	19,00	19,13	18,93
8	19,07	19,33	19,07
9	19,13	19,07	19,27
10	19,53	19,00	18,80
11	19,00	19,00	19,13
12	19,13	19,20	19,13
13	18,93	19,07	19,20

Из таблицы видно, что при применении слоев управляемых подстановок в качестве начального и конечного преобразований асимптотическое значение 19 достигается при минимальном числе циклов равном 2, что существенно эффективнее, чем в уменьшенной версии шифра мини-AES. Мы сделали для этого лучшего варианта просмотр максимальных значений полных дифференциалов для всех вариантов ключей. Результаты представлены в табл. 7.

При этом среднее значение полного дифференциала для 2-х циклового преобразования равно 19,11. Можно сделать вывод, что на двух циклах шифр приходит к асимптотическому значению.

Таблица 7

Максимальные значения дифференциалов двухцикловых характеристик

Мах значение полной диф. хар-ки	Их количество
18	31367
20	31962
22	2109
24	93
26	5

ЗАКЛЮЧЕНИЕ

Таким образом, на примере построения полных дифференциалов уменьшенных моделей 16-битного SPN шифра Хайса с различными начальными и конечными преобразованиями продемонстрирована возможность построения шифрующего преобразования более эффективного, чем реализованное в стандарте AES.

Однако, для того чтобы представлять общую картину, необходимо еще провести ряд дополнительных исследований: посмотреть, как будет себя вести с различными подстановками уменьшенная версия шифра Rijndael со случайными S-блоками и специально сгенерированными (удовлетворяющие критериям случайности), параллельно посмотреть ряд других алгоритмов (например, финалистов проекта NESSIE).

Литература.

[1] *Долгов В.И., Лисицкая И.В., Киянчук Р.И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции «Компьютерные науки и технологии», 8-10 октября 2009 г., Белгород, Ч. II, С. 32-35.

[2] *Feistel, H.* Cryptography and Computer Privacy [Текст] / H. Feistel. // Scientific American. – May 1973. Vol. 228. – PP. 15–23.

[3] *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p 189-221.

[4] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6, № 2. – С. 230-240.

[5] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра «Лабиринт». // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. Том. 8, № 3. – С. 283-289.

[6] *Долгов В.І., Супронюк С.В., Лисицька І.В.* Спосіб недетермінованого криптографічного перетворення блоків даних. Деклараційний патент на винахід 53949 А, Бюл. № 2, від 17.02.2003.

[7] *Скачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука – 1982 – 384 с.

[8] *Долгов В.И., Кузнецов А.А., Лисицкая И.В., Сергиенко Р.В., Олешко О.И.* Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. – Т. 8. – №3. – С. 268-277.

[9] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES // Прикладная радиоэлектроника: научн.-техн. журнал. – 2009. – Т. 8 № 3. – С. 252-257.

Поступила в редколлегию 23.06.2010.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Казимиров Александр Владимирович, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

УДК 681.3.06

Варіації на тему шифра Rijndael / В.І. Долгов, І.В. Лисицька, А.В. Казимиров // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 321-325.

Розглядається підхід до аналізу показників криптографічної стійкості блокових симетричних шифрів, які будуються на основі дослідження властивостей зменшених версій цих шифрів. З використанням цього підходу оцінюються показники стійкості до атак диференційного криптоаналізу декількох модифікацій SPN шифра з 16-бітовим входом, який має структуру загального типу, що була запропонована у роботі Говарда Хейса. Показується, що існують рішення, що перевершують по показникам стійкості шифр Rijndael.

Ключові слова: симетричний блоковий шифр, криптоаналіз, Rijndael.

Табл. 07. Іл. 05. Бібліогр.: 09 найм.

UDC 681.3.06

Variations on Rijndael cipher theme / V.I. Dolgov, I.V. Lisitskaya, O.V. Kazimirov // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 321-325.

The paper considers an approach to the analysis of symmetric block ciphers cryptographic strength indices which is based on the research of the properties of reduced versions of these ciphers. Using this approach estimates strength indices to differential cryptanalysis attacks of several modifications of the 16-bit input SPN cipher haping a general type structure proposed in the work by Howard Heys. It is shown that there exist solutions which exceed the Rijndael in strength indices.

Key words: symmetric block cipher, cryptanalysis, Rijndael.

Tab. 07. Fig. 05. Ref.: 09 items.