УДК 681.3.06: 519.248.681

И.В. ЛИСИЦКАЯ, канд. техн. наук , А.А. НАСТЕНКО

БОЛЬШИЕ ШИФРЫ – СЛУЧАЙНЫЕ ПОДСТАНОВКИ

Введение

В этой работе речь идет об обосновании новой точки зрения по оценке безопасности блочных шифров к атакам дифференциального и линейного криптоанализа, пропагандируемой в работе [1].

Эта точка зрения появилась на основе развития нового подхода в теории и методах криптоанализа, родившегося на кафедре БИТ ХНУРЭ [2]. Он ориентирован, как уже было отмечено в [1], с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – уточненной 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. Предлагаемая идеология основывается на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров (DES, ГОСТ, Rijndael, Лабиринт, Мухомор, Калина, ADE, Камелия, FOX и многих других) положении, состоящем в том, что все эти шифры (и большие, и малые их версии) через определенное число циклов (для рассмотренных уменьшенных моделей – от трех циклов до девяти) независимо от используемых в шифрах S-блоков (речь идет не о вырожденных их конструкциях) 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 [3 – 5]). Соответствующее свойство (переходный период к некоторому установившемуся значению полных дифференциалов и линейных корпусов) отмечается в ряде публикаций и для больших шифров (например, в [6] для шифра Rijndael).

В отношении сохранения в малом шифре свойств большой модели следует отметить, что мы говорим лишь о сохранении свойств и показателей случайной подстановки. Можно считать, что 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 смещений таблиц линейных корпусов будет только повышаться. Тем не менее, находится немало скептиков, которые полагают, что то, что свойственно малым моделям шифров, совсем не обязательно присуще их большим прототипам.

В этой работе мы поставили задачу убедить сомневающихся, в том, что и большие шифры являются случайными подстановками. В дальнейшем речь будет идти только о дифференциальных показателях шифров, хотя соответствующие оценки можно получить и для линейных характеристик.

1. Стратегия анализа показателей случайности больших шифров

Очевидно, что построение закона распределения переходов таблицы полных дифференциалов для большого шифра является вычислительно нереализуемой задачей.

В этих условиях стратегия решения задач оценки показателей случайности больших шифров может быть только одна – суметь найти подтверждение желаемого результата на основе использования выборки ограниченного (приемлемого) объема. Изучить подходы к продвижению вперед в этом направлении и станет нашей ближайшей целью.

Вся таблица XOR разностей (ее A_π-я часть [3, 4]) для шифра с n-битным входом содержит $2^{n-1}\times 2^{n-1}$ ячеек, которые заполнены соответствующими значениями переходов входны

разностей ΔX в выходные разности ΔY. Для полного набора пар входов (пар открытых текстов) с заданной разностью ΔX, которая может принимать значения от 0 до 2^{n-1}, выходные значения – разности зашифрованных текстов ΔY для случайной подстановки при накоплении результатов счета могут принимать значения от 0 до $k^* \le n + 4$) [3].

Заметим, что максимальное значение для каждой ячейки таблицы свое и может быть получено из полностью построенной таблицы разностей (при выполнении полного набора $2^n - 1 \times 2^n - 1$ экспериментов по вычислению отдельных переходов).

Если считать, события, состоящие в выборе пар со случайными значениями входов в таблицу $(\Delta X, \Delta Y)$, независимыми и равновероятными, можно убедиться, что для случайной подстановки порядка 2^n уже при $n = 64$ (например, если в качестве случайной подстановки рассматривать шифр ГОСТ 28147-89) уменьшение выборки до поддающегося вычислениям объема, равного $\sqrt{2^n} = \sqrt{2^{64}} = 2^{32}$, не позволяет получить какое либо нетривиальное значение перехода, превышающее единицу. Тем более, не осуществим анализ такого типа для шифров с большим битовым размером входа.

Таким образом, рассмотренная стратегия, ориентированная на построение выборки из случайного набора дифференциальных переходов для больших шифров, не перспективна.

