УДК 681.3.06

ИССЛЕДОВАНИЕ ЦИКЛИЧЕСКИХ И ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «ЛАБИРИНТ»

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, А.В. ГРИГОРЬЕВ, А.В. ШИРОКОВ

В работе описывается уменьшенная модель шифра «Лабиринт» – одного из претендентов на новый стандарт БСШ Украины, и приводятся результаты сравнительного анализа ее криптографических показателей с показателями других ранее рассмотренных моделей (циклические и дифференциальные свойства).

The paper describes a diminished model of the cipher «Labyrinth» – one of the claimants to the All-Ukrainian national standard of block symmetric ciphering and the comparative analysis results of its cryptographic factors with the factors of other previously considered models (cyclic and differential properties) are provided.

ВВЕДЕНИЕ

В эти дни в Украине проходит конкурс предложений по построению алгоритмов блочного симметричного шифрования, целью которого является отбор претендента на новый стандарт БСШ, взамен используемого до настоящего времени российского шифра ГОСТ 28149-87. Известно, по крайней мере, четыре предложения и сейчас идет их изучение заинтересованными организациями и специалистами.

Опыт показывает, что выполнение экспертизы современного блочного шифра является не простой задачей, требующей привлечения значительных временных и интеллектуальных ресурсов. Хотелось бы найти не только убедительные теоретические обоснования, выполнить которые в криптографии, как правило, очень непросто, но и получить реальные практические результаты для сравнительного анализа претендентов. Но и здесь многие подходы сталкиваются практически во всех случаях с проблемой непреодолимой вычислительной сложности анализа современных БСШ.

Мы развиваем точку зрения, что в определенной мере можно преодолеть стоящие трудности путем анализа криптографических свойств уменьшенных моделей кандидатов, которые уже поддаются проведению вычислительных экспериментов. Конечно, при этом необходимо позаботиться, чтобы в уменьшенных моделях были сохранены все основные преобразования и операции прототипов, т.е. чтобы обеспечивалась в известном смысле их «эквивалентность». В представленных ранее наших работах [1-3] уже обсуждались свойства уменьшенных моделей ряда современных шифров, в том числе и шифров, представленных на Украинский конкурс. Мы здесь продолжаем эту работу. В первой ее части предлагается модель уменьшенной версии шифра «Лабиринт» – еще одного из претендентов на новый стандарт БСШ Украины, а во второй приводятся результаты сравнительного анализа ее криптографических показателей с показателями других ранее рассмотренных моделей (циклические и дифференциальные свойства).

1. ПРЕОБРАЗОВАНИЯ ЗАШИФРОВАНИЯ И РАСШИФРОВАНИЯ ШИФРА МИНИ-«ЛАБИРИНТ»

Уменьшенный алгоритм производит шифрование блоками данных по 16 бит каждый. Размер ключа также составляет 16 бит.

Приведем здесь описание структуры преобразований уменьшенной модели шифра «Лабиринт», практически повторяющей структуру преобразований оригинального предложения [4].

Напомним, что «Лабиринт» является «инволютивным» шифром. Это значит, что зашифрование и расшифрование выполняются на основе одной общей процедуры, отличающейся только противоположной последовательностью применения цикловых ключей, а также ключей начального и конечного преобразований (подключей начального и конечного преобразований).

Преобразования зашифрования и расшифрования состоят из двух фаз:

а) сначала выполняется процедура разворачивания ключа – на основе исходного ключа выполняется формирование подключей рабочего ключа. Порядок применения подключей определяется выбранным «направлением» преобразования: зашифрование или расшифрование;

б) выполняется процедура шифрования/расшифрования – преобразование входного блока данных (P либо C) на рабочем ключе.

1.1. Процедура зашифрования

Алгоритм «Лабиринт» построен по итеративной схеме, т.е. его основу составляет цикловое преобразование, которое повторяется заданное число раз (число циклов шифрования автором обозначено символом r). Каждый цикл состоит из двух абсолютно идентичных итераций, осуществляющих преобразование (зашифрование) двух полублоков, на которые разбивается блок данных на входе каждого цикла. Учитывая, однако, что для обновления обоих полублоков, составляющих один блок, в предлагаемом решении требуется, как минимум, две итерации, автор в своем описании алгоритма отделил понятие цикла от понятия итерации (у него цикл состоит из двух итераций).

