Наводяться результати аналізу диференційних та лінійних властивостей шифрів Rijndael, Serpent, Threefish при 16-бітних вхідних і вихідних блоках даних, які свідчать, що всі представлені шифри повторюють в розглянутому режимі застосування властивості випадкових підстановок. Отримані результати є додатковим свідченням, що повномасштабні шифри, як і їх малі версії, асимптотично повторюють властивості випадкових підстановок відповідного степеня

Ключові слова: випадкова підстановка, максимум лінійної ймовірності, максимум диференціальної ймовірності

Приводятся результаты анализа дифференциальных и линейных свойств шифров Rijndael, Serpent, Threefish при 16-битных входных и выходных блоках данных, свидетельствующие, что все представленные шифры повторяют в рассмотренном режиме применения свойства случайных подстановок. Полученные результаты являются дополнительным свидетельством того, что полномасштабные шифры, как и их малые версии, асимптотически повторяют свойства случайных подстановок соответствующей степени

Ключевые слова: случайная подстановка, максимум линейной вероятности, максимум дифференциальной вероятности

УДК 621. 391:519.2:519.7
DOI: 10.15587/1729-4061.2015.51701

АНАЛИЗ ДИФФЕРЕНЦИАЛЬНЫХ И ЛИНЕЙНЫХ СВОЙСТВ ШИФРОВ RIJNDAEL, SERPENT, THREEFISH ПРИ 16-БИТНЫХ ВХОДАХ И ВЫХОДАХ

И. В. Лисицкая
Доктор технических наук, профессор
Кафедра безопасности
информационных систем и технологий
Харьковский национальный
университет им. В. Н. Каразина
пл. Свободы, 4, г. Харьков, Украина, 61002
E-mail: dolgovvi@mail.ru
Т. А. Гриненко
Кандидат технических наук, доцент*
E-mail: t_lame@mail.ru
С. Ю. Бессонов*
E-mail: stanislav.93@bk.ru
*Кафедра безопасности информационных технологий
Харьковский национальный
университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166

1. Введение

В настоящий момент существует два основных метода криптографического анализа блочных симметричных шифров (БСШ) – дифференциальный и линейный криптоанализ. Если алгоритм выдерживает атаку с использованием этих двух методов, то он считается стойким и может быть использован при передаче конфиденциальных данных.

Для изучения стойкости современных БСШ к дифференциальному, линейному и другим видам криптоанализа обычно используются критерии, которые не гарантируют реальную стойкость шифра.

Например, при проверке стойкости к дифференциальному криптоанализу определяют верхнюю границу вероятности дифференциальных характеристик, однако этот показатель не может гарантировать стойкость БСШ к дифференциальному криптоанализу. Для больших гарантий стойкости следует проверять точный критерий, то есть вероятность дифференциала. Но точный критерий можно проверить только для шифров с небольшим размером блока. Аналогичным образом складывается ситуация и при проверке стойкости шифра к линейному криптоанализу, при изучении циклических свойств шифра, при поиске слабых и эквивалентных ключей. Целью настоящего исследования является изложение подходов к построению уменьшенных (масштабированных) моделей блочных шифров (размер ключа и размер блока не превышают 16 битов), методов тестирования этих моделей, а также обсуждение результатов оценки стойкости уменьшенных моделей современных БСШ.

2. Анализ литературных данных и постановка проблемы

До начала 90-х годов в мировой открытой печати практически не было фундаментальных работ, посвященных блочным симметричным шифрам. Исключением были исследования, касающиеся криптографического алгоритма DES. Критике подвергались, прежде всего, малая длина ключа, недостаточное количество циклов преобразования. Немаловажный аспект критики – отсутствие публикаций о критерии проектирования и показателях оценки. По сути, все атаки сводились к атакам грубой силы (прямого перебора), которые на тот момент из-за ограниченных ресурсов компьютеров не могли быть практически

реализованы [1]. Среди официальных документов, посвященных DES и его модификации DEA, необходимо отметить публикацию федерального стандарта 1981 года – FIPS-74.