Существует, однако, еще одна возможность формирования случайной выборки из дифференциальных переходов большого шифра. Можно анализировать значения переходов разностей не для всей дифференциальной таблицы шифра, а только для ее "пропорционально уменьшенной" части. Предполагается рассматривать, например, дифференциальную таблицу, получающуюся при использовании шифра для шифрования не n-битных блоков данных, а блоков, уменьшенных по размеру в 2 – 4 раза.

Большой шифр используется по типу малого для шифрования блоков данных уменьшенной длины (зашифрованные блоки данных тоже усекаются до необходимого размера), при этом сохраняются все преобразования и внутренние связи большого шифра. Примечательно при таком подходе то, что появляется возможность применить весь наработанный аппарат изучения показателей случайности малых версий шифров для изучения показателей случайности больших шифров.

Предлагаемый подход позволяет получить, по крайней мере, два полезных результата.

В первом случае можно использовать 16-битные блоки открытых и соответствующих им зашифрованных текстов. Здесь мы приходим к условиям, в которых исследовались малые модели шифров [7 – 9 и др.]. Вычислительных ресурсов здесь хватает для построения всей дифференциальной таблицы (большой шифр работает, как его уменьшенная 16-битная версия).

Очевидно, что при рассматриваемом подходе можно построить и строку смещений таблицы линейных аппроксимаций. Этого мало, но уже можно проверить совпадение теоретического и экспериментального законов распределения вероятностей переходов в строке (или нескольких строках) шифра и случайной подстановки соответствующей степени.

Во втором случае можно строить строки дифференциальной таблицы при использовании большого шифра для шифрования 32-битных блоков данных. Для таблиц линейных аппроксимаций удастся вычислить отдельные значения ячеек. Здесь открываются, на наш взгляд, перспективы для решения исследовательских задач и поиска ответов на вопрос, можно ли считать большие шифры случайными подстановками.

Дальнейший материал посвящен изложению результатов применения этой методики для исследования дифференциальных и линейных свойств шифров Rijndael (AES) и ГОСТ 28147.

2. Анализ показателей случайности больших шифров

Первый эксперимент был выполнен с использованием шифра Rijndael в режиме шифрования 16-битных блоков данных. Результаты этого эксперимента иллюстрирует табл.1.

Таблица 1

Поцикловые значения максимумов полных дифференциалов при шифровании 16-битными блоками

Число циклов r	Значение максимума полного дифференциала	Среднеквадратическое отклонение
1	65536	0
2	3652,26	±630,312
3	19,0666	± 1,436
4	19,0666	±0,99777
5	18,8666	±1.23108
6	19,1332	±0,99106
7	19,2666	± 1,0934
8	19,1332	± 1,431394
9	19,0666	± 1,23648
10	19,3333	± 1,2995
11	19.4	± 1,474222
12	18,8666	± 0,991072
13	18,8666	± 0,991072
14	18.9332	± 1,123486

В процессе экспериментов осуществлялось зашифрование 16-битных блоков данных на 30 случайно выбранных ключах. Полученные результаты были усреднены по этому множеству ключей.

Из представленных результатов видно, что большой шифр Rijndael уже с третьего цикла шифрования приходит к установившемуся значению максимума полного дифференциала, повторяющему соответствующее значение (равное 19), свойственное случайной подстановке степени 2^{16} [4]. Видно, что это асимптотическое значение практически не зависит от используемых ключей зашифрования (среднеквадратическое отклонение не превышает 1,5). Отметим, что для уменьшенной до 16-битного входа модели шифра Rijndael асимптотическое значение (19) наступает после трех-четырех циклов (в зависимости от конструкции линейного преобразования).

В табл. 2 представлены результаты аналогичных экспериментов, выполненных с шифром ГОСТ.

Видно, что и в этом случае шифр становится случайной подстановкой, но теперь для этого ему необходимо девять циклов зашифрования. Обратим внимание, что девять циклов для большого шифра ГОСТ – эта для него глубина лавинного эффекта, – уже давно установленный параметр [10], свидетельствующий о наступлении момента, с которого изменение каждого бита входа начинает влиять на все выходные биты (при изменении любого бита входа начинает изменяться в среднем половина битов выходного текста). Заметим, что этот эффект выявлен и в уменьшенной модели этого шифра [11], что свидетельствует о том, что уменьшенная модель шифра повторяет свойства прототипа.

