УДК 336.717:004.78

Сорока Л.С., Кузнецов А.А., Исаев С.А.
(ХНУ им. Каразина)

ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ СВОЙСТВ МИНИ-ВЕРСИЙ БЛОЧНО-СИММЕТРИЧНЫХ ШИФРОВ

Постановка проблемы в общем виде и анализ литературы

Разработка и принятие национального стандарта Украины, устанавливающего параметры и основные правила блочного симметричного криптографического преобразования информации, является важной государственной задачей, непосредственно связанной с рядом отраслевых научно-технических программ и проектов. Об этом свидетельствует и проводимый в Украине конкурс блочно-симметричных шифров (БСШ), на который в качестве конкурсных предложений поданы следующие криптоалгоритмы: Калина, Мухомор, Лабиринт, RSB-32 и ADE [1 – 5]. Актуальной задачей является оценка эффективности представленных БСШ, обоснование выбора алгоритма-кандидата в виде рационального компромисса по вычислительной сложности и обеспечиваемой криптостойкости, на основании которого в дальнейшем может быть разработан национальный стандарт блочного симметричного шифрования Украины.

Одним из требований, предъявляемых к параметрам современных БСШ, является минимальная длина блока открытого текста и ключевых данных, которая должна составлять не меньше 128 бит [6]. Такие большие размеры блоков текста и ключевых данных гарантируют высокую вычислительную сложность для атак типа «грубой силы», однако это усложняет и процесс верификации существующих криптоалгоритмов, исследования их свойств и характеристик безопасности.

Одним из подходов по изучению и анализу алгоритмов БСШ является разработка и исследование уменьшенных моделей шифров. Именно этот подход и был положен в основу данной работы.

Проведенные исследования являются логическим продолжением полученных ранее результатов по оценке дифференциальных свойств мини-версий шифров [8]. Под мини-версией понимается шифр, который при сохранении математической структуры основных преобразований имеет меньшие, чем шифр-оригинал длины блоков данных и ключей [7]. Это достигается пропорциональным уменьшением соответствующих длин блоков данных и ключей исходного шифра.

Как и в предыдущей нашей работе [8], при проведении исследований рассматривались свойства мини-версий шифров, поданных на украинский конкурс (за исключением шифра RSB-32), а также американского стандарта шифрования AES [9]. Исследования состояли в построении таблиц линейных аппроксимаций, оценке максимальных значений отклонений и сравнении их с асимптотическим показателем среднего значения максимума отклонений для мини-версий шифров. При этом оценивалось влияние используемых блоков замен на требуемое число циклов зашифрования для выхода к асимптотическому значению. В ходе исследований использовались два различных типа S-блоков – один обладал заведомо лучшими показателями стойкости (по нелинейности и автокорреляции), чем другой. Так же, как и в [8], нами исследовалась эффективность шифров по обеспечению стойкости к линейному криптоанализу по требуемым вычислительным затратам.

Подробное описание мини-версий рассмотренных в работе шифров можно найти в работах [9 – 14], описание методики оценки вычислительных затрат шифров в работе [15], быстрый рекурсивный алгоритм построения линейных таблиц аппроксимаций – в работе [16].

Таким образом, ***целью данной статьи*** является анализ БСШ Калина, Мухомор, Лабиринт, ADE и AES, исследование эффективности их мини-версий к линейному криптоанализу как в зависимости от числа раундов преобразования, так и в зависимости от

числа операций и требуемых затрат памяти, оценка влияния свойств применяемых нелинейных узлов замен на линейные характеристики рассматриваемых криптоалгоритмов.

1. Линейные свойства БСШ

В статье [17] приводятся теоретические расчеты для оценки значения максимумов таблиц линейных аппроксимаций. На основании полученных расчетов предложен подход к сравнению эффективности БСШ в виде минимального числа циклов алгоритма, при котором реализуется асимптотический показатель среднего значения максимума отклонений [18]. Приведем основные обозначения, аналитические выражения и расчетные результаты из [17].

Положим, что $\pi: Z_2^n \to Z_2^n$ - биективное *n*–битным отображением, и пусть S_{2^n} – множество всех таких отображений. Для *n*–битного вектора $X \in Z_2^n$, пусть *X[i]* обозначает *i*-й бит *X*.