В дальнейшем появляется ряд работ [2, 3], которые были посвящены анализу схем развертывания ключей в БСШ. Фундаментальной работой можно считать публикацию Бихама [4]. В данной работе впервые описана атака на схему развертывания ключей типа «связанные ключи», которая могла быть применена к БСШ. Однако этот метод криптоанализа с атакой на схему развертывания ключей имел больше теоретическую, чем практическую ценность, и не представлял, по сравнению с дифференциальным и линейным криптоанализом цикловой функции шифра, реальной угрозы.

Далее поиск новых решений коснулся совершенствования криптографических преобразований цикловой функции. Появляется ряд новых криптографических алгоритмов PES, RC5 и SAFER. В дальнейшем на указанные шифры были разработаны эффективные методы криптоанализа через схемы разворачивания ключей.

Дальнейший анализ показал, что до конца 90-х сложилась ситуация, при которой в несекретных государственных и коммерческих учреждениях использовали морально и технически устаревшие шифры. Кроме того, разработанные криптографические алгоритмы не подтвердили необходимый уровень безопасности, чтобы стать заменой существующих стандартов шифрования. В январе 1997 года NIST США объявил о начале конкурса на новый стандарт шифрования XXI века AES (Advanced Encryption Standard) [5]. В результате выполнения этого проекта по результатам голосования победителем был объявлен алгоритм Rijndael [6]. По аналогии с проектом AES в 2000 году в Европе был развернут и выполнен проект NESSIE. В ходе этих проектов подтверждено, что использование схемы формирования цикловых ключей с высокими криптографическими свойствами позволит снизить уровень затрат на проектирование цикловой функции и уменьшить количество итераций [7]. Также показано, что криптографически сильная схема разворачивания ключей повышает устойчивость к линейному и дифференциального криптоанализу [8, 9].

В предыдущих работах [10, 11] была предложена методика оценки дифференциальных и линейных показателей шифров, строящаяся на основе использования полномасштабных шифров в режиме их активизации укороченными 16-битными блоками данных. В них решалась задача подтверждения одного из основных положений новой методологии оценки стойкости блочных симметричных шифров [11], в соответствии с которым все современные итеративные шифры асимптотически (на полноцикловой длине) приобретают свойства случайных подстановок.

Практически проверить многие теоретические результаты оценок дифференциальных и линейных показателей удалось впервые на основе использования уменьшенных (малых) моделей шифров, являющихся основой развиваемого подхода. Именно с помощью экспериментов с уменьшенными моделями были получены основные содержательные результаты, подтверждающие новую идеологию оценки показателей доказуемой стойкости шифров и обладающие высокой степенью доверия, не достижимой для всех известных до последнего времени методов и подходов.

Идея развиваемого подхода состояла в том, чтобы убедиться, что полномасштабные шифры в режиме их активизации укороченными 16-битными блоками данных должны продемонстрировать показатели случайности уменьшенных моделей, для которых уже был накоплен уже большой объём материала [12–15]. Этими публикациями подтверждается, что асимптотические показатели уменьшенных моделей шифров совпадают со свойствами случайных подстановок соответствующей степени. В отмеченных работах были рассмотрены шифры Rijndael, ГОСТ 28147 и FOX. Эксперименты с этими шифрами полностью подтвердили справедливость развиваемого подхода.

В этой работе представлены результаты вычислительных экспериментов с шифрами Rijndael, Serpent, Threefish. Программные реализации этих шифров взяты из Интернета. Речь идет об оценке линейных и дифференциальных свойствах этих шифров. В этой работе для исследования взяли шифр Rijndael, как дополнительную проверку ранее полученных результатов.

Будет показано, что и эти шифры повторяют свойства уменьшенных до 16-битных входов моделей.

3. Цель и задачи исследования

Целью работы является анализ криптографических свойств фейстель-подобных и SPN (Substitution-Permutation Network) блочных шифров, а именно Rijndael, Serpent, Threefish с уменьшенным размером блока и ключа (8 или 16 битов). В ходе анализа необходимо проверить, что все представленные шифры повторяют в рассмотренном режиме применения свойства случайных подстановок. Этот результат позволит подтвердить основные положения новой методологии ускоренного криптоанализа блочных симметричных шифров к атакам линейного и дифференциального криптоанализа. Эти положения состоят в том, что все современные блочные шифры через определенное число циклов по законам распределения переходов таблиц *XOR* разностей (полных дифференциалов) и законам смещений таблиц линейных аппроксимаций (линейных оболочек) повторяют соответствующие показатели случайных подстановок.