Кроме повторяющегося циклового преобразования процедура зашифрования включает также начальное (IT) и конечное (FT) преобразования. Свойство инволютивности шифра достигается за счёт применения классической конструкции полублоковой цепи Фейстеля.

Все эти решения естественно сохранены в уменьшенной модели алгоритма «Лабиринт». Фейстель подобную структуру процедуры зашифрования с учетом уменьшенного размера входного блока данных иллюстрирует рис.1. Число циклов в нашей уменьшенной версии может меняться от 4 до 16. Далее будет представлено описание 4-х цикловой модели ($r = 4$).

Процедура зашифрования EF состоит из трёх этапов:

– Исходный блок данных P<16> (длиной 16 бит, что подчеркивается приставкой <16> к символу исходного блока данных P) обрабатывается начальным (IT) преобразованием на ключе K^{IT} (здесь и далее мы по возможности будем сохранять символику и обозначения, использованные автором в оригинальной разработке).

– Результат 1-го этапа разбивается на два полублока длиной по 8 бит каждый: левый $L^{(0)}_{<8>}$ («старший») и правый $R^{(0)}_{<8>}$ («младший»). Полученная пара полублоков преобразуется на 8 итерациях (4 циклах) цепи Фейстеля. Все итерации полностью идентичны и построены на базе общего нелинейного преобразования – F-функции, управляемой ключами итерации $K^{(i)}$, $i = 1, , \ldots, 2r$;

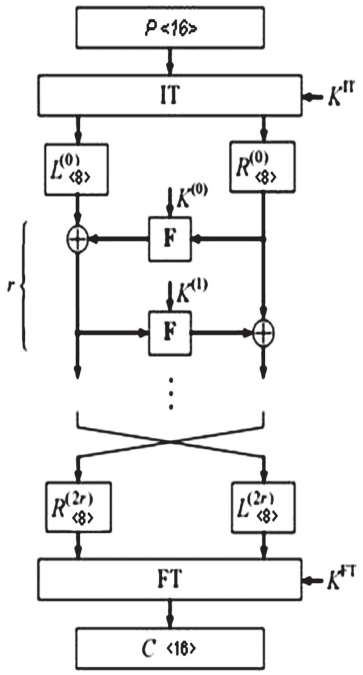

Рис. 1. Структура процедуры шифрования

– На третьем этапе два полублока $L^{(2r)}_{<8>}$ и $R^{(2r)}_{<8>}$, полученные в результате 4-х циклового итеративного преобразования, меняются местами и обрабатываются конечным (FT) преобразованием на ключе K^{FT}. Полученный после FT преобразования двоичный вектор C<16> (длиной 16 бит) является зашифрованным блоком («криптограммой»).

На каждой итерации F-функция использует 8-битный подключ $K^{(i)}$. Длина ключей начального (K^{IT}) и конечного (K^{FT}) преобразований составляет по 16 бит каждый.

1.2. Базовая функция зашифрования

Конструкция F-функции алгоритма «Лабиринт» построена, как отмечает автор, в соответствии с принципами, позволяющими обеспечить свойства рассеивания и размножения активизации[1] (автор ссылается здесь на работу [5]). В большом шифре она состоит из четырёх элементарных преобразований:

• сложение полублока (последовательности байтов) входного блока данных с байтами (в терминах автора – словами) циклового ключа по модулю 2^{64};

• фиксированная байтовая перестановка P;

• фиксированная нелинейная подстановка байтов, составляющих блок;

• фиксированное преобразование линейного смешивания.

Последние два пункта объединены в SL_0-преобразование.

В уменьшенной модели мы повторили конструкцию F-функции большого шифра, только теперь операции выполняются не над байтами, а над двумя полубайтами (над одним байтом), а сложение полубайтов (двух) циклового ключа с полублоками из полубайтов (байтом) входного блока данных выполняется теперь уже по модулю 2^8. Кроме того, фиксированная перестановка P (как и в большом шифре для значения длительности блока данных 128 бит) в уменьшенной версии шифра не применяется. В итоге, F-функция, использующая в процессе преобразований подключ из 8 бит, может быть представлена схемой рис. 2, повторяющей структуру F-функции большого шифра.

