УДК 681.3.06

Л.С. Сорока[1], А.А. Кузнецов[2], И.В. Московченко[3], С.А. Исаев[1]

[1]*Харьковский национальный университет им. В.Н. Каразина, Харьков*
[2]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[3]*Национальный технический университет «ХПИ», Харьков*

ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ БЛОЧНО-СИММЕТРИЧНЫХ ШИФРОВ

Рассматриваются блочно-симметричные шифры, поданные на открытый конкурс по отбору кандидатов на национальный стандарт блочного симметричного шифрования Украины. Исследуется эффективность мини-версий поданных на конкурс шифров относительно дифференциального криптоанализа как в зависимости от числа раундов преобразования, так и в зависимости от числа операций и требуемых затрат памяти. Оценивается влияние свойств применяемых нелинейных узлов замен на дифференциальные характеристики блочно-симметричных шифров.

Ключевые слова: *шифр, дифференциал, S-бокс, моделирование, криптоанализ.*

Постановка проблемы в общем виде и анализ литературы

Несколько лет назад институтом кибернетики имени В.М. Глушкова НАНУ и Департаментом специальных телекоммуникационных систем и защиты информации СБУ был объявлен открытый конкурс, основной целью которого является определение криптографического алгоритма, на базе которого в дальнейшем может быть разработан национальный стандарт блочного симметричного шифрования (БСШ) Украины [1]. В качестве кандидатов поданы следующие алгоритмы: Калина, Мухомор, Лабиринт, RSB-32 и ADE [2 – 6]. Актуальной задачей является оценка эффективности БСШ, обоснование выбора алгоритма-кандидата в виде рационального компромисса по вычислительной сложности и обеспечиваемой криптостойкости шифра.

Один из подходов по анализу и оценке свойств БСШ состоит в использовании их уменьшенных моделей (версий) [7 – 9]. Под мини-версией будем понимать шифр, который, при сохранении математической структуры шифра, имеет меньшие, чем шифр-оригинал длины блоков данных и ключей. Это достигается пропорциональным уменьшением соответствующих длин блоков данных и ключей, например, с 128 бит до 16 бит. В работе мы рассматривали свойства мини-версий шифров, поданных на украинский конкурс, а также американского стандарта шифрования AES [7 – 9] и простейшего SPN шифра Хейса [10].

Первая часть наших исследований состояла в оценке влияния используемых при проектировании БСШ нелинейных узлов замен (S-боксов) на их устойчивость к дифференциальному криптоанализу. Исследования состояли в построении таблиц XOR разностей, оценке максимальных значений переходов и сравнении их с асимптотическим показателем среднего значения максимума полных дифференциалов для мини-версий шифров с использованием двух различных S-боксов: один обладал заведомо лучшими свойствами по нелинейности и автокорреляции, чем другой. Вторая часть исследований заключалась в оценке вычислительной эффективности шифров при фиксированном уровне стойкости к атакам дифференциального криптоанализа. В данном случае оценивались вычислительные ресурсы, которые требуется внести в качестве «платы» за реализацию асимптотического показателя среднего значения максимума полных дифференциалов для конкретного шифра.

Проводимые исследования являются логическим продолжением работ [11, 12]. При подготовке материала статьи были использованы также теоретические сведения из [13, 14] и методика расчета вычислительной сложности из [15].

Дифференциальные свойства БСШ

В статьях [13, 14] приводятся теоретические расчеты для среднего значения максимумов таблиц XOR разностей подстановок. Также в работе [14] на основании полученных расчетов выдвигается идея подхода к сравнению эффективности БСШ в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов. В основу первой части наших исследований как раз и был положен данный подход. Приведем основные обозначения, аналитические выражения и расчетные результаты из [13, 14].

Согласно [13, 14] положим, что $\pi : Z_2^m \to Z_2^m$ является биективным m-битным отображением и пусть S_{2^m} будет множеством всех таких отображений. Пусть $\Lambda_\pi(\Delta X, \Delta Y)$ будет значением XOR в ячейке таблицы разностей для пары значений разностей вход-выход ΔX, $\Delta Y \in Z_2^m$, $\Delta X = X + X'$, $\Delta Y = \pi(X) + \pi(X')$ подстановки $\pi \in S_{2^m}$.

Выражение для оценки числа $\Lambda_{m,2k}$ переходов таблицы дифференциальных разностей подстановки порядка 2^m, а именно для оценки среднего значения числа ненулевых характеристик $\Delta X \to \Delta Y$, таких, что $\Lambda_\pi(\Delta X, \Delta Y) = 2k$, имеет вид [13, 14]:

$$\Lambda_{m,2k} = \frac{(2^m - 1)^2}{2^m!} \cdot \binom{2^{m-1}}{k}^2 \cdot k! 2^k \cdot \Phi(2^{m-1} - k). \quad (1)$$

Согласно [13, 14] среднее значение максимума таблицы XOR разностей находится из соотношения (1) путем определения максимального значения *k*, при котором результат расчетов по этому выражению приводит к наименьшему целому значению. Другими словами, нужно найти решение уравнения

$$\frac{(2^m - 1)^2}{2^m!} \cdot \binom{2^{m-1}}{k}^2 \cdot k! 2^k \cdot \Phi(2^{m-1} - k) \approx 1. \quad (2)$$

Расчеты, выполненные в соответствии с соотношениями (1) и (2), представлены в табл. 1. В табл. 2 из [14] приведены расчеты, выполненные в соответствии с выражением (1), а также представлены соответствующие результаты для 16-битного шифра по Хейсу с линейным преобразованием, подобным операции MixColumn в шифре Rijendael.