Для достижения поставленной цели необходимо провести анализ показателей случайности шифров. При этом проверка показателей случайности больших шифров может быть выполнена на основе разработки и последующего анализа показателей случайности уменьшенных моделей, которые допускают проведение вычислительных экспериментов в реальные временные сроки.

4. Построение уменьшенных моделей блочных симметричных шифров

В рамках проведенных исследований рассматривались криптографические свойства фейстель-подобных и SPN (Substitution-Permutation Network) блочных шифров с уменьшенным размером блока и ключа

(8 или 16 битов). Целесообразность рассмотрения именно уменьшенных моделей шифров объясняется тем, что для изучения стойкости шифра к дифференциальной и линейной атаке следует, соответственно, оценивать вероятности полных дифференциалов и вероятности линейных корпусов – параметры, которые можно оценить только для шифра с небольшим размером блока. В качестве операций перемешивания и рассеивания были взяты преобразования, предложенные в [11] для уменьшенной версии шифра Rijndael. На рис. 1 и 2 схематически представлены преобразования, которые выполняются в рассматриваемых моделях фейстель-подобных и SPN шифров.

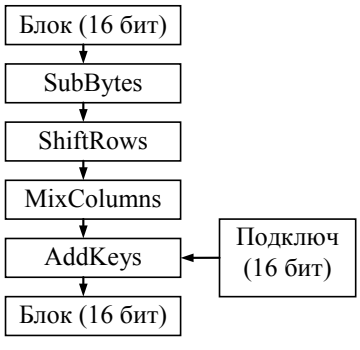

Рис. 1. Схема одного цикла SPN-шифра

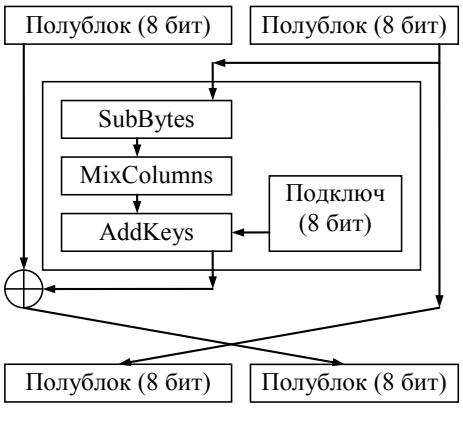

Рис. 2. Схема одного цикла фейстель-подобного шифра

К основным особенностям предложенных уменьшенных моделей шифров следует отнести:

– размер блока 16 бит, размер ключа 8 бит или 16 бит;

– структура блока для SPN шифра: 2 колонки по 2-а 4-битовых элемента или 1 колонка из 4-ех 4-битовых элемента;

– структура полублока для фейстель-подобного шифра: 2-а 4-битовых элемента;

– умножение элементов каждой колонки на фиксированную МДР-матрицу размером 2 на 2 над $GF(2^4)$ или умножение единственной колонки, состоящей из 4-ех 4-битовых элементов, на фиксированную МДР-матрицу размером 4 на 4 над $GF(2^4)$ (MixColumns);

– подстановка 4 в 4 бита (SubBytes);

– число ветвей активизации линейного преобразования MixColumns B=3 (МДР-матрица размером 2 на 2 над $GF(2^4)$) или B=5 (МДР-матрица размером 4 на 4 над $GF(2^4)$).

5. Дифференциальные свойства шифров Rijndael, Serpent, Threefish

В соответствии с развиваемой методикой [11], большой шифр используется как бы как малый для шифрования блоков данных уменьшенной длины (зашифрованные блоки данных тоже усекаются до необходимого размера), при этом сохраняются все преобразования и внутренние связи большого шифра. Самое же примечательное при таком подходе это то, что появляется возможность применить весь наработанный аппарат изучения показателей случайности малых версий шифров для изучения показателей случайности больших шифров.