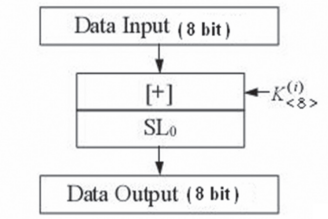

Рис. 2. 8-битная F-функция

Конструкция SL_0-преобразования будет рассмотрена далее отдельно.

[1] *Числом ветвей активизации* линейного преобразования называется минимальное суммарное количество активных S-блоков на входе и выходе этого преобразования, при условии фактической активизации входа. Для байтовых S-блоков – это минимальное количество активных байтов до и после преобразования. В этом случае, число ветвей активизации (в терминах [2] – степень «размножения» активизации) может быть определена, как минимальное суммарное количество ненулевых байтов на входе и выходе этого преобразования, при отображении отличного от нуля входного значения.

1.3. Начальное и конечное преобразования

Начальное IT преобразование уменьшенной версии шифра «Лабиринт» (рис.3), повторяя по структуре оригинальную разработку, включает сложение теперь уже по модулю 2^8 полублоков входного блока данных (по 8 бит) с 8-битными рабочими подключами (левый полублок ключа (8 бит) суммируется с левым полублоком входного блока данных, а правый полублок ключа (8 бит) соответственно с правым полублоком входного блока данных). На следующем шаге 16 результирующих бит разбиваются на блоки по 4-е бита, которые подаются на нелинейные преобразования S-блоки. Результат 16 бит снова разбивается на два полублока, над которыми выполняются циклические сдвиги: левый полублок сдвигается на 2 бита влево, а правый соответственно на два бита вправо, и в заключение над полученным 16-ти битным блоком выполняется операция инволютивного линейного смешивания IMix.

В уменьшенной версии шифра операция IMix, повторяя идею оригинального алгоритма, реализует сложение по модулю два 8-ми битных половинок входного блока данных, и после циклического сдвига результата влево на 5 бит, его сложение по модулю два с полублоками входного блока данных поступающими на вход преобразования IMix.

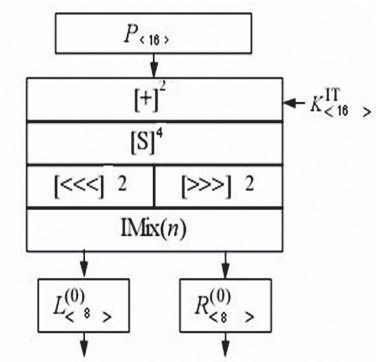

Рис. 3. Начальное преобразование IT

Конечное FT преобразование (рис.4) выполняет те же операции, что и начальное, но только в обратном порядке.

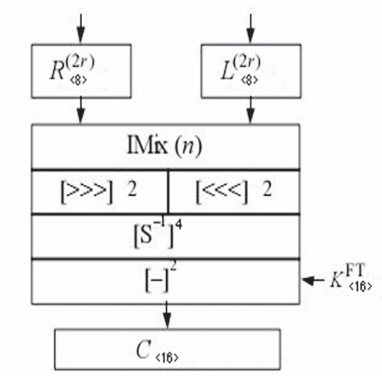

Рис. 4. Конечное преобразование FT

Как и в большом шифре, после выполнения последней итерации цепи Фейстеля, левый и правый полублоки меняются местами, и только после этого результирующий блок поступает на вход FT-преобразования.

1.4. Преобразование SL

SL-преобразование определяет фиксированное биективное отображение слов. Это преобразование представляет собой объединение нелинейного преобразования байтов (с помощью байтовых S-блоков), с последующим линейным «смешиванием» результатов нелинейного преобразования.

В уменьшенной модели операции выполняются над полубайтами. Поэтому сначала над каждыми двумя полубайтами, объединенными в полублок, выполняется нелинейное преобразования с помощью уменьшенных (полубайтовых) S-блоков, над выходными полубайтами которых выполняется MBN-преобразование (линейное смешивание). Это преобразование осуществляет биективное линейное отображение слов, составляющих полублок (для уменьшенной модели полублок имеет размерность байта).