Таблица 1

Расчетные результаты

m	10		12		14		16	
2k	12	14	14	16	16	18	18	20
$\Lambda_\pi(\Delta X,\Delta Y)=2k$	13,85	0,99	15,79	0,99	15,78	0,88	14,02	0,7

Таблица 2

Распределение ***парных*** разностей для SPN шифра

Расчет	Эксперимент
#2. 1302484861	#2. 1302551726
#4. 325626184	#4. 325625709
#6. 54271858	#6. 54253870
#8. 6784085	#8. 6781574
#10. 678418	#10. 677785
#12 56535	#12 56793
#14. 4038	#14. 3974
#16. 252	#16. 272
#18. 14	#18. 17
#20. 1	#20. 0

На основании полученных результатов предлагается подход к оценке эффективности БСШ в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума полных дифференциалов, который и был положен в основу наших исследований.

В данной статье проводится оценка эффективности мини-версий БСШ по минимальному числу циклов (число выполняемых операций) криптоалгоритма, необходимых для выхода на асимптотический показатель среднего значения максимума полных дифференциалов. Также исследовано влияние свойств используемых в БСШ нелинейных узлов замен на минимальное число циклов, при которых реализуются асимптотические свойства полных дифференциалов.

Методика исследований

Наши исследования состояли в том, чтобы рассмотреть каждый шифр как одну большую подстановку и оценить дифференциальную характеристику, покрывающую весь шифр. Другими словами, в качестве подстановки мы рассматриваем весь набор шифрующих преобразований для одного ключа. Рассматриваются 16-ти разрядные мини-версии шифров с 16-ти разрядным ключом. Следовательно, общее число различных подстановок равно мощности ключевого пространства 2^{16} и для каждого ключа таблица дифференциалов имеет размер $2^{16} \times 2^{16}$.

Дифференциальная характеристика шифра как подстановки изменяется от раунда к раунду. Однако, как следует из [13, 14] после некоторого числа раундов шифрующего преобразования дифференциальная характеристика шифра будет стремиться к дифференциальной характеристике случайной подстановки.

Полное множество рассчитанных средних значений таблицы XOR разностей для случайной подстановки приведено в левой колонке таблицы 2, которую можно расценивать как асимптотическую характеристику распределения парных разностей. Нас будет интересовать асимптотическое значения максимума таблицы XOR разностей (характеризующие устойчивость шифра к дифференциальному криптоанализу) и дифференциальные свойства мини-версий шифров по отношению к этой (теоретической) границе.

Как следует из табл. 1, среднее значение максимума таблицы XOR разностей для m = 16 лежит в диапазоне от 18 до 20. Это и есть интересующая нас теоретическая оценка дифференциальной характеристики случайной подстановки. Число раундов (число требуемых операций) шифра, при котором реализуется это асимптотическое значение, является оценкой сложности (затратности) шифра, то есть оценкой той «платы», которую требуется внести для обеспечения устойчивости конкретного шифра к дифференциальному криптоанализу.

При исследовании дифференциальных свойств шифров использованы мини-версии с различными S-боксами. Во-первых, использованы узлы замен шифра DES с характеристиками: NL = 2, AC = 16, Deg = 2. Во-вторых, использованы сформированные S-боксы с улучшенными показателями: NL = 4, AC = 8, Deg = 3, где NL – нелинейность, AC – автокорреляция, Deg – алгебраическая степень булевых функций, задающих узел замен в терминах [16].

Описание мини-версий некоторых шифров приводятся в работах [11, 12]. Здесь мы приведем только способы построения нелинейных узлов замен для рассматриваемых мини-шифров.

В 16-битном шифре Хейса для каждого цикла используются 4 одинаковых S-бокса размерностью 4x4. В табл. 3 приведены табличные представления отобранных для проведения экспериментов S-боксов.

Таблица 3

S-боксы для шифра Хейса

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
2	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
3	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
4	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D
5	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
6	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
7	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
8	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9
9	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
10	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
11	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
12	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C
13	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
14	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
15	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
16	A	4	3	B	8	E	2	C	5	7	6	F	0	1	9	D
17	A	3	8	2	5	6	0	9	B	4	C	E	F	7	D	1
18	A	B	2	E	0	D	6	7	F	5	1	9	C	8	4	3
19	A	8	5	0	B	C	F	D	2	3	9	6	E	4	1	7
20	A	E	6	D	C	3	1	5	9	F	8	4	7	0	B	2
21	A	2	0	6	F	1	C	4	E	B	7	D	9	5	3	8
22	A	C	9	7	D	5	4	2	1	6	B	8	3	E	0	F
23	A	5	B	F	2	9	E	1	0	8	D	C	6	3	7	4
24	A	7	4	5	3	F	B	6	8	1	E	0	2	D	C	9
25	A	6	C	1	9	8	7	B	D	E	5	3	4	F	2	0
26	A	F	E	9	6	4	D	8	C	0	3	7	1	2	5	B
27	A	0	F	C	E	7	9	3	6	2	4	1	D	B	8	5
28	A	1	7	8	4	0	5	E	3	D	F	2	B	9	6	C
29	A	9	D	4	1	B	3	0	7	C	2	5	8	6	F	E
30	A	D	1	3	7	2	8	F	4	9	0	B	5	C	E	6
31	D	E	B	5	4	2	1	F	0	9	6	A	7	C	8	3
32	B	8	6	4	A	0	D	2	C	5	1	E	3	F	9	7
33	0	6	C	2	D	5	E	8	4	9	B	7	3	1	F	A

Первый S-бокс (строка 1 табл. 3) соответствует узлу замен шифра DES, он обладает свойствами: NL = 2, AC = 16, Deg = 2. Второй S-бокс (строка 31 табл. 3) сгенерирован случайным образом. Его свойства следующие: NL = 4, AC = 16, Deg = 2. При реализации mini-AES использован узел замен DES (строка 1 табл. 3) и улучшенный по нелинейности и автокорреляции S-бокс, соответствующий узлу замен мини-шифра ADE [11, 12] (строка 16 табл. 3). Свойства последнего S-бокса: NL = 4, AC = 8, Deg = 3.

В шифре ADE используются сменные таблицы блоков замены, которые динамически формируются с помощью дополнительно введенного параметра $\gamma \in GF(2^8)$, который определяется битами расширенного ключа [6]. Идея этого преобразования повторена и в мини-шифре ADE, с учетом масштабирования к размеру 16-битного состояния.