Таблица линейных аппроксимаций для π, обозначаемая LAT_π, является таблицей размера $2^n x 2^n$ и задается следующим соотношением:

$$LAT_\pi(\alpha,\beta) \stackrel{def}{=} \#\{X \mid X \in Z_2^n, \bigoplus_{i=1}^{n} X[i]\cdot\alpha[i] = \bigoplus_{i=1}^{n} \pi(X)[i]\cdot\beta[i]\}, \qquad (1)$$

где $\alpha,\beta \in Z_2^n$.

Таким образом, $LAT_\pi(\alpha,\beta)$ задает количество равенств линейной комбинации входных бит (задаваемых α) и линейной комбинации выходных бит (задаваемых β).

В линейном криптоанализе используют *нормализованную таблицу линейных аппроксимаций* $LAT_\pi^*(\alpha,\beta)$, значения ячеек в которой представляют собой разность действительного значений ячеек $LAT_\pi(\alpha,\beta)$ от числа 2^{n-1} (отклонение).

Нормализованная таблица линейных аппроксимаций $LAT_\pi^*(\alpha,\beta)$ задается:

$$LAT_\pi^*(\alpha,\beta) = \left|LAT_\pi(\alpha,\beta) - 2^{n-1}\right|. \qquad (2)$$

Пусть $E[\lambda(\pi,2k)]$ – оценка ожидаемого числа ячеек таблицы LAT_π^*, имеющих значение *2k*. При *k>0* имеем:

$$E[\lambda(\pi,2k)] = \frac{2\cdot(2^n-1)^2\cdot(2^{n-1}!)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2. \qquad (3)$$

Асимптотический показатель среднего значения максимального отклонения находится из решения уравнения:

$$\frac{2\cdot(2^n-1)^2\cdot(2^{n-1}!)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+k}^2 \approx 1. \qquad (4)$$

Решение данного уравнения можно искать переборным методом, ориентируясь на экспериментальные данные. Расчеты, выполненные в соответствии с соотношениями (3) и (4), представлены в табл. 1.

Таблица 1

Расчетные результаты

n	4		6		8		10		12		14		16	
E[λ(π,2k)]	2,23	0,03	3,408	0,47	1,49	0,49	1,28	0,70	1,18	0,85	1,07	0,89	1,07	0,98
$2k$	6	8	14	16	34	36	76	78	166	168	358	360	762	764

2. Методика исследований. Суть наших экспериментов состояла в том, что весь набор шифрующих преобразований для одного конкретного ключа для каждого мини-шифра рассматривался как одна большая случайная подстановка, свойства которой мы и исследовали. Мы определяли линейную характеристику, которая покрывает весь шифр.

Линейная характеристика мини-шифра как подстановки изменяется от раунда к раунду. Однако, как следует из [18] после некоторого числа раундов шифрующего преобразования линейная характеристика мини-шифра будет стремиться к линейной характеристике случайной подстановки.

Асимптотическое значение максимума таблицы линейных аппроксимаций рассчитано и приведено в табл. 1. Отношение линейных свойств мини-версий шифров к данному асимптотическому значению как раз и характеризует их устойчивость к линейному криптоанализу. Как следует из табл. 1, среднее значение максимума таблицы линейных аппроксимаций для $n = 16$ лежит в диапазоне от 762 до 764. Это и есть интересующая нас теоретическая оценка линейной характеристики случайной подстановки. Число раундов (а также число операций зашифрования) мини-версии 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 линейному криптоанализу.

При проведении исследований линейных свойств мини-версий шифров были взяты два типа S-блоков со свойствами $NL = 2$, $AC = 16$ (были взяты S- блоки шифра DES) и $NL = 4$, $AC = 8$ соответственно. Здесь NL – нелинейность, AC – автокорреляция [19].

Подробное описание мини-версий исследуемых шифров приводятся в работах [9 – 14], принципы отбора S-блоков для исследований описаны в нашей предыдущей работе, посвященной исследованию дифференциальных свойств мини-версий шифров [8]. Здесь же мы приведем только таблицы нелинейных узлов замен, участвовавших в вычислительном эксперименте (табл. 2).

