УДК 621. 391:519.2:519.7

ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА ШИФРА FOX

И.В. ЛИСИЦКАЯ, Д.С. КАЙДАЛОВ

Изучаются свойства законов распределения XOR таблиц (таблиц полных дифференциалов) уменьшенной и больших версий современного шифра FOX. Демонстрируется, что и большие версии шифра при ограничении длины шифруемого блока асимптотически (после нескольких начальных циклов) ведут себя как случайные подстановки.

Ключевые слова: уменьшенная версия шифра, случайная подстановка, XOR таблица подстановки, закон распределения вероятностей однотипных переходов таблицы XOR разностей, полный дифференциал.

ВВЕДЕНИЕ

При анализе современных блочных шифров одним из основных критериев их пригодности для применения являются показатели стойкости к известным методам криптоанализа. Однако выполнить всесторонний криптоанализ и проверку надежности шифра – это довольно не простая задача. Ее решение требует больших временных и интеллектуальных ресурсов, а для некоторых видов криптоанализа, и, в частности, для дифференциального и линейного, решить такую задачу практически невозможно.

В широком спектре стоящих задач большое значение приобретает развитие и применение технологий, позволяющих ускорить процессы исследования и принятия решений. Одним из таких путей, направленных на создание и отработку эффективных методов сопоставления различных предложений, может стать анализ криптографических показателей уменьшенных моделей шифров, в которых сохранены все принципиальные преобразования основного (большого) шифра [1]. Естественно, здесь сразу возникает вопрос об адекватности перехода от больших версий к малым (в смысле сохранения в модели всех свойств прототипа). Однако здесь можно положиться на достаточно очевидный принцип (назовем его постулатом): если хороши свойства модели, то свойства прототипа как минимум будут не хуже. Когда прототип поддается масштабируемости, то есть удается в модели сохранить структуру преобразований блоков данных и свойства основных операций, то результаты анализа свойств модели могут быть перенесены на прототип. Несмотря на простоту и внешнюю очевидность изложенного принципа остается все же еще очень много скептиков, требующих более весомых аргументов в пользу адекватности перехода от больших версий к малым и наоборот.

В этой работе мы ставим задачу получить дополнительные более веские аргументы в пользу правомерности наших утверждений. Объектом исследований является один из современных блочных симметричных шифров FOX [2]. Мы приведем здесь сравнение дифференциальных свойств уменьшенной 16-битной и большой 64-битной версий.

1. ОПИСАНИЕ УМЕНЬШЕННОЙ ВЕРСИИ ШИФРА FOX

Уменьшенная версия построена на основе версии шифра FOX с 64-битным входным блоком. В уменьшенной версии длина блока, как и длина ключа равна 16 битам.

Данный шифр основан на схеме Лей-Месси [3,4]. Ее реализация (Imor16) представлена на рис. 1. Сам шифр представляет собой r–1-разовое повторение функции Imor16. После её выполнения (в последнем цикле) вызывается слегка изменённая функция Imid16 (отсутствует функция *or*).