Таким образом, в качестве S-бокса выступает сменная матрица подстановок, которая строится с помощью вычисления мультипликативно обратного элемента поля $(a \cdot \gamma)^{-1} \in GF(2^4)$ с дальнейшим выполнением аффинного преобразования над полем GF(2): $b = M \cdot (a \cdot \gamma)^{-1} + \beta$, где M – квадратная невырожденная матрица 4×4:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad \beta^T = (1 \quad 0 \quad 1 \quad 0).$$

При $\gamma_i = k_0 = 0 \to 0000$ параметр γ_i принимается равным k_1. Если полубайт k_1 также равняется нулю, то $\gamma_i = 3 \to 0011$.

В наших исследованиях в мини-шифре ADE использовались S-боксы DES (строки 1-15 табл. 3), и улучшенные S-боксы, построенные описанным выше способом (строки 16-30 табл. 3). S-боксы DES и мини-ADE обладают следующими свойствами, соответственно: NL = 2, AC = 16, Deg = 2 и NL = 4, AC = 8, Deg = 3.

S-блок шифра «Лабиринт» выбран из множества так называемых предельно-нелинейных биективных преобразований [4], в основе которых лежит конструкция Ниберг-Динга, т.е. преобразование, аффинно-эквивалентное функции вычисления обратного элемента в поле $GF(2^8)$. Математически данная функция записывается в виде:

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

где $x, V_x, V_y \in GF(2^8)$; $E = 2^8 - 1 - 2^t, 0 \le t \le 8$; 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 (2^8), $M_x, M_y \in GL(8, GF(2))$.

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

$$M_x = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{vmatrix}; \; M_y = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{vmatrix}; \; V_x = \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \end{vmatrix}; \; V_y = \begin{vmatrix} 0 \\ 0 \\ 0 \\ 1 \end{vmatrix},$$

т.е. строки (столбцы) рассматриваются как элементы векторного пространства, образуемого полем $GF(2^4)$. Соответствующий неприводимый полином выбран вида $f_{MBN}(x) = x^4 + x + 1$, а параметр E взят равным $2^4 - 1 - 2^2 = 11$. Табличное представление подстановки, вычисленной для этих параметров, приведено в строке 32 таблицы 3, его параметры следующие: NL = 4, AC = 8, Deg = 3. В качестве худшего S-бокса был взят S-бокс DES (строка 1 табл. 3).

Отметим также, что для мини-шифра Лабиринт начальное и конечное преобразования IT и FT считались как отдельные раунды преобразования. По этой причине исследования мини-шифра Лабиринт проведены начиная с трех раундов преобразования.

В шифре Калина таблицы подстановок сформированы случайным образом [2]. В уменьшенной версии шифра Калина используются 2 фиксированные подстановки 16-го порядка. Текущее состояние шифруемого сообщения представляется в виде массива

полубайт размера 2×2. К первой строке массива применяется одна подстановка, ко второй – вторая. Подстановка определяется как замена полубайта состояния на полубайт из таблицы, такой, что номер его столбца определяется двумя младшими, а строки – двумя старшими битами полубайта состояния. При реализации мини-Калины также использованы S-боксы двух видов: с худшими свойствами были взяты из шифра DES (строки 1 и 2 табл. 3), улучшенные S-боксы (строки 16 и 17 табл. 3) – из мини-шифра ADE.

В шифре Мухомор таблицы подстановок сформированы случайным образом [3]. При выполнении SL-преобразования 4-битное входное значение подвергается замене в соответствии с фиксированной таблицей подстановки: DES S-бокс (строка 1 табл. 3) и улучшенный S-бокс, взятый из шифра мини-ADE (строка 16 табл. 3).

Схема построения S-боксов, посредством которых реализуются операции нелинейной подстановки (замены) байтов в RSB алгоритме имеет вид [5]: $y = (x \oplus \alpha)_{\varphi}^{-1} \otimes A \oplus \beta$, где α и β – байты блочного раундового ключа; A – невырожденная (0, 1)-матрица преобразования, формируемая с помощью обобщенных кодов Грея; x^{-1} – элемент, мультипликативно обратный байту x над выбранным неприводимым полиномом φ. Операции нахождения мультипликативно обратного элемента и умножение на матрицу A можно заменить табличным преобразованием.

Следовательно, формула замены примет вид: $y = tab[x \oplus \alpha] \oplus \beta$. В нашей реализации мини-шифра RSB использовались следующие S-боксы: вычисленный по формуле замены S-бокс (строка 33 табл. 3) и узел замен шифра DES (строка 1 табл. 3).

Результаты исследований

При проведении экспериментальных исследований построено 100 таблиц разностей для каждого из исследуемых мини-шифров как с использованием нелинейных узлов замен шифра DES, так и с использованием улучшенных S-боксов при количестве раундов преобразования от 1 до 6 и случайно выбранных 16-битных значений ключей зашифрования. При проведении исследований определялись показатели:

– средние по множеству из 100 случайно выбранных ключей шифрования (по множеству таблиц) значения условных максимумов таблиц разностей мини-шифров;

– абсолютные значения условного максимума таблиц разностей мини-шифров по множеству из 100 ключей зашифрования.

В табл. 4 и 5 представлены полученные экспериментальные результаты. По результатам экспериментов построены также диаграммы, которые наглядно демонстрируют преимущества использования улучшенных S-боксов как для каждого шифра в отдельности (рис. 1), так и для всех мини-шифров вместе (рис. 2).