Таблица 2

Таблицы замен S-блоков, использованных в мини-версиях шифров

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

Строки 1 – 15 представляют собой табличные представления S-блоков DES [20] со свойствами NL=2, AC=16, строки 16-31 – табличные представления улучшенных S-блоков со свойствами NL = 4, AC = 8 соответственно. В табл. 3 приведено соответствие строк табличных представлений S-блоков каждому мини-шифру, в которых они использовались

Таблица 3

Соответствие S-блоков мини-шифрам

Мини-шифр	Строки таблицы 3	
	Худший S-блок	Лучший S-блок
AES	1	16
ADE	1-15	16-30
Лабиринт	1	31
Калина	1-2	16-17
Мухомор	1	16

В рассматриваемых мини-версиях шифров используются 16-битные блоки данных, следовательно, таблицы линейных аппроксимаций имеют размер $2^{16} \times 2^{16}$. Таблица линейных аппроксимаций представляет собой полное перечисление всех линейных аппроксимаций получаемой подстановки мини-шифра. Каждая строка таблицы соответствует конкретному значению суммы входных бит, каждый столбец соответствует конкретному значению суммы выходных бит, а значения соответствующих ячеек таблицы соответствуют количеству выполнений линейных равенств, т.е. равенств вида сумма входных бит равна сумме выходных бит. Мы рассматриваем отклонения нормализованных таблиц, значения которых получаются путем вычитания из значений таблиц линейных аппроксимаций числа, равного половине всех возможных линейных выражений (т.е. в нашем случае $2^{16}/2 = 32768$). Число, представляющее сумму входных/выходных бит, при представлении в двоичном виде указывает на биты входных/выходных блоков, которые вовлечены в сумму.

Заметим, что для построения одной таблицы линейных аппроксимаций по формуле (1) для 16-ти битной подстановки необходимо перебрать 2^{16} значений α, для каждого из которых необходимо в свою очередь перебрать 2^{16} значений β, для которых в свою очередь необходимо перебрать 2^{16} значений X. Следовательно, для вычисления одной таблицы линейных аппроксимаций по формуле (1) необходимо произвести вычисления над $2^{16} \times 2^{16} \times 2^{16} = 2^{48}$ блоками данных, что вычислительно емко. Поэтому в наших экспериментах мы строили таблицы линейных аппроксимаций, используя быстрый рекурсивный алгоритм, описание которого можно найти в работе [16].

Заметим также, что в отличие от классического подхода, где изучаются линейные свойства S-блоков (не зависящие от значений ключевых битов), в рассматриваемом случае мини-шифр является ключезависимой подстановкой. Это значит, что интересующее нас максимальное значение отклонения, будет зависеть от ключа шифрования, и для полного представления линейных свойств мини-шифра необходимо выполнить эксперименты еще и для всего множества ключей, мощность которого для рассматриваемых в этой работе моделей мини-версий шифров составляет 2^{16}. Это приводит к необходимости выполнения очень большого объема вычислений.

В проводимых исследованиях мы оценивали показатели стойкости мини-версий шифров в среднестатистическом смысле. Следовательно, оценивая устойчивость шифров к атакам линейного криптоанализа, мы ориентировались на среднее по множеству ключей (ожидаемое) максимальное значение вероятности отклонения.

Таким образом, эксперимент проводился для ограниченного набора ключей. Соответствующие результаты рассматривались как выборка из генеральной совокупности. Для обработки результатов эксперимента и оценки их достоверности были использованы методы математической статистики и проверки гипотез.

Мы ограничились изучением статистических характеристик максимального значения отклонений (обозначим его Δy_i), а также сравнили полученные результаты для всех рассматриваемых мини-шифров.