Следующим экспериментом стало вычисление закона распределения переходов для отдельной строки дифференциальной таблицы для 32-битного варианта использования рассматриваемых шифров. В табл. 3 приведен закон распределения вероятностей переходов строки дифференциальной таблицы для шифра ГОСТ с полным числом циклов (32). В этой таблице в левой колонке приведены результаты экспериментов, а в правой – результаты, полученные для случайной подстановки степени 2^{32} расчетным путем. Видно и без привлечения методов оценки близости распределений хорошее совпадение результатов.

В табл. 4 представлены аналогичные результаты для шифра Rijndael (при 14-цикловом шифровании). И в этом случае можно констатировать, что шифр Rijndael действительно можно считать случайной подстановкой.

В табл. 5 приводятся модульные значения максимальных смещений для шифра ГОСТ вместе со среднеквадратическими отклонениями.

Аналогичные результаты для шифра Rijndael иллюстрирует табл. 6.

Интересно отметить, что закон распределения переходов для строки случайной подстановки степени 2^n (в нашем случае 2^{32}) полностью повторяет закон распределения всей дифференциальной таблицы подстановки степени 2^{n-1} (в нашем случае 2^{16}).

Видно, что и 128-битный Rijndael тоже хорошо повторяет свойства случайных подстановок. В табл. 5, 6 представлены результаты экспериментов с определением линейных свойств наших шифров.

Таблица 2

Поцикловые значения максимумов полных дифференциалов при шифровании 16-битными блоками

Число циклов r	Значение максимума полного дифференциала	Среднеквадратическое отклонение
1	65536	0
2	65536	± 12,934
3	61952	± 1278,614
4	56008.6	± 5181,74
5	31358	± 857,546
6	2046,7	± 637,692
7	973,4	± 29,7630
8	52,2	± 6,80882
9	19,1	± 0,97978
10	19,5	± 2,32664
11	18,7	± 0,86602
12	18,9	± 0,99498
13	19,1	± 1,16618
14	19,4	± 0.97978
15	19,4	±1,337908
16	19,3	±0,979796
17	19,3	±1,07338
18	19,4	±0,994988
19	19,4	±0,95394
20	19,9	±1,193216
21	19,9	±1,176190
22	19,10	±0,95394
23	18,90	±1,083216
24	19,30	±1,044552
25	18,6	±0,979796
26	19,2	±1,307670
27	19,0	±1,179982
28	19,9	±0,979796
29	19,6	±1,729162
30	19,1	±1,176190
31	19,3	±1,356466
32	19,1	±1,144552

Таблица 3

Закон распределения переходов в строке таблицы дифференциальных разностей шифра ГОСТ в режиме шифрования 32-битных блоков данных

Значение перехода $2k$	Количество переходов (эксперимент)	Количество переходов (расчет)
0	2604902589	$2{,}6049\times10^{9}$
2	1302505752	$1{,}30245\times10^{9}$
4	325630272	$3{,}25612\times10^{8}$
6	54278054	$5{,}42687\times10^{7}$
8	6779658	6.78359×10^{6}
10	679466	678359
12	56094	56529.9
14	4077	4037,85
16	253	252,366
18	10	14,0203
20	1	0,701016

Таблица 4

Закон распределения переходов в строке таблицы дифференциальных разностей шифра Rijndael в режиме шифрования 32-битных блоков данных

Значение перехода $2k$	Количество переходов (эксперимент)	Количество переходов (расчет)
0	2605041617	$2{,}6049\times10^{9}$
2	1302473402	$1{,}30245\times10^{9}$
4	325669098	$3{,}25612\times10^{8}$
6	54262758	$5{,}42687\times10^{7}$
8	6783634	6.78359×10^{6}
10	676065	678359
12	56376	56529,9
14	4089	4037.85
16	232	252.366
18	16	14,0203
20	0	0,701016

Таблица 5

Поцикловые значения максимумов смещений линейных корпусов при шифровании 16-битными блоками для шифра ГОСТ 28147

Число Циклов r	Значение максимума смещения линейного корпуса	Среднеквадратическое отклонение
1	0	0
2	32768	0
3	17162	± 1425,35
4	31181,7	± 2676,77
5	16150,1	± 1228,27
6	16669,5	± 3530,38
7	2144,77	± 374,142
8	2380,93	± 632,23
9	826,833	± 21,1157
10	828,1	± 22,4148
11	823,767	± 18,9573
12	821,433	± 28,5723
13	826,067	± 18,3556
14	830,567	± 27,4817
15	818,833	± 23,3539
16	823,767	± 23,8868
17	821,7	± 20,2075
18	823,933	± 21,9286
19	819,3	± 22,3967
20	816,467	± 17,5798
21	815,567	± 19,0817
22	817,967	± 20,9467
23	820,067	± 22,2844
24	822,067	± 16,7729
25	823,333	± 21,9109
26	817,833	± 17,6467
27	823,967	± 27,0549
28	820,9	± 24,6405
29	824,467	± 25,6239
30	840,067	± 35,3553
31	823,333	± 17,8612
32	820,733	± 18,6582

Таблица 6

Поцикловые значения максимумов смещений линейных корпусов при шифровании 16-битными блоками для шифра Rijndael

Число Циклов r	Значение максимума смещения линейного корпуса	Среднеквадратическое отклонение
1	0	0
2	9284.27	± 657.454
3	818.467	± 26.8809
4	815	± 28.204
5	818.5	± 18.536
6	815.967	± 20.18
7	832.1	± 33.1887
8	823.133	± 23.5722
9	829.9	± 33.5741
10	827.4	± 25.2885
11	815.6	± 22.3138
12	819	± 27.0025
13	824.9	± 23.7716
14	821.2	± 22.653

Заключение

Представленные результаты свидетельствуют о том, что шифры Rijndael и ГОСТ28147-89 по своим дифференциальным и линейным показателям полностью укладываются в рамки случайных подстановок. Экспериментальные результаты хорошо согласуются с теоретическими, т.е. полностью подтверждается гипотеза о том, что большие шифры, как и малые их версии, после определенного числа циклов шифрования приобретают свойства случайных подстановок соответствующей степени.

Общий вывод, который напрашивается из представленных материалов, состоит в том, что не только Rijndael и ГОСТ, но и все другие известные итеративные шифры на полной цикловой длине обладают свойствами случайных подстановок. Мы тем самым подтвердили в известной степени общепринятую и естественную точку зрения о том, что всякий хороший шифр должен быть случайной подстановкой.

Список литературы: 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. *Долгов В.И.* Подход к криптоанализу современных шифров /Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй междунар. конф. "Современные информационные системы. Проблемы и тенденции развития". – Харьков-Туапсе, Украина, 2–5 октября, 2007. – С. 435-436. 3. *Олейнико*

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. 4. *L. J. O'Connor.* On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, pages 360–370, 1994. 5. *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. 6. *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). 7. *Лисицкая И.В.* Криптографические свойства уменьшенной версии шифра "Мухомор" / Лисицкая И.В., Олешко О.И., Руденко С. Н, Дроботько Е. В., Григорьев А. В. // Спеціальні телекомунікаційні системи та захист інформації : Зб. наук. праць. – Київ, 2010. – С. 31-42. 8. *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. – 2009. – Т.8. №3 – С. 283-289. 9. *Долгов В.И.* Криптографичекие 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. 10. *Б. Шнаер.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : ТРИУМФ, 2002. – 816 с. 11. *Лисицкая И.В.* Исследование криптографических показателей уменьшенных моделей шифров ГОСТ и DES / Лисицкая И.В., Макарчук Я.В. // Прикладная радиоэлектроника. – 2011. – (в печати).

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.08.2011