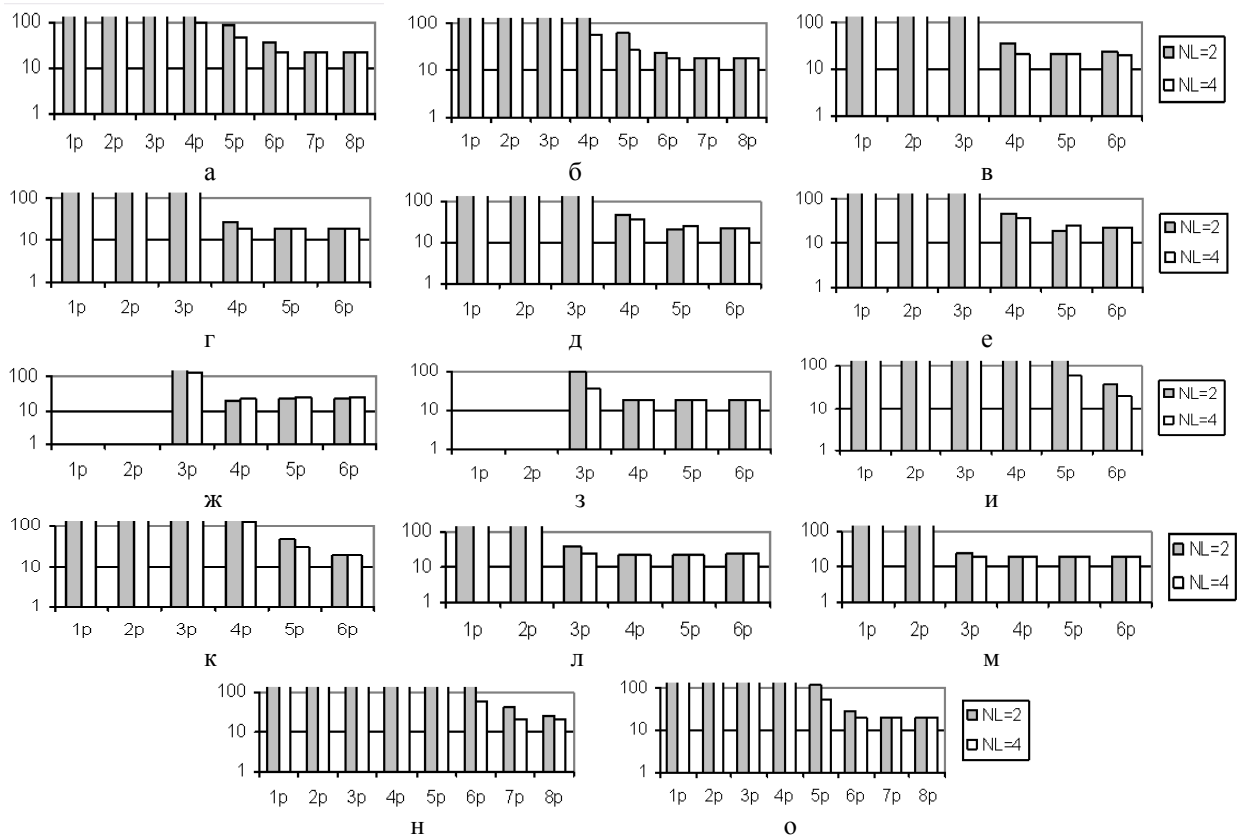


Рис. 1. Абсолютные и средние максимумы и (а, б – шифр Хейса; в, г – AES; д, е – ADE; ж, з – Лабиринт; и, к – Мухомор; л, м – Калина; н, о – RSB соответственно)

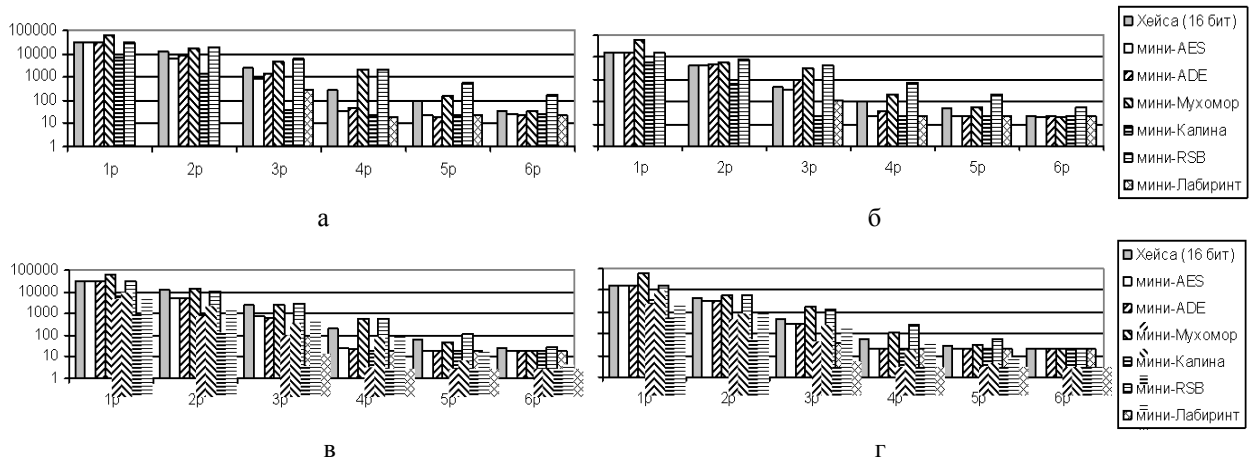


Рис. 2. Абсолютный (а, б) и средний (в, г) максимумы, S-боксы с NL=2 (а, с) и NL=4 (б, г)

Таблица 4

Абсолютные значения условного максимума таблиц разностей

# раундов	Шифр Хейса		Мини-AES		Мини-ADE		Мини-Лабиринт		Мини-Мухомор		Мини-Калина		Мини-RSB	
	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4
1	32768	16384	32768	16384	32768	16384	-	-	65536	65536	7168	6144	32768	16384
2	12288	4096	5632	4096	7680	5120	-	-	16384	6144	1376	640	20480	8192
3	2490	488	896	352	1312	1024	262	128	4608	3072	38	24	6152	4096
4	286	98	36	22	48	38	20	22	2304	224	22	22	2308	768
5	92	46	22	22	20	24	22	24	156	60	22	22	562	214
6	36	22	24	20	22	22	22	24	36	20	24	24	180	60
7	22	22	-	-	-	-	24	26	-	-	-	-	44	22
8	22	22	-	-	-	-	22	22	-	-	-	-	24	24

Таблица 5

Средние значения условного максимума таблиц разностей

# раундов	Шифр Хейса		Мини-AES		Мини-ADE		Мини-Лабиринт		Мини-Мухомор		Мини-Калина		Мини-RSB	
	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4	S-бокс NL=2	S-бокс NL=4
1	32768	16384	32768	16384	30392,32	16384	-	-	65536	65536	6082,56	3732,48	32768	16384
2	12288	4096	5437,44	3036,16	4910,08	3353,6	-	-	14187,5	5770,24	826,88	382,4	11486,7	5647,2
3	2326,81	439	817,28	274,24	672	307,2	101,96	37,5	2496,32	1802,24	24,8	19,36	2738,88	1305,8
4	216,803	56,964	26,02	19,326	23,02	20,54	19,14	19,04	542,72	125,53	19,04	19,14	572,298	261,81
5	65,38	26,18	19,06	19,02	19,08	19,08	19,02	19,24	46,28	29,7	19,14	19,2	117,338	54,288
6	24,108	19,11	19,187	18,812	19,24	19,24	19,06	19,04	19,48	18,88	19,14	19,36	28,775	20,641
7	19,021	19,09	-	-	-	-	18,96	19,14	-	-	-	-	19,315	19,073
8	19,16	19,1	-	-	-	-	19,32	19,24	-	-	-	-	19,151	19,017

Как видно из приведенных результатов (в таблицах соответствующие ячейки выделены серым цветом), использование улучшенных S-боксов по нелинейности и автокорреляции позволяет для некоторых шифров на 1 раунд раньше выйти к асимптотическому показателю условного максимум таблиц разностей, чем с использованием в шифрах S-боксов с худшими свойствами (в данном случае, DES S-боксов).

Анализ полученных результатов показывает, что рассматриваемые шифры выходят на асимптотический показатель среднего значения максимума полных дифференциалов в таком порядке: 1) Калина, 2) Лабиринт, 3) AES, 4) ADE, 5) Мухомор, 6) шифр Хейса, 7) RSB.

В тоже время, как показал проведенный анализ, число операций для реализации раунда преобразований одного шифра может существенно отличаться от числа операций для реализации раунда другого. Вторая часть проводимых исследований состояла в оценке вычислительной эффективности рассматриваемых БСШ, сравнении вычислительных ресурсов, которые необходимы для реализации асимптотического показателя среднего значения максимума полных дифференциалов для конкретного шифра.

Оценка вычислительной сложности

Задачу проектирования практического алгоритма БСШ следует рассматривать как задачу минимизации «затрат» на реализацию криптопреобра-

зования, обеспечивающего необходимые показатели криптостойкости [15]. Под «затратами» будем понимать перечень и объём ресурсов целевой аппаратной платформы, необходимых для реализации анализируемого алгоритма БСШ. Нас будут интересовать следующие аппаратные затраты [15]: вычислительные затраты – количество тактов либо микроопераций вычислителя, необходимых для шифрования одного блока данных длиной L_B**;** затраты оперативной памяти (RAM, единица измерения – байт или КБайт), необходимы для хранения, используемого в процессе вычислений, ключевого материала и промежуточных данных. Для оценки сложности в качестве аппаратной платформы будем использовать 32-битную процессорную архитектуру x86.

При проведении исследований использована методика, изложенная в [15], в соответствии с которой рассматривается случай достижения максимальной производительности. Для этого были применены следующие программные и алгоритмические методы оптимизации: общая табличная реализация S-блока и нелинейного смешивания байт (MBN-преобразования); реализация байтовых перестановок, где это возможно, «явным» способом, т.е. с нулевыми вычислительными затратами; применение техник «разворачивания» циклов и «inline-подстановки» подпрограмм.

Под элементарными микрооперациями ALU (Arithmetic and Logic Unit – арифметико-логическое устройство) понимаются операции, которые выполняются как отдельная команда ALU микропроцессора. Таким образом, нас будут интересовать следующие микрооперации ALU, используемые в рассматриваемых алгоритмах: сложение по модулю 2 (*XOR*); сложение с переносом, т.е. по модулю 2^m, где $m > 1$ (*ADD*); вычитание с переносом, т.е. по модулю 2^m, где $m > 1$ (*SUB*); сдвиг вправо (*ROTR*); сдвиг влево (*ROTL*); пересылка машинного слова между регистрами либо регистром и памятью (*MOV*).

Согласно [15] алгоритмы Калина, Мухомор, Лабиринт имеют следующую сложность циклового преобразования (табл. 6). В двух последних строках табл. 6 приведена оцененная по методике из [15] сложность циклового преобразования шифров AES и ADE. Как видно из таблицы, шифры AES и ADE имеют одинаковую сложность, т.к. в цикле шифрования оба алгоритма используют общую табличную реализацию S-блока и MBN-преобразования. Следует учесть, что последний раунд в обоих алгоритмах не имеет MBN-преобразования. С этих позиций приведем сложность преобразования последнего раунда шифров AES и ADE (табл. 7).

Шифры Калина, Мухомор, Лабиринт имеют начальное IT и конечное FT преобразования, а шифры AES и ADE имеют только начальное преобразование. Сложность данных преобразований приведена в таблице 8. Общая сложность шифров с учетом IT и FT преобразований приведена в таблице 9 ($L_B = 128$; $L_K = 128$ – длина ключа). Оценки затрат памяти приведены в таблице 10, они включают в себя: таблицы, использованные для S-блоков и MDN-преобразования; S-блоки, используемые в FT-преобразовании и последних раундах AES и ADE.

Таблица 6

Сложность циклового преобразования Калины, Мухомор и Лабиринта

Длина блока	$L_B = 128$	$L_B = 256$	$L_B = 512$
Алгоритм	*T*	*T*	*T*
Калина	56–58	112–116	224–232
Мухомор	51–54	131–139	329–345
Лабиринт	68–70	136–140	262–280
AES	36–38	72–76	144–156
ADE	36–38	72–76	144–156

Таблица 7

Сложность последнего раунда преобразования AES и ADE

Преобразование	Микрооперации		
	sum	**S-box**	**Всего**
AES	$(L_B/32)\times2$	$(L_B/64)\times8\times3+1$	$56\times L_B/128+1$
ADE	$(L_B/32)\times2$	$(L_B/64)\times8\times3+1$	$56\times L_B/128+1$

Наибольшую трудность, в виду нетрадиционного построения слоев шифрования, представляет оценка вычислительной эффективности шифра RSB. Согласно [5] каждый раунд зашифрования RSB алгоритма включает следующую совокупность последовательно выполняемых криптографических примитивов: стохастическая круговая прокрутка шифруемого блока (ShiftRow); стохастическая нелинейная подстановка (замена) байтов блока (SubByte); стохастическая перестановка элементов (слов) блока (PermuBox); скользящее кодирование 32-разрядных элементов блока (SlideCode). Поскольку скользящее кодирование применяется для блоков, начиная со второго, то сложность раундового преобразования следует рассчитывать для произвольного i-го ($i > 1$) блока сообщения.

Учитывая сложность всех криптографических примитивов, общая сложность раундового преобразования шифра RSB: 414 – 422 элементарных операций. Сложность всех рассмотренных шифров представлена в таблицах 9 и 10.

В соответствии с данными табл. 9 и 10 построены графики (рис. 3), которые наглядно демонстрируют эффективность рассматриваемых шифров относительно дифференциального криптоанализа по необходимым вычислительным затратам (в этой части исследований шифр Хейса не рассматривался). Сведения, относительно шифра RSB на графиках не отображены как неинформативные: асимптотический показатель условных максимумов, как для абсолютных, так и средних значений при его реализации достигается на 7 раунде, т.е. при выполнении 2898 элементарных операций.

Как видно из полученных графиков, рассматриваемые шифры выходят к своему асимптотическому показателю условных максимумов, как для абсолют-

ных, так и средних значений, по количеству необходимых операций преобразования в таком порядке: 1) AES, 2) ADE, 3) Калина, 4) Лабиринт, 5) Мухомор, 6) RSB. Очевидно, что порядок, в котором шифры выходят на асимптотику изменился. По расходам памяти шифры идут в таком порядке (для числа раундов меньше 5): 1) RSB 2) AES, 3) Мухомор, 4) Лабиринт, 5) ADE, 6) Калина. Следует отметить небольшие затраты памяти нашей реализации шифра RSB (в авторской реализации затраты памяти несравненно выше).

На рис. 4 приведены графики, показывающие влияние используемых в шифрах S-боксов на стойкость к дифференциальному криптоанализу и количество требуемых для ее обеспечения операций для каждого из рассматриваемых шифров в отдельности. Как видно из приведенных зависимостей, использование в шифрах S-боксов с улучшенными свойствами по нелинейности и автокорреляции позволяет выйти на асимптотику абсолютных и средних значений условных максимумов дифференциальных таблиц переходов, как правило, раньше, чем с использованием S-боксов с худшими свойствами.

Как показали проведенные эксперименты, это справедливо для всех рассмотренных шифров, кроме шифра Лабиринт, у которого асимптотическое значение максимумов достигается при том же числе раундов/операций, однако мы видим, что его дифференциальные свойства для предшествующих раундов несколько лучше при использовании улучшенных S-боксов.

Таблица 8

Структурный состав IT/FT-преобразований

Преобразование	Микрооперации				
	sum	**S-box**	**rol/ror**	**IMix**	**Всего**
Калина IT	$(L_B/32)\times3$				$12\times L_B/128$
Калина FT	$(L_B/32)\times2$	$(L_B/64)\times8\times3+1$			$56\times L_B/128+1$
Мухомор IT	$(L_B/32)\times3$				$12\times L_B/128$
Мухомор FT	$(L_B/32)\times2$				$8\times L_B/128$
Лабиринт IT	$(L_B/32)\times3$	$(L_B/64)\times8\times3+1$	$(L_B/64)\times3$	$(L_B/128)\times4+3$	$70\times L_B/128+4$
Лабиринт FT	$(L_B/32)\times2$	$(L_B/64)\times8\times3+1$	$(L_B/64)\times3$	$(L_B/128)\times4+3$	$66\times L_B/128+4$
AES IT	$(L_B/32)\times3$				$12\times L_B/128$
ADE IT	$(L_B/32)\times3$				$12\times L_B/128$

Таблица 9

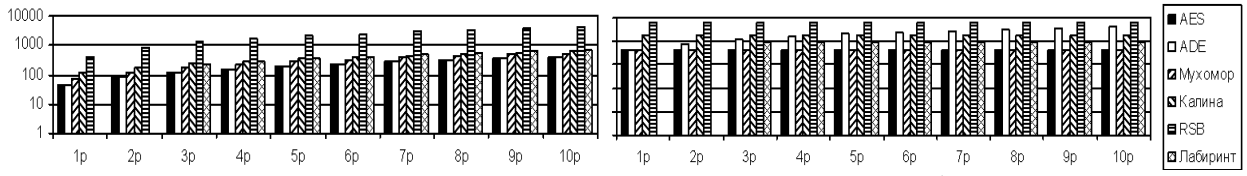
Вычислительные затраты шифров

#раундов	AES	Калина	Мухомор	ADE	Лабиринт	RSB
1	48	125	71	48	212	414
2	84	181	122	84	280	828
3	120	237	173	120	348	1242
4	156	293	224	156	416	1656
5	192	349	275	192	484	2070
6	228	405	326	228	552	2484
7	264	461	377	264	620	2898
8	300	517	428	300	688	3312
9	336	573	479	336	-	3726
10	393	629	530	393	-	4140
11	-	-	581	-	-	4554

Таблица 10

Затраты памяти шифров

#раундов	AES	Калина	Мухомор	ADE	Лабиринт	RSB
1	4096	18432	4096	4096	8448	256
2	4096	18432	4096	8192	8448	256
3	4096	18432	4096	12288	8448	256
4	4096	18432	4096	16384	8448	256
5	4096	18432	4096	20480	8448	256
6	4096	18432	4096	24576	8448	256
7	4096	18432	4096	28672	8448	256
8	4096	18432	4096	32768	8448	256
9	4096	18432	4096	36864	-	256
10	4352	18432	4096	41216	-	256
11	-	-	4096	-	-	256



а б

Рис. 3. Соотношение: число раундов (а) или количество памяти в байтах (б) – число операций

Выводы

В результате проведенных исследований получены следующие важные в прикладном значении результаты:

– по устойчивости к дифференциальному криптоанализу в зависимости от числа раундов преобразования, исследуемые шифры идут в следующем порядке: 1) Калина, 2) Лабиринт, 3) AES, 4) ADE, 5) Мухомор, 6) шифр Хейса, 7) RSB;

– по устойчивости к дифференциальному криптоанализу в зависимости от числа операций преобразований, исследуемые шифры идут в следующем порядке: 1) AES, 2) ADE, 3) Калина, 4) Лабиринт, 5) Мухомор, 6) RSB;

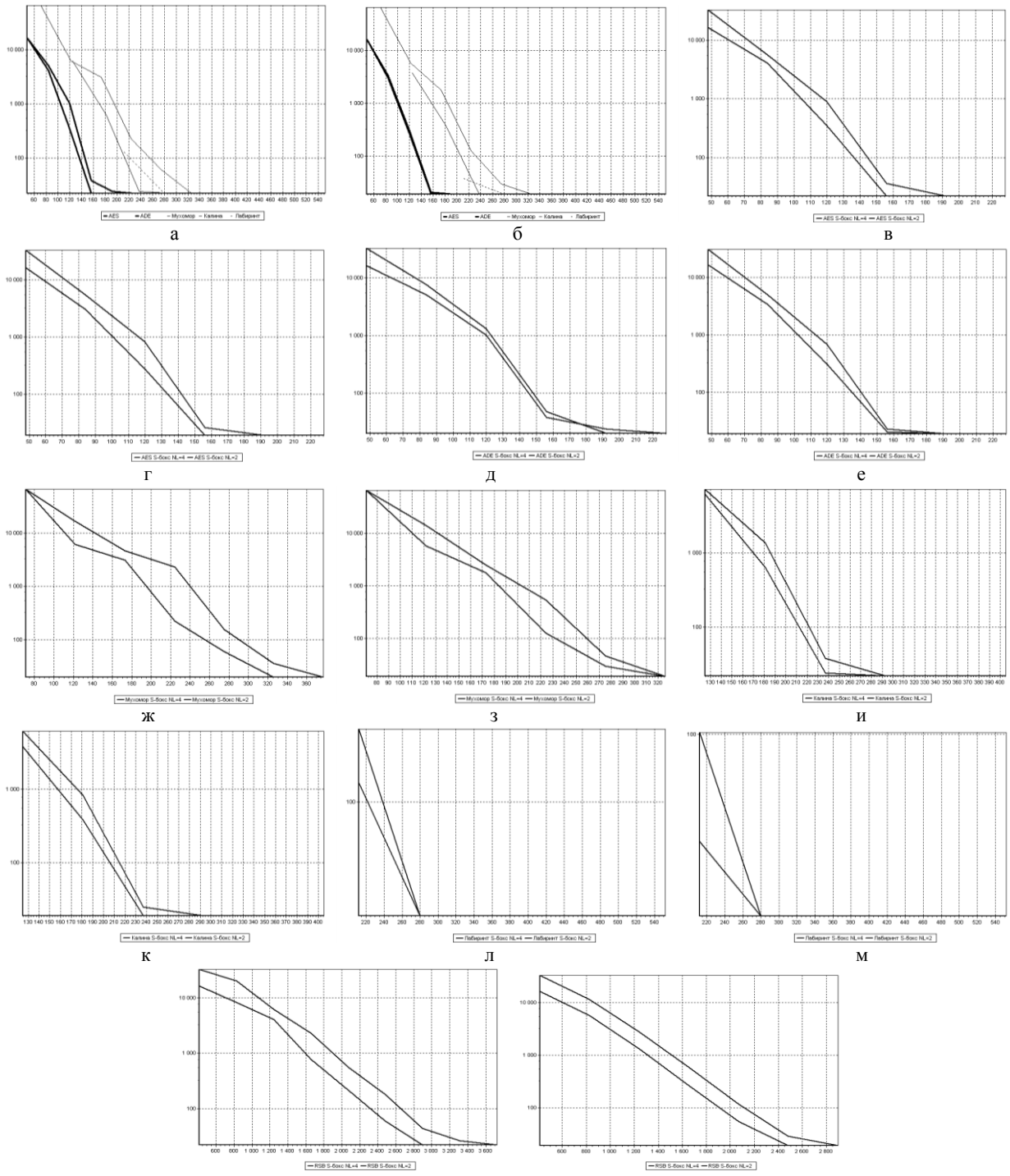


Рис. 4. Соотношение: абсолютный (а, в, д, ж, и, л, н) или средний (б, г, е, з, к, м, 0) максимум – число операций (а,б – S-бокс с NL=4; в, г – шифр AES; д,е – шифр ADE; ж,з – шифр Мухомор; и,к – шифр Калина; л, м – шифр Лабиринт; н,о – шифр RSB соответственно)

– шифры AES и ADE показали практически одинаковые результаты, однако шифр ADE требует больших затрат памяти;

– шифр Калина выходит на асимптотику раньше, чем шифр Лабиринт, однако он требует больших затрат памяти для своих преобразований (на первых раундах);

– худшим по эффективности (устойчивости к дифференциальному криптоанализу) при фиксированных вычислительных затратах оказался шифр RSB;

– по совокупности частных показателей наиболее рациональным решением следует, очевидно, считать шифр AES.

Наиболее примечателен последний вывод. Очевидно, что обеспечение требуемой стойкости к дифференциальному криптоанализу при меньшем числе раундов не всегда является рациональным. При выборе криптоалгоритма следует ориентироваться, прежде всего, на вычислительные затраты, которые требуется внести в качестве «платы» за реализацию шифра,

обеспечивающего требуемые показатели стойкости (напомним, что нами исследовалась устойчивость шифров лишь к дифференциальному криптоанализу).

Полученные результаты исследований о влиянии используемых в шифрах S-боксов на их эффективность свидетельствуют о том, что использование узлов замен с улучшенными свойствами по нелинейности и автокорреляции позволяет усилить дифференциальные свойства шифров, и выйти к асимптотическому показателю максимумов таблиц разностей раньше, чем с использованием S-боксов с худшими свойствами. Следовательно, разработка методов построения нелинейных узлов замен с улучшенными свойствами является одним из *перспективных направлений* для дальнейшего развития БСШ. Перспективным представляется также исследование эффективности поданных на конкурс шифров относительно других методов криптоанализа как в зависимости от числа раундов преобразования, так и в зависимости от числа операций и требуемых затрат памяти.

Список литературы

1. *Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] // Режим доступу : http://dstszi.gov.ua/dstszi/control/uk/publish/.*
2. *Горбенко І.Д. Перспективний блоковий симетричний шифр «КАЛИНА». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. - С. 195-208.*
3. *Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та ін. // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 147-157.*
4. *Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» / С.А. Головашич // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 230-240.*
5. *Белецкий А.Я. Семейство симметричных блочних RSB криптографических алгоритмов с динамически управляемыми параметрами шифрования / А.Я. Белецкий, А.А. Белецкий, А.А. Кузнецов // Електроніка та системи управління. – 2007. – № 1 (11). – С. 5-16.*
6. *Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. – Х.: ХНУРЭ. – 2007. – Т. 6, №2. – С. 241-249.*
7. *A Description of Baby Rijndael // ISU CprE/Math 533; NTU ST765-U. – 2003.*
8. *Raphael Chung-Wei Phan. Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students / Raphael Chung-Wei Phan // Cryptologia. – October 2002. – XXVI(4). – P. 283-306.*
9. *Raphael Chung-Wei Phan. Impossible Differential Cryptanalysis of Mini-AES / Raphael Chung-Wei Phan // Cryptologia. - October 2003. – XXVII(4). – P. 361-374.*
10. *Heys H.M. A Tutorial on Linear and Differential Cryptanalysis. / H.M. Heys // CRYPTOLOGIA. – 2002. – V. 26, N 3. – P. 189-221.*
11. *Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – Х.: ХНУРЭ, 2009. – Т. 8, № 3. – С. 252-257.*
12. *Долгов В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов, И.В. Лисицкая, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника.. – Х.: ХНУРЭ. – 2009. – Т.8, № 3. – С. 268 – 277.*
13. *O'Connor L.J. On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology / L.J. O'Connor // EUROCRIPT 93, Lecture Notes in Computer Science, T. Helleseth ed., Springer-Verlag. – 1994. – V. 795. – P. 360–370.*
14. *Олейников Р.В. Исследование дифференциальных свойств подстановок / Р.В. Олейников, И.В. Лисицкая, А.В. Широков, К.Е. Лисицкий // Компьютерные науки и технологии: сб. научн. тр. первой межд. НТК - Ч. І. – Б., 2009. – С. 59-63.*
15. *Головашин С.А. Анализ эффективности проектирования алгоритмов-участников конкурса БСШ Украины [Електронний ресурс] / С.А. Головашич // Х.: ООО КРИПТОМАШ, 2009. – С. 70. – Режим доступу до журн.: http://www.cryptomach.com/upload/ru/files/bc_design_ effectiveness.pdf.*
16. *Кузнецов А.А. Методика исследования эффективности нелинейных узлов замен симметричных криптографических средств защиты информации / А.А. Кузнецов, Ю.А. Избенко, И.В. Московченко // Збірник наукових праць ДонІЗТ. – Донецьк: ДонІЗТ. – 2008. – № 14. – С. 74-81.*

Поступила в редколлегию 24.05.2010

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ДОСЛІДЖЕННЯ ДИФЕРЕНЦІЙНИХ ВЛАСТИВОСТЕЙ БЛОКОВО-СИМЕТРИЧНИХ ШИФРІВ

Л.С. Сорока, О.О. Кузнецов, І.В. Московченко, С.О. Ісаєв

Розглядаються блоково-симетричні шифри, подані на відкритий конкурс по відбору кандидатів на національний стандарт блокового симетричного шифрування України. Досліджується ефективність міні-версій поданих на конкурс шифрів відносно диференційного криптоаналізу як в залежності від числа раундів перетворення, так і в залежності від числа операцій і необхідних затрат пам'яті. Оцінюється вплив властивостей застосовуємих нелінійних вузлів замін на диференційні характеристики блоково-симетричних шифрів.

Ключові слова: *шифр, диференціал, S-бокс, моделювання, криптоаналіз.*

RESEARCH OF DIFFERENTIAL PROPERTIES OF MINI-VERSIONS OF BLOCK SYMMETRIC CIPHERS

L.S. Soroka, A.A. Kuznetsov, I.V. Moskovchenko, S.A. Isaev

The block symmetric ciphers submitted to open tender for selection of candidates at the national standard for block symmetric encryption of Ukraine are considered. The effectiveness of the mini-versions of data on competition with respect to differential cryptanalysis of the cipher as a function of the number of rounds of pre-education, and depending on the number of transactions and the required cost of memory is investigated. The influence of properties applies the nonlinear nodes substitutions on the differential characteristics of block-symmetric ciphers are considered.

Keywords: *cipher, differential, S-box, simulation, cryptanalysis.*