В качестве основных критериев и показателей, по которым проводилось сравнение экспериментальных данных (максимумов отклонений Δy_i), характеризирующих полученную таблицу линейных аппроксимаций, использовались:

- максимальное значение максимумов отклонений для определенного значения ключа (абсолютный максимум отклонений):

$$\Delta y_{\max} = \max_{1 \le i \le 2^{16}-1} \{\Delta y_i\};$$

- математическое ожидание максимумов отклонений для определенного значения ключа (средний максимум отклонений):

$$m_y = \frac{1}{2^{16}-1} \sum_{i=1}^{2^{16}-1} \Delta y_i ;$$

- дисперсия, характеризующая рассеивание значений максимумов отклонений относительно его математического ожидания:

$$d_y = \frac{1}{2^{16}-1} \sum_{i=1}^{2^{16}-1} \left(\Delta y_i - m_y\right)^2 .$$

Естественной оценкой для математического ожидания m случайной величины X является среднее арифметическое ее наблюдаемых значений X_i (или статистическое среднее) [21]:

$$\tilde{m} = \frac{1}{N} \sum_{i=1}^{N} X_i ,$$

где N – количество реализаций.

Оценка дисперсии определяется выражением:

$$\tilde{D} = \frac{1}{N-1} \sum_{i=1}^{N} (X_i - \tilde{m})^2 .$$

После обработки опытных данных по выборке из генеральной совокупности ключей, мы определили следующие статистические характеристики:

– M_y – математическое ожидание максимумов отклонений (среднего максимума отклонений);

– D_y – дисперсия максимумов отклонений (среднего максимума отклонений);

– $M_{y\max}$ – математическое ожидание максимального значения максимумов отклонений (абсолютного максимума отклонений);

– $D_{y_{\max}}$ – дисперсия максимального значения максимумов отклонений (абсолютного максимума отклонений).

Количество реализаций N = 100 (из 65535) было выбрано исходя из положений центральной предельной теоремы теории вероятностей: при больших значениях N среднее арифметическое будет иметь распределение, близкое к нормальному [21] с математическим ожиданием:

$$M[\tilde{m}] \approx \tilde{m}$$

и средним квадратическим отклонением:

$$\sigma[\tilde{m}] \approx \frac{\sigma}{\sqrt{N}},$$

где σ – среднее квадратическое отклонение оцениваемого параметра.

При этом вероятность того, что оценка $\tilde{m}$ отклоняется от своего математического ожидания меньше, чем на ε (доверительная вероятность), равна [21]:

$$P(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right),$$

где – $\Phi(x)$ функция Лапласа, определяемая выражением:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt. \qquad (5)$$

Для заданной доверительной вероятности P доверительный интервал определяется следующим образом:

$$\tilde{m} - t_\rho \cdot \sigma[\tilde{m}] < m < \tilde{m} + t_\rho \cdot \sigma[\tilde{m}], \qquad (6)$$

где t_ρ – корень уравнения $2\Phi(t_\rho) = P$.

3. Результаты исследований. В результате проведенных исследований было построено по 100 таблиц 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. Определялись следующие показатели:

– *максимальное* по множеству из 100 случайно выбранных ключей шифрования (по множеству таблиц) значение *абсолютного* максимума отклонений таблиц линейных аппроксимаций мини-шифров;

– *среднее* по множеству из 100 случайно выбранных ключей шифрования (по множеству таблиц) значение *абсолютных* максимумов отклонений таблиц линейных аппроксимаций мини-шифров;

– среднее по множеству из 100 случайно выбранных ключей шифрования (по множеству таблиц) значение *средних* максимумов отклонений таблиц линейных аппроксимаций мини-шифров.

Для определения доверительного интервала полученных оценок использовалось выражение (6); мы задались уровнем значимости α =0,01, что соответствует доверительной вероятности $P = (1 - \alpha) \cdot 100\% = 99\%$. При этом определение значения функции Лапласа (5) производилось согласно [21]. Выбранная высокая доверительная вероятность (99%) позволяет утверждать об адекватности сравнения полученных результатов для мини-шифров и соответствия их статистическим свойствам всей генеральной совокупности данных.

Результаты статистических исследований линейных свойств мини-шифров приведены в табл. 4-6.

Заметим, что для мини-шифра Лабиринт начальное и конечное преобразования IT и FT считались как отдельные раунды преобразования.