MBN-преобразование, использованное в шифре «Лабиринт», автор представляет в виде умножения квадратной матрицы размерностью 8×8 байт, образованной циклическим MBN-кодом, справа на вектор-столбец длиной 8 байт (соответствующий слову-аргументу). Элементы матрицы (байты), и элементы векторов аргумента – результата, интерпретируются как элементы поля $GF(2^8)$, образованного выбранным неприводимым (над полем GF(2)) полиномом 8-й степени $f_{MBN}(x)$.

Мы постарались сохранить идею построения MBN-преобразования и в уменьшенной модели шифра «Лабиринт». Оно реализовано в виде умножения квадратной матрицы размерностью 2×2 полубайта (ПВ), образованной циклическим MBN-кодом, справа на вектор-столбец длиной 1 байт (два полубайта, соответствующих слову-аргументу). Элементы матрицы и элементы векторов аргумента – результата, интерпретируются как элементы поля $GF(2^4)$ (полубайты), образованного выбранным неприводимым (над полем GF(2)) полиномом 4-й степени $f_{MBN}(x) = x^4+x^3+1$.

В данной разработке мини-версии БСШ «Лабиринт» используется следующий полином второй степени, порождающий MBN-код:

$$g(x) = 11x + 01.$$

1.5. Узел замены

Как отмечает сам автор разработки в [4], S-блок шифра «Лабиринт» выбран из множества так называемых предельно-нелинейных биективных преобразований, в основе которых лежит конструкция Ниберг-Динга, т.е. преобразование, аффинно-эквивалентное функции вычисления обратного элемента в поле $GF(2^8)$. Математически функция, определяющая преобразование $S(x)$, которое осуществляется S-блоком шифра «Лабиринт», автором разработки представлена в виде:

$$S(x) = M \times \left\lfloor \left(M_x \times x \oplus V_y \right)^E \right\rfloor_B \oplus V_y ,$$

где $x, V_x, V_y \in GF(2^8)$; $E = 2^8 - 1 - 2^t$, $0 \le t < 8$; B – некоторый базис над $GF(2^8)$, который определяется образующим (неприводимым) полиномом 8-й степени $f_S(x)$; M_X, M_Y – квадратные невырожденные матрицы размера 8×8, с элементами из поля $GF(2)$, $M_X, M_Y \in GL(8, GF(2))$ В приведенном соотношении для упрощения записи вектора, участвующие в матричном умножении, рассматриваются как вектор-столбцы. Более подробно с соображениями автора по выбору этого преобразования можно познакомиться в его работе [4].

В уменьшенной модели шифра «Лабиринт» операции выполняются над полубайтами. Поэтому матрицы входного и выходного аффинных преобразований были взяты размером 4×4, а конкретнее:

$$M_X = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{vmatrix};$$

$$M_Y = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{vmatrix}; \; V_X = \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \end{vmatrix}; V_X = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 1 \end{vmatrix},$$

т.е. строки (столбцы) рассматриваются как элементы векторного пространства, образуемого полем $GF(2^4)$. Соответствующий неприводимый полином выбран вида $f_S(x) = x^4 + x + 1$, а параметр E взят равным $2^4 - 1 - 2^2 = 11$. Матричное представление подстановки вычисленной для этих параметров имеет вид:

$$\begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15 \\ 11\ 8\ 6\ 4\ 10\ 0\ 13\ 2\ 12\ 5\ 1\ 14\ 3\ 15\ 9\ 7 \end{pmatrix}.$$

1.6. Процедура разворачивания ключа

Из приведенной выше структуры шифрующего преобразования алгоритма «Лабиринт» следует, что процедура шифрования требует рабочий ключ длиной 8×8 + 2×16 бит (8 ключей итераций по 8 бит, а также ключи начального и конечного преобразований по 16 бит). Для формирования рабочего ключа указанной длины на основе исходного (пользовательского) ключа существенно меньшего объёма используется процедура разворачивания ключа.

Процедура разворачивания ключа мини версии алгоритма «Лабиринт» поддерживает длину пользовательского ключа 16 бит, по 8 бит на один полублок.

Процедура разворачивания ключа состоит из двух этапов:

– инициализация буфера рабочего ключа на основе исходного ключа пользователя;

– выборка подключей из буфера рабочего ключа.