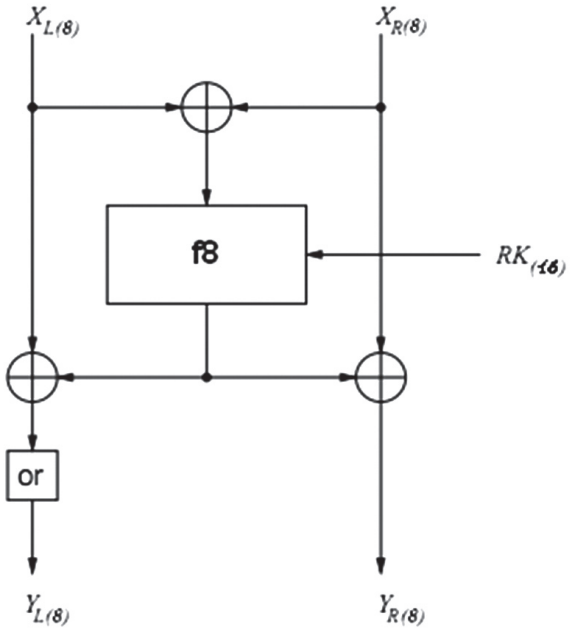

Рис. 1. Функция Imor16

Количество циклов, в зависимости от настроек, может быть любым (в большом шифре используется 16 циклов зашифровывания). В качестве схемы разворачивания ключей в нашем случае используется стандартная схема 64 битного алгоритма, которая генерирует раундовые ключи длиной по 64 бита, однако от каждого такого ключа в уменьшенной версии шифра используются только первые 16 бит.

Схема цикловой 8-битной функции f_8 представлена на рис. 2. Раундовый ключ длиной 16 бит разделяется на 2 части по 8 бит (rk_0 и rk_1) и после

сложения по mod2 с соответствующими половинками входного 16-битного блока данных поступает на входы двух полубайтовых S-блоков. S-блоки для всех частей входных данных одинаковые.

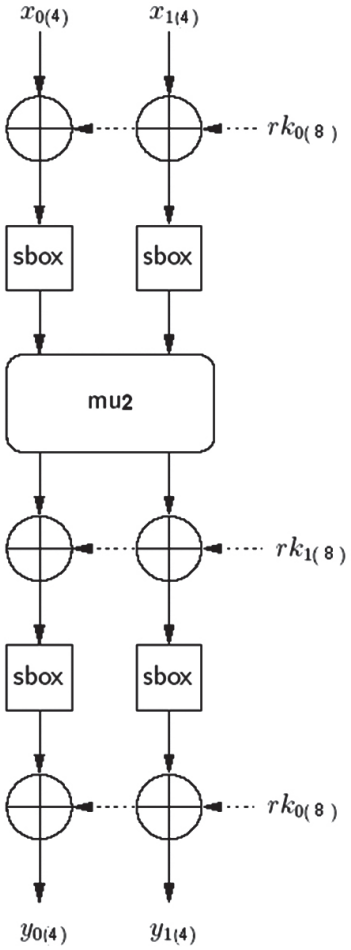

Рис. 2. Цикловая функция уменьшенной версии шифра FOX

В шифре FOX использована S-блоковая функция авторской разработки. Она является нелинейным биективным отображением 8-ми битных входных значений в 8-ми битные выходные и строится с помощью схемы Лэя-Мэсси с тремя циклами и тремя разными «малыми» (размером 4×4) подстановками.

В нашем случае были взяты сразу полубайтовые S-блоки (SboxAES [5]):

Таблица 1

S-блок, используемый в шифре

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
A	4	3	B	8	E	2	C	5	7	6	F	0	1	9	D

В качестве преобразования mu2, как и в оригинальной разработке, используется умножение на матрицу следующего вида:

$$\begin{pmatrix} y_0(4) \\ y_1(4) \end{pmatrix} = \begin{pmatrix} x_0(4) \\ x_1(4) \end{pmatrix} \begin{pmatrix} \alpha - 1 & \alpha \\ \alpha & \alpha - 1 \end{pmatrix}.$$

Входные векторы $x_0(4)$ и $x_1(4)$ представляются в виде полиномов над расширенным двоичным полем $GF(2^4)$. Умножение полиномов происходит по модулю $f(\alpha) = \alpha^4 + \alpha + 1$.

В качестве преобразования *or* используется цепь Фейстеля. Схема приведена на рис. 3.

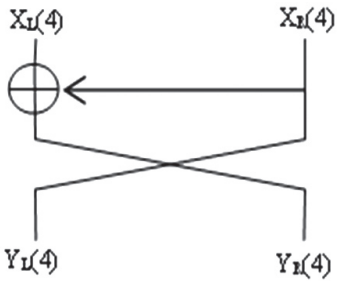

Рис. 3. Функция *or*2

2. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

С помощью разработанной программной реализации уменьшенной версии шифра FOX подсчитаны максимальные значения таблиц XOR разностей (полных дифференциалов) для различного числа циклов зашифрования (для случайно выбранного ключа зашифрования). Полученные результаты иллюстрирует табл. 2.