В таблицах серым цветом выделены те ячейки, для значений которых достигаются асимптотические значения отклонений линейных таблиц мини-шифров. Как видно из приведенных результатов, использование улучшенных S-блоков по нелинейности и автокорреляции позволяет несколько улучшить линейные показатели шифров, а для некоторых мини-шифров позволяет выйти к асимптотическому показателю отклонений на один раунд раньше, чем с использованием худших S-блоков (мини-шифры AES, ADE, Калина).

Таблица 4

Абсолютный максимум

R	Mini-AES		Mini-ADE		Mini-Labyrinth		Mini-Kalina		Mini-Muhomor	
	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4	NL=2	NL=4
1	24576	16384	24576	16384	-	-	18432	12288	18432	12288
2	10240	10240	14336	12288	-	-	7808	4480	18432	9728
3	4736	4352	6400	4352	2082	1444	2000	936	12496	8396
4	1268	940	1544	932	884	914	890	912	12581	8450
5	912	900	906	896	902	902	898	900	12746	8667
6	890	922	898	880	900	906	896	912	12609	8696

Также отметим, что для мини-шифра Мухомор полученные результаты не дали адекватной оценки оригинального шифра Мухомор. Как видно из приведенных в таблицах результатов, использованная мини-версия шифра Мухомор не позволила выйти к асимптотическим линейным показателям таблиц аппроксимаций. Это объясняется трудностями, с которыми столкнулись авторы шифра при переносе шифрующих операций преобразования со 128-битной размерности на 16-битную. В результате, некоторые операции перенести с шифра-оригинала в мини-шифр не удалось. По этой причине мы не привели сравнения мини-шифра Мухомор с остальными мини-шифрами, которые рассматривались в этой работе.

Анализ полученных результатов показывает, что рассматриваемые мини-шифры выходят на асимптотический показатель среднего максимума отклонений в таком порядке: 1) Калина, 2) Лабиринт, 3) AES и ADE. Аналогичный порядок сохраняется и для абсолютного, и для среднего абсолютного максимума.

Сравнивая полученные экспериментальные результаты с теоретическими расчетами для среднего максимума отклонений, можно сказать, что все рассматриваемые мини-шифры подходят близко к асимптотической границе, однако не достигают ее (теоретический максимум – около 760, экспериментальный – около 820). Это говорит о том, что мини-шифры по своим характеристикам близки к случайным подстановкам, однако полное соответствие между ними не достигается.

Следует отметить, что число операций для реализации раунда преобразований одного шифра может существенно отличаться от числа операций для реализации раунда другого. То же относится и к затратам памяти. Для адекватного сравнения полученных результатов, используя методику оценки ресурсоемкости шифров из работы [15] и некоторые результаты из [8], мы оценили вычислительную эффективность рассматриваемых мини-версий БСШ.

В табл. 7 представлены оценки требуемых вычислительных ресурсов (количество элементарных операций) рассматриваемых мини-версий БСШ в соответствии с работой [8]. Серым цветом выделены ячейки со значениями количества операций, при которых мини-шифр выходит к асимптотическому значению отклонений.

Таблица 7

Вычислительные затраты шифров

#раундов	AES	Калина	ADE	Лабиринт
1	48	125	48	212
2	84	181	84	280
3	120	237	120	348
4	156	293	156	416
5	192	349	192	484
6	228	405	228	552
7	264	461	264	620
8	300	517	300	688
9	336	573	336	-
10	393	629	393	-

Как видно из приведенных данных в табл. 7, рассматриваемые шифры выходят к своему асимптотическому показателю максимумов, как абсолютных, так и средних значений, по количеству необходимых операций преобразования в таком порядке: 1) AES и ADE, 2) Калина, 3) Лабиринт. Очевидно, что порядок, в котором мини-шифры выходят на асимптотику изменился: алгоритмы AES и ADE требуют наименьших вычислительных

ресурсов в качестве «платы» за реализацию асимптотических свойств случайной подстановки.

Выводы

Полученные результаты исследований хорошо согласуются с полученными ранее дифференциальными результатами для мини-шифров [8], а именно:

- по устойчивости к линейному криптоанализу в зависимости от числа раундов преобразования, исследуемые мини-версии шифров идут в следующем порядке: 1) Калина, 2) Лабиринт, 3) AES и ADE;
- по устойчивости к линейному криптоанализу в зависимости от числа операций преобразований, исследуемые мини-версии шифров идут в следующем порядке: 1) AES и ADE, 2) Калина, 3) Лабиринт;
- по совокупности частных показателей наиболее рациональным решением следует, очевидно, считать мини-версию шифра AES.

Последний из выводов является наиболее примечательным. Очевидно, что обеспечение требуемой стойкости к линейному криптоанализу при меньшем числе раундов (например, для мини-шифров Калина и Лабиринт) 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.

Полученные результаты исследований о влиянии используемых S-блоков на эффективность шифров свидетельствуют о том, что использование узлов замен с улучшенными по нелинейности и автокорреляции свойствами позволяет усилить линейные свойства шифров, а в некоторых случаях и выйти к асимптотическому показателю максимумов таблиц линейных аппроксимаций раньше, чем с использованием S-блоков с худшими свойствами.

Заметим, что мини-версии шифров AES и ADE показывают практически одинаковые показатели стойкости относительно статистических методов криптоанализа, а именно – дифференциального и линейного. Именно к этому и стремились авторы шифра ADE (который представляет собой, по сути, шифр AES с динамически изменяемыми блоками замен и параметрами линейных матриц рассеивания), т.е. к сохранению в шифре ADE хороших статистических свойств шифра-оригинала, но и к увеличению его стойкости относительно алгебраического криптоанализа.

Следует отметить, что на текущий момент нет теоретической и экспериментальной базы, подтверждающей адекватность исследуемых мини-версий шифров их полным аналогам. Поэтому ***перспективным направлением дальнейших исследований*** представляется теоретическое и экспериментальное обоснование адекватности предлагаемой методики исследований, основанной на использовании мини-версий шифров.

Список литературы

1. 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.

2. 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.

3. Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» / С.А. Головашич // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 230-240.

4. Белецкий А.Я., Белецкий А.А., Кузнецов А.А. Семейство симметричных блочних RSB криптографических алгоритмов с динамически управляемыми параметрами шифрования // Електроніка та системи управління. - 2007. - № 1 (11). - С. 5-16.

5. Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. – Харьков: ХНУРЭ. – 2007. – Том 6, №2. – С.241 – 249.

6. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] // Режим доступу : http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=48383.

7. 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.

8. Сорока Л.С. Исследование дифференциальных свойств блочно-симметричных шифров. / Л.С. Сорока, А.А. Кузнецов, И.В. Московченко, С.А. Исаев // Системи обробки інформації. – Харьков: ХУ ПС. – 2010. – Випуск 6(87). – С. 286-294.

9. A Description of Baby Rijndael // ISU CprE/Math 533; NTU ST765-U. – 2003.

10. 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.

11. 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.

12. Долгов В.И., Олейников Р.В., Лисицкая И.В., Дроботько Е.В., Григорьев А.В. Криптографические свойства уменьшенной версии шифра «Мухомор». Email: bit@kture.kharkov.ua.

13. Долгов В.И., Олейников Р.В., Лисицкая И.В., Дроботько Е.В., Григорьев А.В. Криптографические свойства уменьшенной версии шифра «Калина». Email: bit@kture.kharkov.ua.

14. Долгов В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра "Лабиринт". / В.И. Долгов, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // Прикладная радиоэлектроника. – Х.: ХНУРЭ. – 2009. – Т.8, № 3. – С. 283-289.

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. Krzysztof Chmiel. On Differential and Linear Approximation of S-box Functions / Chmiel Krzysztof // Biometrics, computer security systems and artificial intelligence applications. – Springer Science+Business Media, LLC. – 2006. – P. 111-120.

17. Luke O'Connor. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts.Edu.au, 1995.

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

19. 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.

20. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — Пер. с англ.: М.: Издательство ТРИУМФ, 2002 — 816 с.

21. Вентцель Е.С. Теория вероятностей. – М.: Государственное издательство физико-математической литературы, 1958 – 564 с.

Рецензент Скрипник Л.В.
Поступила 16.02.2011