Процедура инициализации заключается в загрузке исходного ключа в буфер рабочего ключа и дополнения этого ключа до полного заполнения буфера ключевым материалом, сформированным из исходного ключа. Для формирования «дополнительного» ключевого материала используется базовая F-функция шифратора, на основе которой построен простой криптографический генератор псевдослучайных последовательностей – исходный ключевой материал циклически зашифровывается в режиме «связки шифроблоков» (CBC-режим [4]).

Более детально. Процедура разворачивания ключа начинается с загрузки пользовательского ключа в шифратор, а именно в буфер рабочего ключа.

Затем исходный ключ длиной 16 бит разбивается на полублоки. Правый полублок берется в качестве первого подключа, левый полублок – второго подключа.

Далее формируется ключ k_{KS}, путем сложение полублоков исходного ключа по модулю 2. Ключ k_{KS} используется для формирования остальных подключей. Для этого на следующем шаге выполняется циклический сдвиг k_{KS} на 5 битов влево и затем в цикле формируется еще 6 подключей. В цикле формирования подключей операции осуществляются в следующем порядке. Сначала выполняется функция «обновления» ключа k_{KS} путём сложения k_{KS} по модулю 2^8 с константой 0×21 (в шестнадцатеричном формате), далее результат складывается по модулю два с константой 0×44. Рабочий подключ $WKey_i$ вычисляется как сумма по модулю два подключа $WKey_{i-2}$ с результатом преобразования подключа $WKey_{i-1}$, выполняемым с использованием базовой функции зашифрования F с ключом k_{KS}.

Последовательность выбора подключей итераций $K^{(t)}$) для осуществления зашифрования представлена в табл. 1. При выполнении расшифрования эти же подключи выбираются в обратном порядке.

Как видно из табл. 1, каждый полублок буфера рабочего ключа используется только на двух итерациях цепи Фейстеля.

Одним из достоинств данной схемы разворачивания ключа, и всей конструкции шифра в целом, отмечает автор, является применимость одного и того же материала «развёрнутого» ключа как для преобразования зашифрования, так и расшифрования.

По приведенному алгоритму была реализована библиотека программной реализации мини версии шифра «Лабиринт», и на ее основе выполнены исследования ряда криптографических показателей уменьшенной модели.

2. ИССЛЕДОВАНИЕ ЦИКЛИЧЕСКИХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «ЛАБИРИНТ»

Следуя методике, рассмотренной в работе [2], приведем теперь результаты сравнительного ана-

лиза циклических свойств уменьшенной модели шифра «Лабиринт». В качестве эталонов рассматриваются аналогичные результаты исследований, выполненные с использованием уменьшенных моделей шифров Baby Rijndael и Baby Camellia. Первый шифр представляет финалиста конкурса по выбору AES-а, а второй – одного из победителей конкурса NESSIE. Примечательно, что, если Baby Rijndael построен по классической SPN схеме, то шифр Baby Camellia использует, как и рассматриваемый шифр «Лабиринт», структуру цепи Фейстеля. Результаты исследования цикловых свойств рассмотренных мини шифров приведены в табл. 2.

Как следует из представленных данных, распределение подстановок (ключей) по числу циклов для шифра «Лабиринт» практически повторяет соответствующие показатели для шифров Baby Rijndael и Baby Camellia. Полученный закон распределения подстановок (ключей) очень близок к асимптотическому закону, характерному для подстановок случайного типа, однако он не проходит проверку на соответствие нормальному закону распределения с асимптотически предельными значениями параметров – в некоторых точках выходит за границы, определяемые статистическим критерием Колмогорова). Тем не менее, полученное распределение, как и распределения циклов по длительности для других приведенных в табл. «эталонных» шифров, имеет числовые характеристики практически повторяющие характеристики асимптотических распределений. Поэтому мы сделали заключение, что и для шифра «Лабиринт» справедливы все выводы и обобщения в отношении циклических свойств больших прототипов, приведенные в работе [2].

3. ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ УМЕНЬШЕННОЙ МОДЕЛИ ШИФРА «ЛАБИРИНТ»

Мы также рассмотрели дифференциальные свойства уменьшенной модели шифра «Лабиринт». Как и в предыдущей нашей работе [6], мы и в этом случае вычисляли полные дифференциалы и искали их максимальные значения Δ^r (Δ^r -равномерность r-циклового шифра – максимальное значение его таблицы дифференциальных разностей). Методика выполнения исследований повторяет изложенную в работе [6], только приведенные в табл. 3 результаты вычислялись по выборке из 10-ти ключей.

Таблица 1

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k_i	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7

Таблица 2

Число циклов k	Baby Rijndael		Baby Camellia		Baby «Лабиринт»	
	Число подстановок N_n (ключей)	Расчетное значение вероятности P_k	Число циклов k	Число подстановок N_n (18 циклов)	Число подстановок N_n (2 цикла)	Число подстановок N_n (8 циклов)
2	18	0,00027	2	28	16	25
4	499	0,00761	4	496	517	559
6	3255	0,04967	6	3147	3246	3129
8	9436	0,14398	8	9373	9306	9447
10	15429	0,23543	10	15567	15397	15320
12	15963	0,24358	12	15903	16008	16085
14	11580	0,1767	14	11530	11566	11642
16	5956	0,09088	16	6168	6120	6066
18	2411	0,03679	18	2406	2401	2277
20	774	0,01181	20	713	708	775
22	174	0,00266	22	160	198	173
24	35	0,00053	24	36	44	33
26	6	0,00009	26	9	6	5
28		0	28	0	3	
30		0	30	0		
32		0	32	0		

Таблица 3

$\Delta^{(r)}$ / Шифр	Число циклов r						
	2	3	4	5	6	7	8
Baby ADE	3254±59	301,3±7,3	20,064±0,348	19,170±0,124	19,120±0,092	19,166±0,093	19,106±0,091
Mini AES	4955±24	640,6±4,6	43,066±0,999	20,538±0,202	19,082±0,093	19,122±0,092	19,122±0,096
Baby «Лабиринт»	19,2	19	18,6	19,2	19,2	19,2	19,142

Табл. 3 иллюстрирует результаты сравнительного анализа дифференциальных свойств шифров Baby Rijndael, Baby ADE и Baby «Лабиринт» ($\Delta^{(r)}$-равномерность r-циклового шифра).

Результаты свидетельствуют о том, что показатели стойкости рассмотренных мини-версий шифров оказываются весьма близкими. Все они после 4-х циклов (Mini AES после 5-ти) демонстрируют уже потенциальные характеристики ($\Delta^{(r)} \approx 19$), что позволяет заключить, что и большая версия шифра.

«Лабиринт» будет обладать стойкостью к атакам дифференциального криптоанализа не уступающей шифрам Rijndael и Camellia. Следует, однако, отметить, что начальное преобразование шифра «Лабиринт» демонстрирует заметную эффективность. Благодаря этому преобразованию, шифр «Лабиринт» выходит на потенциальные показатели уже после второго цикла.

В табл. 4 представлены максимумы дифференциальных разностей (*DP*) для 16-цикловой мини версии шифра «Лабиринт» с наборами S-блоков с различными значениями максимумов таблиц дифференциальных разностей уже самих S-блоков, сформированных генератором случайных подстановок.

Таблица 4

DP S блока	Среднее значение максимумов DP	DP максимумы	
		Максимум	Число ключей
«Лабиринт» максимум $\Delta = 4$	19,142 1000 ключей	18	466
		20	498
		22	35
		24	1
Случайный $\Delta = 6$	19,2 Далее 10 ключей	18	4
		20	6
Случайный $\Delta = 8$	19,6	18	2
		20	8
Случайный $\Delta = 10$	19,2	18	4
		20	6
Случайный $\Delta = 12$	19,2	18	5
		20	4
		22	1

Из представленных результатов следует, что результирующие («асимптотические») значения полных дифференциалов (для 16-ти цикловой версии мини-шифра) практически не зависят от выбора *S*-блоков.

По-видимому, определяющее значения в обеспечении стойкости шифра к дифференциальным атакам имеют не свойства используемых в шифре подстановочных преобразований, а свойства самого шифра как подстановки. Большое число циклов приводит к тому, что механизм перемешивания битов выходит на предельные показатели, свойственные асимптотическим показателям случайных подстановок.