Таблица 2

Максимальные значения таблиц XOR разностей для различного количества циклов уменьшенной версии шифра FOX

Количество циклов	Максимум ДХ	Количество ДХ с максимальным значением
1	65536	255
2	3584	1
3	2048	1
4	82	1
5	24	1
6	20	1
7	18	12
8	20	1
9	18	15
10	18	18
11	20	2
12	20	2
13	18	11
14	20	2
15	18	14
16	20	1

Как видно из представленных результатов, уменьшенная версия шифра FOX повторяет свойства рассмотренных ранее уменьшенных моделей других SPN шифров (baby-Rijndael-я, Калины, ADE и др. [6-9]). Уже после шести циклов шифр становится случайной подстановкой (приходит к асимптотическому значению максимума полного дифференциала, характерному для случайной подстановки).

Мы повторили далее эксперимент, только теперь уже для 64-битной (большой) версии шифра FOX. Мы решили проверить, повторяет ли большой шифр свойства своей уменьшенной модели. Конеч-

но, для длины блока 64 бита таблица полных дифференциалов содержит 2128-мой ячеек. Подсчитать в этом случае всю дифференциальную таблицу с использованием существующих вычислительных мощностей не представляется возможным. Поэтому было принято решение сымитировать с помощью большого шифра его малую версию: расчет выполнялся для множества из первых 216 входных разностей (рассматривались 16-битные входные разности). Выходные разности также определялись для первых 16 бит соответствующих шифртекстов. В результате, дифференциальная таблица при таком подходе содержит 232 ячеек, как и при уменьшенной версии шифра.

Результаты этого вычислительного эксперимента иллюстрирует табл. 3, в которой снова приведены максимальные значения полных дифференциалов в зависимости от числа циклов, но теперь уже для 64-битной версии шифра.

Как видно из таблиц 2, 3 уменьшенная версия достигает минимальных значений дифференциальных характеристик на 6 цикле преобразования. В то же время как для полной версии шифра требуется максимум 2 цикла, чтобы достичь таких же показателей. В целом же, при количестве циклов 6 и более уменьшенная версия имеет такие же дифференциальные свойства, как и большой шифр с усечением зашифрованных блоков.

В третьей серии экспериментов мы убедились, что результаты, зафиксированные в табл. 2, практически повторяются при любом входном 16-битном (усеченном) блоке и при использовании в качестве результата зашифрования любого 16-битного сегмента выходного зашифрованного блока. Соответствующие результаты отражены в таблицах 4 и 5, в которых приводятся результаты оценки максимальных значений полных дифференциалов для 64-битной версии шифра FOX и его 128-битной версии (с усечением зашифрованных блоков до 16-битного размера).

Сравнивая результаты табл. 4 и 5, можно прийти к выводу о том, что и большой шифр FOX демонстрирует (подтверждает) нашу позицию в том, что большие шифры ведут себя как случайные подстановки (имеют законы распределения переходов XOR таблиц (и мы уверены, что и таблиц линейных аппроксимаций) свойственные случайным подстановкам соответствующей степени).

Таблица 3

Максимальные значения таблиц дифференциальных разностей для различного количества раундов для 64-битной версии шифра

Количество циклов	Максимум ДХ	Количество ДХ с максимальным значением
1	60	1
2	18	8
3	20	1
4	18	17
5	18	13
6	20	2
7	18	14
8	18	13
9	20	1
10	20	1
11	20	2
12	18	10
13	22	1
14	18	6
15	18	13
16	18	13

Наконец, в последней серии экспериментов, мы построили закон распределения переходов отдельной строки дифференциальной таблицы полного 64-битного шифра, рассматриваемого

Таблица 4

Максимальные значения полных дифференциалов для 64-битной версии шифра FOX (для подсчета входных и выходных разностей во внимание берутся отдельные 16 бит блоков данных)

Количество циклов	Биты 0..15 шифртекстов		Биты 16..31 шифртекстов		Биты 32..47 шифртекстов		Биты 48..63 шифртекстов	
	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов
1	60	1	36	1	60	1	36	1
2	18	8	20	1	20	2	20	1
3	20	1	20	2	18	19	18	9
4	18	17	18	6	18	12	18	10
5	18	13	20	4	20	2	18	17
6	20	2	20	1	20	1	20	2
7	18	14	18	11	18	10	18	13
8	18	13	20	1	20	1	18	9
9	20	1	18	14	18	15	18	9
10	20	1	18	30	20	1	18	18
11	20	2	20	2	20	1	20	1
12	18	10	20	1	20	1	20	1
13	22	1	22	1	20	1	18	19
14	18	6	18	15	20	2	20	2
15	18	13	20	1	18	14	20	2
16	18	13	18	15	18	19	20	1

Таблица 5

Максимальные значения полных дифференциалов для 128-битной версии шифра FOX (для подсчета разностей во внимание берутся отдельные 16 бит блоков данных)

Количество циклов	Биты 64..79 шифртекстов		Биты 80..95 шифртекстов		Биты 96..111 шифртекстов		Биты 112..127 шифртекстов	
	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов
1	32	1	38	1	32	1	38	1
2	18	10	20	1	20	1	18	11
3	18	14	22	1	20	1	18	10
4	18	10	22	1	18	20	22	1
5	18	10	18	19	20	1	18	16
6	18	15	18	14	18	13	18	15
7	20	1	20	1	20	1	20	2
8	20	1	18	18	20	1	18	17
9	18	13	20	1	18	20	20	2
10	18	12	18	17	20	3	20	1
11	20	1	20	1	20	1	20	1
12	20	1	18	13	20	2	18	11
13	20	1	18	13	20	1	18	17
14	18	12	18	11	18	17	18	9
15	18	11	20	1	20	1	18	19
16	18	16	20	1	20	1	18	15

как шифра с 32-х битными входами. В этом случае для подсчета входных разностей рассматривались 32 первых бита 64-х битных входных блоков данных, а на выходе использовались первые 32 бита шифртекстов для подсчета выходных разностей. Результаты этого эксперимента иллюстрирует табл. 6. И в этом полученные результаты дают все основания считать, что шифр и в рассмотренном примере демонстрирует интересующие нас свойства. Буквально начиная со второго цикла он приходит к асимптотическому значению максимума полного дифференциала, свойственного случайной подстановке соответствующего порядка.

Мы также построили закон распределения числа переходов отдельной строки дифференциальной таблицы, рассматривая большой шифр в режиме зашифрования 32-битных блоков данных. Результаты этого эксперимента представлены в табл. 7 (левая колонка).

Если вспомнить полученное в работе [10] соотношение для определения числа переходов таблицы XOR разностей случайной подстановки, то по аналогии с выводом этого соотношения для числа ячеек строки отдельной таблицы XOR разностей случайной подстановки степени 2^n можно получить расчетное соотношение:

$$\Lambda_{n,2k}^{(c)} = (2^n - 1) \times \frac{e^{-1/2}}{2^k\, k!}.$$

Расчеты, выполненные с использованием этого соотношения, также приведены в табл. 7. Сопоставление данных вычислительного эксперимента с результатами, полученными расчётным путем, очень убедительно свидетельствует о том, что блочный симметричный шифр FOX с большой точностью повторяет свойства случайной подстановки, в чем мы и хотели убедиться.

Таблица 6

Максимальные значения полных дифференциалов отдельной строки для 64-битной версии шифра FOX (для подсчета разностей берутся первые 32 бита входов и первые 32 бита выходов)

Количество циклов	Максимум ДХ	Количество ДХ с максимальным значением
1	248	2476
2	18	12
3	18	17
4	20	1
5	20	3
6	18	8
7	20	1
8	18	11
9	18	12
10	18	8
11	20	1
12	18	11
13	20	1
14	20	3
15	18	12
16	18	11

Таблица 7

Распределение переходов для одной строки XOR таблицы 64-битной версии шифра FOX для 14 циклов при 32-х битном шифровании

Значение перехода 2k	Количество переходов (эксперимент)	Количество переходов (расчет)
0	2605029873	$2{,}6049 \cdot 10^9$
2	1302512713	$1{,}30245 \cdot 10^9$
4	325628210	$3{,}25612 \cdot 10^8$
6	54276635	$5{,}42687 \cdot 10^7$
8	6780336	$6{,}78359 \cdot 10^6$
10	678395	678359
12	56881	56529,9
14	4030	4037,85
16	212	252,366
18	11	14,0203
20	0	0,701016

ЗАКЛЮЧЕНИЕ

Результатами работы подтверждено, что большие шифры повторяют свойства своих уменьшенных версий, и, в частности, имеют законы распределения переходов XOR таблиц (а мы уверены и таблиц линейных аппроксимаций) свойственные случайным подстановкам соответствующей степени. Тем самым подтверждаются тезисы и утверждения, пропагандируемые в работах [6,7].

Литература

[1] *Долгов В.И.* Подход к криптоанализу современных шифров. / Долгов В.И., Лисицкая И.В. // II-я международная конференция “Современные информационные системы. Проблемы и тенденции развития”, Сборник материалов конференции, Харьков, ХНУРЭ, 2007.

[2] *Pascal Junod.* FOX: a New Family of Block Ciphers. / Pascal Junod and Serge Vaudenay.// Selected Areas in Cryptography 2004: Waterloo, Canada, August 9-10, 2004. Revised papers, Lecture Notes in Computer Science. Springer-Verlag. pp. 1-16.

[3] *X. Lai.* On the design and security of block ciphers, volume 1 of ETH Series in Information Processing. Hartung-Gorre Verlag, 1992.

[4] *X. Lai.* A proposal for a new block encryption standard. / X. Lai and J. Massey. // In I. Damgard, editor, Advances in Cryptology – EUROCRYPT’90, volume 473 of Lecture Notes in Computer Science, pages 389–404. Springer-Verlag, 1991.

[5] *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.

[6] *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.

[7] *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.

[8] *Долгов В.И.* Криптографические свойства уменьшенной версии шифра “Калина” / Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев А.В., Дроботько Е.В. // Прикладная радиоэлектроника, 2010. – Т. 9. – № 3. – С. 349-354.

[9] *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.

[10] *Олейников Р.В.* Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е. // Прикладная радиоэлектроника. – 2010. Т. 9. – № 3. – С. 326-333.

Поступила в редколлегию 12.04.2011

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

Кайдалов Дмитрий Сергеевич, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: анализ стойкости блочных симметричных шифров.

УДК 621. 391:519.2:519.7

Диференціальні властивості шифру FOX / І.В. Лисицька, Д.С.Кайдалов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 122–126.

Вивчаються властивості законів розподілу XOR таблиць (таблиць повних диференціалів) зменшених та великих версій сучасного шифру FOX. Демонструється, що і великі версії шифру при обмеженні довжини шифруємого блоку асимптотично (після декількох початкових циклів) ведуть себе як випадкові підстановки.

Ключові слова: зменшена версія шифру, випадкова підстановка, XOR таблиця підстановки, закон розподілу ймовірностей однотипних переходів таблиці XOR різниць, повний диференціал.

Табл. 7. Іл. ..3. Бібліогр.: 10 найм.

UDC 621. 391:519.2:519.7

Differential properties of cipher FOX / I.V. Lisitskaya, D.C. Kaydalov / / Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 122–126.

The paper studies the properties of laws of distributing XOR tables for modern cipher FOX. It is shown that this cipher has properties like random substitutions.

Keywords: small version of a cipher, random permutation, XOR substitution table, law of probability distribution of similar transitions of XOR table of differences, total differential.

Tab. 7. Fig. 3. Ref.: 10 items.