В проведенном эксперименте длина ключа и блока для шифров Rijndael и Serpent была взята одинаковой и равной 128 битам, а в реализации шифра Threefish использовалась длина для блока и ключа 512 бит.

В первом эксперименте были построены законы распределения переходов XOR таблиц всех трёх шифров на полноцикловой длине.

В табл. 1 представлены результаты поциклового распределение значений ячеек таблицы XOR-разностей для 16-битных сегментов входных и выходных блоков данных всех трех шифров после всех раундов преобразований (Rijndael – 10, Serpent – 32, Threefish –72). Вычисления проводились с использованием 30 различных выбранных случайно ключей зашифрования.

Таблица 1

Распределение значений ячеек таблицы XOR-разностей для 16-битных сегментов шифртекстов

Значение перехода $2k$	Количество переходов (Rijndael)	Количество переходов (Serpent)	Количество переходов (Threefish)
0	2604948298	2604933270	2604928534
2	1302476170	1302501597	1302508996
4	325620651	325614188	325612232
6	54268159	54265223,5	54265483,9
8	6783987,73	6782692,47	6782055,87
10	678135,4	678425,133	678148,067
12	56512,2	56524,067	56449,467
14	4045,33	4027,133	4061,533
16	252,6	261,267	249,467
18	13,93	15,267	13,667
20	0	0	0

В табл. 2 представлены для сравнения результаты расчётов распределения ячеек дифференциальной таблицы случайной подстановки степени 2^{16}.

Из табл. 1 и 2 следует, что распределения значений ячеек таблицы XOR-разностей для 16-битных сегментов шифртекстов для всех трех шифров очень близки к результатам случайной подстановки. Можно сделать вывод, что законы распределения переходов полных дифференциалов для всех трёх рассмотренных шифров асимптотически приходят к дифференциальному закону случайной подстановки степени 2^{16}.

В табл. 3 приводятся поцикловые распределения значений максимумов полных дифференциалов для исследуемых шифров. Для криптоалгоритмов Serpent и Threefish показаны первые 10 циклов, чего вполне

достаточно для свидетельствования того, что шифры реализуют свой асимптотический показатель среднего значения максимума полных дифференциалов.

Таблица 2

Расчётные значения закона распределения переходов XOR таблицы случайной подстановки степени 2^{16}

Значение перехода 2k	Количество переходов (расчет для подстановки)
0	2605070418
2	1302484861
4	325626184
6	54271858
8	6784085
10	678418
12	56535
14	4038
16	252
18	14
20	1

Таблица 3

Поцикловые значения максимумов полных дифференциалов для 16-битных сегментов

Число циклов, r	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	16384	18,93	65536
2	8904,25	19,24	65536
3	1911.47	18,64	65536
4	19,24	18,33	42440,04
5	20,31	18,75	30704,23
6	18,83	19,21	9534,57
7	19,21	18,98	37,75
8	19,4	18,37	19,27
9	18,33	19,24	18,78
10	19,17	19,63	18,44

Результаты свидетельствуют о том, что шифрующие преобразования асимптотически для различных ключей зашифрования ведут себя как случайная подстановка, т. е. и для них оказываются справедливыми расчетные соотношения, которые найдены для случайных подстановок [12, 13]. Представленные для анализа шифры по-разному выходят на асимптотический показатель среднего значения максимума. Rijndael после 4-го цикла (раунда), шифр Serpent выходит на данный показатель уже после 1-го цикла шифрующего преобразования за счет наличия в алгоритме начальной перестановки. Threefish выходит на асимптотический показатель среднего значения максимума только с 8-го цикла. На основе полученных ранее и здесь результатов можно, тем не менее, предложить подход к сравнению эффективности решений по построению алгоритмов шифрования (при прочих равных условиях) в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов.

Одновременно можно отметить, что полученные результаты анализа шифра Rijndael практически повторили результаты, приведенные в [11].

6. Линейные свойства шифров Rijndael, Serpent, Threefish

Была выполнена серия экспериментов для рассмотренных шифров, когда в них используются S-блоки с различными показателями нелинейности. Отобранные конструкции S-блоков представлены в табл. 4.

Таблица 4

Полубайтовые подстановки (S-блоки) с различными показателями нелинейности

Нелинейность	S-блок
0	S_1 = {12, 13, 5, 1, 10, 11, 6, 2, 14, 3, 7, 15, 4, 0, 8, 9}
2	S_2 = {5, 0, 13, 6, 4, 8, 2, 3, 9, 1, 15, 10, 12, 14, 7, 11}
2	S_3 = {10, 4, 5, 8, 2, 15, 7, 0, 14, 9, 11, 12, 6, 13, 1, 3}
4	S_4 = {2, 5, 0, 9, 3, 14, 4, 1, 10, 11, 8, 15, 7, 12 ,6, 13}
4	S_5 = {10, 4, 3, 11, 8, 14, 2, 12, 5, 7, 6, 15, 0, 1, 9 ,13}

Представленные в таблице подстановки были использованы в качестве S-блоков во всех исследуемых малых моделях шифров (в каждом шифре использовались S-блоки с одинаковыми показателями нелинейности).

В процессе вычислительных экспериментов определялись поцикловые средние значения максимумов смещений линейных корпусов ($\sqrt{\mathrm{ALHMP}\cdot 2^{n-1}}$) уменьшенных моделей трех шифров из представленных.

Для каждого шифра с фиксированным числом циклов шифрования выполнялось построение линейных корпусов (таблиц линейных аппроксимаций) для 30 различных ключей зашифрования, сгенерированных случайным образом и определялись максимальные значения смещения для каждой из таблиц, а затем результаты усреднялись. Строилась зависимость средних значений максимумов смещений линейных корпусов от числа циклов зашифрования.

Для криптоалгоритмов Serpent, Threefish и Rijndael как и в предыдущем случае показаны первые 10 циклов.

В табл. 5 представлены математические ожидания максимальных значений смещений линейных корпусов для всего набора исследуемых шифров в зависимости от числа циклов шифрования r.

Таблица 5

Математические ожидания максимальных смещений линейных корпусов полных моделей шифров

Число циклов, r	MAX (Rijndael)	MAX (Serpent)	MAX (Threefish)
1	0	810,4	32768
2	16313,36	825,0667	32680,93
3	7728,66	828,2667	31306,13
4	817,43	825,9333	23730,93
5	821,98	828,4667	19722,67
6	825,716	824,8667	19722,67
7	817,367	820,3333	7899,8
8	820,167	817,5333	844,0667
9	821,767	820,4	822,1333
10	820,167	816,6	815,8

Представленные результаты свидетельствуют о том, что и в случае рассмотрения линейных показателей, блочные симметричные шифры после определенного числа раундов повторяют свойства случайных подстановок. Шифр Rijndael приходит к показателям случайно подстановки после 4-го цикла, шифр Serpent приходит к установившемуся значению максимума линейного корпуса, характерному для случайных подстановок уже после 1-го раунда шифрующего преобразования за счет наличия в алгоритме начальной перестановки. Threefish выходит на асимптотический показатель среднего значения максимума только с 8-го раунда.

Таким образом, дифференциальные и линейные свойства шифрующих преобразований исследуемых шифров (при заявленном числе циклов преобразования) являются одним из проявлений свойств случайных подстановок.

7. Выводы

Как следует из представленных результатов, дифференциальные и линейные свойства рассмотренных шифрующих преобразований (при заявленном числе циклов преобразования) повторяют показатели случайных подстановок. Экспериментальные результаты также свидетельствуют о том, что реальные асимптотические (при полных наборах цикловых преобразований) значения максимальных и средних вероятностей дифференциальных и линейных характеристик (полных дифференциалов и линейных корпусов) для рассмотренных шифров являются свойством, не зависящим ни от свойств *S*-блоков, ни от числа циклов (после определенного их числа). Прекрасным примером послужил анализ блочного симметричного шифра Threefish, в шифрующем преобразовании которого не используются таблицы нелинейных замен. Особенностью шифрующего преобразования в виде БСШ, рассматриваемого как подстановка, является существенно меньшее множество реализуемых им подстановок. БСШ реализует только 2^n (по числу ключей) подстановок из общего их числа $2^n!$, причем, несмотря на такое существенное уменьшение допустимого множества подстановок, оно продолжает сохранять свойства, характерные для множества случайных подстановок.

Представленные результаты также подтверждают подход к оценке эффективности алгоритмов шифрования в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов и смещений линейных корпусов. Шифр Rijndael реализует данный показатель после 4-го цикла шифрования, шифр Serpent уже после 1-го цикла, шифр Threefish выходит на данный показатель после 8-го цикла шифрования.

Второй важный вывод, следующий из представленных результатов, сводится к тому, что показатели стойкости больших (полных реализаций) шифров к атакам дифференциального и линейного криптоанализа (таких шифров, как Rijndael и многих других известных шифров) могут быть получены расчетным путем.

Литература

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ [Текст] / Б. Шнайер. – М.: «Триумф», 2002. – 797 с.2. Biham, E. Differential cryptanalysis of DES-like cryptosystems. Advances in Cryptology [Text] / E. Biham, A. Shamir // CRYPTO'90(LNCS 537), 1990. – P. 2–21.
2. Langford, S. K. Differential-linear cryptanalysis. Advances in Cryptology [Text] / S. K. Langford, M. E. Hellman // Lecture Notes in Computer Science. CRYPTO'94(LNCS 839), 1994. – P. 17–25. doi: 10.1007/3-540-48658-5_3
3. Biham, E. Differential cryptanalysis of the full 16-round DES. Advances in Cryptology [Text] / E. Biham, A. Shamir // Lecture Notes in Computer Science. CRYPTO'92(LNCS 740), 1993. – P. 487–496. doi: 10.1007/3-540-48071-4_34
4. Advanced Encryption Standard [Electronic resource]. – FIPS 197, 2001. – Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
5. AES discussion forum [Electronic resource]. – Available at: http://aes.nist.gov
6. Lim, C. H. CRYPTON: A New 128-bit Block Cipher [Text] / C. H. Lim. – NIST AES Proposal, 1998.
7. Ohkuma, K. Security Assessment of Hierocrypt and Rijndael against the Differential and Linear Cryptanalysis [Text] / K. Ohkuma, H. Shimizu, F. Sano, S. Kawamura // In Proceedings of the 2nd NESSIE workshop, 2001.
8. Park, S. On the security of Rijndael-like structures against differential and linear cryptanalysis [Text] / S. Park, S. H. Sung, S. Chee, E-J. Yoon, J. Lim. // Advances in Cryptology, Proceedings of Asiacrypt '02, LNCS 2501, 2002. – P. 176–191. doi: 10.1007/3-540-36178-2_11
9. Лисицкая, И. В. Большие шифры - случайные подстановки [Текст] / И. В. Лисицкая, А. А. Настенко // Межведомственный научн. технический сборник "Радиотехника". – 2011. – Вып. 166. – С. 50–55.
10. Лисицкая, И. В. Методология оценки стойкости блочных симметричных шифров [Текст] / И. В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.
11. Долгов, В. И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс [Текст] / В. И. Долгов, А. А. Кузнецов, С. А. Исаев // Электронное моделирование. – 2011. – Т. 33, № 6. – С. 81–99.
12. Долгов, В. И. Свойства таблиц линейных аппроксимаций случайных подстановок [Текст] / В. И. Долгов, И. В. Лисицкая, О. И. Олешко // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 334–340.
13. Keliher, L. Toward the true random cipher: On expected linear probability values for SPNs with randomly selected s-boxes [Text] / L. Keliher, H. Meijer, S. Tavares. – Communications, Information and Network Security, 2003. – P. 123–146. doi: 10.1007/978-1-4757-3789-9_8
14. Zhang, X. M. Non-existence of Certain Quadratic S-boxes and Two Bounds on Nonlinear Characteristics of General S-boxes [Electronic resource] / X. M. Zhang, Y. Zheng, H. Imai, 1997. – P. 1–18. – Available at: http://webpages.uncc.edu/yzheng/publications/files/sac97-non-existence-of-certain.pdf