В табл. 5 представлены более полные результаты, характеризующие зависимость DP от числа итераций (на 10 ключах).

Таблица 5

Число циклов	Число итераций	Среднее значение максимумов DP	DP максимумы	
			Максимум	Число ключей
1	1	289.4	376	1
	2	51.2	138	1
2	3	19,0	22	1
	4	19,2	20	6
3	5	18,8	20	4
	6	19	20	5
4	7	19	20	5
	8	18,6	20	3
5	9	19,4	20	7
	10	19,2	20	6
	11	19,0	20	5
8	16	19,142	24	1

ЗАКЛЮЧЕНИЕ

Как следует из представленных результатов, циклические свойства уменьшенной модели шифра «Лабиринт» оказываются весьма близкими к циклическим свойствам Baby Rijndael. Повторяющими показатели стойкости к диффенциальному криптоанализу шифра Baby Rijndael являются и соответствующие показатели уменьшенной модели шифра «Лабиринт». Учитывая дуальную связь между дифференциальными и линейными свойствами, можно ожидать, что будут близкими и линейные аппроксимационные характеристики (линейные корпуса) обоих шифров.

Все это позволяет заключить, что по основным показателям стойкости шифр «Лабиринт» не уступает соответствующим показателям победителя конкурса AES шифру Rijndael.

Вместе с тем, анализ решений, использованных при построении шифра «Лабиринт», позволяет заключить, что он во многом унаследовал принципиальные идеи победителя конкурса AES. Как и в Rijndael, основой линейного преобразования является матричное преобразование, построенное на использовании проверочной матрицы MDR кода. Близкими по выполнению (алгебраическими по структуре) оказываются и его S-блоки. Как и в шифре Rijndael они строятся на основе конструкции, указанной еще в работах К. Ниберг, т.е. преобразования, использующего вычисление обратного элемента в поле $GF(2^8)$, встроенного в аффинное преобразование.

В целом, однако, конструкция шифра «Лабиринт» представляется существенно более сложной (утяжеленной) и запутанной для понимания. Вряд ли можно считать оправданными явно усложненные начальное и конечное преобразования, более сложное нелинейное преобразование, использующее умножение на две матрицы (свойства S-блока шифра «Лабиринт» ничем не лучше свойств S-блока шифра Rijndael). Платой за эти усложнения является снижение скоростных характеристик алгоритма. По результатам измере-

ний, проведенных в ИИТ-е, он почти в полтора раза уступает AES-у по скорости зашифрования.

Можно также отметить, что механизм образования потенциальных показателей в отношении значений полных дифференциалов и линейных корпусов нуждается в дальнейшем изучении. Хотелось бы установить более четкие аргументы по связи криптографических показателей с предельно достижимыми показателями, обеспечивающими стойкость шифров к атакам дифференциального и линейного криптоанализа.

В заключение хотелось бы отметить, что развиваемый нами подход, предложенный ранее на конференции в Туапсе [3], подтверждает свое право рассматриваться как один из прогрессивных новых методов криптоанализа.

Литература.

[1] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) // Прикладная радиоэлектроника. – 2008. – Т.7 – № 3. – С. 215-224.

[2] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника – 2007. – Т.6, №2 – С. 257-263.

[3] *Долгов В.И., Лисицкая И.В., Олейников Р.В.* Подход к криптоанализу современных шифров // Материалы второй международной конференции «Современные информационные системы. Проблемы и тенденции развития», Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436.

[4] *Головашич С.А.* «Алгоритм Блочного Симметричного Шифрования «Лабиринт», Версия 1.1 //www.cryptomach.com/publications.

[5] *Головашич С.А.* Метод конструирования цикловых функций БСШ // Автоматизированные системы управления и приборы автоматики. Всеукр. межвед. научн.-техн. сб. 2001. – Вып. 117. – С. 155–161.

[6] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES // Прикладная радиоэлектроника – 2009. – Т.8. – № 3. – С. 25-257.

Поступила в редколлегию 18.09.2009

Долгов Виктор Иванович, доктор технических наук, профессор кафедры «Безопасности информационных технологий» ХНУРЭ. Область научных интересов: математические методы защиты информации.

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

Григорьев Андрей Владимирович, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: криптоанализ.

Широков Алексей Викторович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптоанализ.