УДК 621.3.06

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ПОКАЗАТЕЛЕЙ УМЕНЬШЕННЫХ МОДЕЛЕЙ ШИФРОВ ГОСТ И DES

В.И. ДОЛГОВ, Я.А. МАКАРЧУК, А.В. ГРИГОРЬЕВ, Е.В. ДРОБОТЬКО

Для обоснования правомерности оценки свойств и криптографических показателей блочных симметричных шифров на основе изучения и сопоставления свойств их уменьшенных моделей приводятся результаты анализа свойств и криптографических показателей уменьшенных моделей хорошо известных и детально изученных шифров DES и ГОСТ. На основе полученных результатов делается вывод о том, что уменьшенные модели шифров DES и ГОСТ практически повторяют характеристики своих больших прототипов.

Ключевые слова: уменьшенная версия шифра, сжимающая перестановка, циклические свойства, полный дифференциал.

ВВЕДЕНИЕ

Одним из важных вопросов, решаемых в процессе разработки ускоренной методики криптоанализа современных блочных шифров, предложенной в работах [1, 2], остается адекватность использования уменьшенных моделей вместо их больших прототипов. Исследования ряда таких уменьшенных моделей для шифров Rijndael, а также шифров, представленных на украинский конкурс по выбору претендента на национальный стандарт блочного симметричного шифрования (Лабиринт, ADE, Калина, Мухомор), показали, что эти шифры допускают масштабирование, при котором свойства больших шифров переносятся на их малые версии. Привести строгое обоснование соответствия малых моделей большим все еще представляет известные трудности в части определения и оценки степени “эквивалентности” замены операций над “большими” блоками соответствующими операциями над “малыми” блоками. Естественным в таких условиях представляется стремление получить необходимые аргументы в пользу развиваемого подхода не только на уровне сопоставительного анализа свойств и показателей малых моделей современных шифров, но и на уровне сравнения показателей уменьшенных моделей возможно большего числа апробированных решений по построению шифров, по применению которых уже накоплен достаточно убедительный материал. Эта работа посвящена развитию этой точки зрения. Внимание в ней сосредотачивается на исследовании свойств и показателей уменьшенных моделей, хорошо известных как в историческом, так и в практическом отношении, шифров DES и ГОСТ.

1. МИНИ ВЕРСИЯ ШИФРА ГОСТ

Алгоритм baby-Gost является уменьшенным прототипом российского стандарта блочного симметричного шифрования ГОСТ-28147-89. Входной размер блока 16 бит, ключ 32 бита.

В шифре ГОСТ 28147-89 повторена полностью последовательность его операций (16-битный вход разбивается на левый (L) и правый (R) полублоки по 8 бит, которые подаются на основное шифрующее преобразование – цепь Фейстеля: правый полублок R подается на вход цикловой функции, выход которой объединяется с левым полублоком L путем побитного сложения по модулю 2), только число блоков (строк) таблицы подстановок уменьшено соответственно до двух. В качестве ключей использованы 16-битные случайно порождаемые строки, которые в соответствии с построением алгоритма шифрования были по-байтово распределены (для восьмицикловой версии) между циклами из восьми преобразований в порядке следования байтов 1, 2, 3, 4, 1, 2, 3, 4, отражающем в определенной мере реальную структуру распределения битов мастер-ключа шифра. Соответственно в этой усеченной версии шифра восьмибитовый подключ вводился в цикловую функцию с помощью операции сложения по модулю 28, а циклический сдвиг результата подстановок выполнялся на 5 позиций. При разработке программной реализации была предусмотрена возможность изменения числа циклов шифрования.

Цикловое преобразование. На вход циклового преобразования подаются 8-ми битный подключ и полублок данных. Сначала выполняется сложение подключа по модулю 28 с полублоком данных.

После этого результат разбивается на два 4-х битных значения, которые подаются на входы S блоков. Выходные значения S-блоков “склеиваются” (объединяются) и циклически сдвигаются на 5 бит влево. Поученный результат и является выходом циклового преобразования.

S-box. В цикловом преобразовании используются 2 блока замены – первые две строки стандартного блока замены ГОСТ Р 34.11-94.

Общий алгоритм шифрования. Сначала входной блок разбивается на левую L и правую R части по 8 бит каждая. Затем выполняется 8 циклов зашифрования. На каждом цикле на вход циклового преобразования подается часть ключа (8 бит) и левый полублок на 1, 3, 5, 7 цикле, правый – на 2, 4, 6, 8, после чего полублоки меняются местами. На последнем цикле полублоки местами не меняются.

Выходное значение цикловой функции проходит традиционное для схемы Фейстеля сложение по модулю два с левым полублоком входных данных в результате чего формируются полублоки входа в очередной цикл.

После выполнения всех циклов алгоритма, полублоки на выходе последнего цикла объединяются ("склеиваются"), и выходной 16-битный блок является результатом работы алгоритма.

Для генерации подключей используются различные схемы разворачивания исходного 32-битного ключа, зависящие от количества циклов шифра:

1. Для 4-цикловой версии 32-битный ключ разбивается на 4-е 8-битных подблока $K_1 \ldots K_4$, которые используются в алгоритме в прямом порядке.

2. Для 6-цикловой версии 32-битный ключ разбивается на 4-е 8-битных подблока $K_1 \ldots K_4$, которые используются в следующем порядке: K_1, K_2, K_3, K_4, K_1, K_2.

3. Для 8-цикловой версии 32-битный ключ разбивается на 4-е 8-битных подблока $K_1 \ldots K_4$, которые используются в следующем порядке: K_1, K_2, K_3, K_4, K_1, K_2, K_3, K_4.

4. Для 10-цикловой версии 32-битный ключ разбивается на 4 8-битных подблока $K_1 \ldots K_4$, которые используются в следующем порядке: K_1, K_2, K_3, K_4, K_1, K_2, K_3, K_4, K_1, K_2.

5. Для 12-цикловой версии 32-битный ключ разбивается на 4 8-битных подблока $K_1 \ldots K_4$, которые используются в следующем порядке: K_1, K_2, K_3, K_4, K_1, K_2, K_3, K_4, K_4, K_3, K_2, K_1.

Расшифрование выполняется так же, как и зашифрование, но порядок использования подключей K_i. меняется на обратный.

2. МИНИ ВЕРСИЯ ШИФРА DES

Мини версия шифра DES также взята, по возможности, повторяющей в соответствующем масштабе операции оригинальной разработки (FIPS 46-3).

Входными данным алгоритма являются блок текста и ключ длиной по 16 бит.

Алгоритм шифрования. представленный на рисунке 1, как известно, состоит из следующих процедур:

– начальная перестановка IP;

– цепь Фейстеля с функцией усложнения *f*;

– конечная перестановка IP^{-1}.

Процедура шифрования состоит из трёх шагов:

1. Исходный блок данных P (длиной 16 бит) обрабатывается начальным (IP) преобразованием.

2. Результат 1-го шага разбивается на два полублока длиной по 8 бит: левый *L* («старший») и правый *R* («младший»). Полученная пара полублоков преобразуется на 16 итерациях цепи Фейстеля. Все итерации полностью идентичны и построены на базе общего преобразования – *f*-функции, управляемой ключом итерации K_i.

3. Два полублока *L* и *R*, полученные в результате итеративного преобразования, меняются местами и обрабатываются конечным (IP^{-1}) преобразованием. Полученный после FT преобразования двоичный вектор C (длиной 16 бит) является результирующим блоком («криптограммой»).

Начальная перестановка выполняется ещё до 1 этапа. Биты входного блока выставляются в выходной блок в соответствии с табл. 1. Так, 14-й бит входного блока становится на место 1-го бита выходного блока, 10й бит – на 2-е и т.д.

Таблица 1

Начальная перестановка

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
13	9	5	1	15	11	7	3	12	8	4	0	14	10	6	2

Конечная перестановка, выполняющая преобразование обратное начальной, приведена в табл. 2.

Таблица 2

Конечная перестановка

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	3	15	7	10	2	14	6	9	1	13	5	8	0	12	4

16-битный выход начальной перестановки разбивается на левый (*L*) и правый (*R*) блоки по 8 бит, которые подаются на основное шифрующее преобразование – цепь Фейстеля.

Цикловая функция усложнения, полностью повторяющая по конструкции оригинальную разработку, в качестве параметров принимает блок длиной 8 бит и цикловый (раундовый) ключ длиной 12 бит.

Функция состоит из процедуры расширения блока (с 8 до 12 бит), побитового сложения с ключом, подстановочного и перестановочного преобразований.

Функция расширения (E). Биты входного блока выставляются в выходной блок в соответствии с табл. 3. Так 8й бит входного блока, становится на место 1го бита в выходного блока, 1й бит – на 2е и т.д.

Таблица 3

Функция расширения (E)

7	0	1	2	3	4
3	4	5	6	7	1

S блоки для подстановочного преобразования взяты из оригинальной версии шифра. В уменьшенной версии, используется только два 6-ти битовых S блока.

S_3

10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1
13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

S_4

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

Процедура перестановки (P). Данная процедура принимает на вход 8 битовый выход двух S блоков и осуществляет битовую перестановку, показанную в табл. 4:

Таблица 4

Битовая перестановка P

0	1	2	3	4	5	6	7
4	5	0	1	6	7	2	3

Так 4-й бит входа, становится 1-м битом выходного блока, 5-й бит – 6-м и т.д.

Схема разворачивания ключей состоит из сжимающей перестановки PC1, которая представлена в табл. 5

Таблица 5

Сжимающая перестановка PC1 (16 →14)

0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	12	8	4	0	11	3	14	10	6	2	13	9	5

После сжимающего преобразования полученный 14-битный ключ делится на 2-е 7-битных половины. Затем над полученными половинами выполняется побитовый циклический сдвиг влево на один или два бита в зависимости от номера цикла [см. табл. 6].

Таблица 6

Число циклических сдвигов влево

№ цикла	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Результат циклического сдвига объединяется в 14-битовое слово и подаётся на вход второй сжимающей перестановка PC2 (табл. 7), выходом которой является 12-битовый цикловый подключ.

Таблица 7

Сжимающая перестановка PC2 (14→12)

0	1	2	3	4	5	6	7	8	9	10	11
1	12	4	0	11	3	14	10	6	13	9	5

3. ЦИКЛИЧЕСКИЕ СВОЙСТВА ШИФРОВ

Для исследования комбинаторных свойств шифров ГОСТ и DES использовалась методика, развитая в работе [3].

В этой работе мы наряду с циклическими свойствами выполнили также исследование (оценку) законов распределения инверсий и возрастаний.

Результаты выполненного вычислительного эксперимента по определению циклических свойств иллюстрируют табл. 8 и рис. 1.

Таблица 8

Циклические свойства малых версий шифров ГОСТ, DES и Rijndael

Число циклов	Baby-GOST		Baby-DES		Baby-Rijndael	
	Число подстановок	Расчетное значение вероятности P_k	Число подстановок	Расчетное значение вероятности P_k	Число подстановок	Расчетное значение вероятности P_k
2	20	0,00031	3	0,000183	18	0,00027
4	484	0,00739	154	0,00939	499	0,00761
6	3328	0,05078	799	0,04877	3255	0,04967
8	9600	0,14648	2361	0,15611	9436	0,14398
10	15256	0,23279	3853	0,235168	15429	0,23543
12	15672	0,23914	3925	0,239563	15963	0,24358
14	11344	0,1731	2938	0,179321	11580	0,1767
16	6024	0,09192	1519	0,09271	5956	0,09088
18	2328	0,03552	585	0,03570	2411	0,03679
20	768	0,01172	196	0,1196	774	0,01181
22	160	0,00244	37	0,002258	174	0,00266
24	32	0,00049	10	0,00061	35	0,00053
26	8	0,00012	0	0	6	0,00009
128	8	0,00012	0	0	0	0
130	52	0,00079	0	0	0	0
132	52	0,00079	0	0	0	0
134	54	0,00082	0	0	0	0
136	48	0,00073	0	0	0	0
138	22	0,00034	0	0	0	0
140	14	0,00021	0	0	0	0
142	2	0,00003	0	0	0	0
144	4	0,00006	0	0	0	0
32896	256	0,00391	4	0,000244	0	0

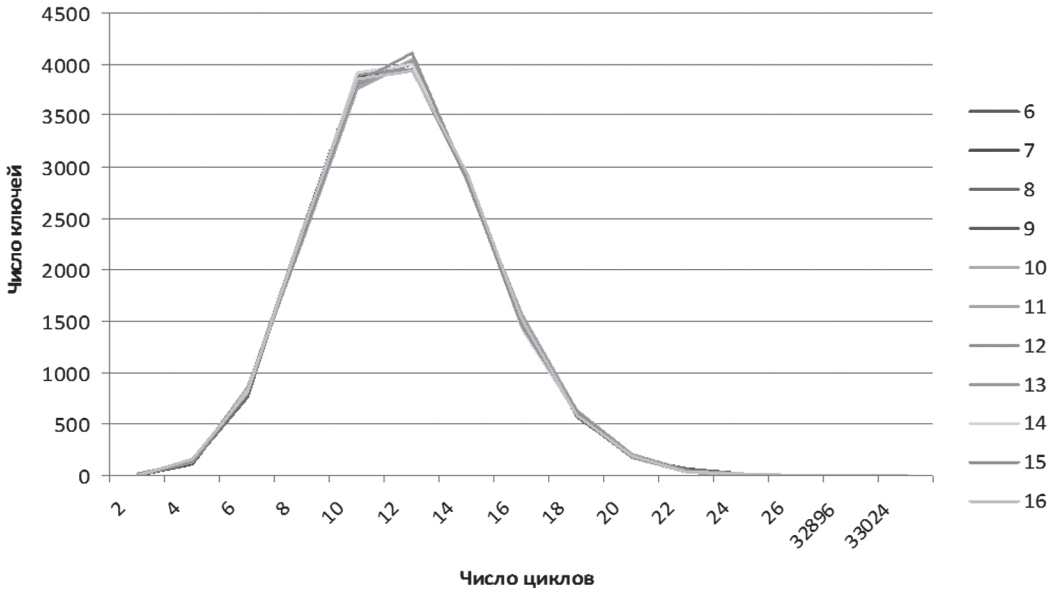

Рис. 1. Циклические свойства шифра baby-DES при разном числе циклов

Как следует из представленных результатов, рассмотренные малые версии шифров подтверждают с достаточно высокой точностью по комбинаторным показателям известные свойства случайных подстановок, причем явно просматривается очень слабая зависимость комбинаторных показателей от числа циклов, использованных при построении шифрующего преобразования. Малые модели подтверждают свойства своих больших прототипов.

В частности система введения цикловых подключей в шифре baby-ГОСТ и в маленькой версии подтверждает наличие слабых ключей (таких ключей в шифре ГОСТ половина от общего множества, и это ключи, состоящие из двух идентичных половинок). Число циклов для таких ключей равно 32896 (256 циклов единичной длины и 32640 длины два). Повторное зашифрование на таких ключах приводит к расшифрованию текстов (естественно, что тексты, отличающиеся только первым байтом, оказываются для таких ключей нешифруемыми).

Слабые ключи такого же типа присутствуют и в шифре DES, только их четыре, что также хорошо согласуется с известными данными [4]. Это инверсные ключи K_i^*, для которых выполняется условие $K_i^* = K_{17-i}$ (это для полной версии шифра), но они имеют аналоги и в уменьшенной версии.

4. ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА ШИФРОВ

Результаты исследования дифференциальных свойств шифра ГОСТ представлены в табл. 9.

В табл. 10 представлены данные анализа дифференциальных свойств шифра DES, а также других шифров, рассматриваемых на украинском конкурсе.

Как следует из результатов, представленных в табл. 9, шифр ГОСТ приходит к асимптотическим значениям дифференциальных показателей при 9-10 циклах шифрования. Заметим, что этот результат хорошо согласуется с нашими экспериментами по изучению лавинного эффекта большой версии шифра [5, 6]. В свое время было установлено, что шифр ГОСТ имеет глубину лавинного эффекта равную 9-ти циклам. Соответствующие данные по шифру DES приводят к выводу, что для него асимптотическое значение максимума полного дифференциала наступает при 7-ми циклах (по известным данным [Шнаер] и нашим экспериментам глубина лавинного эффекта для шифра DES составляет 5-ть циклов).

5. ЛИНЕЙНЫЕ СВОЙСТВА ШИФРОВ

Результаты исследования линейных свойств шифра ГОСТ иллюстрируют табл. 11. Как видно из представленных данных, они относятся к отдельному (фиксированному) значению пары масок вход-выход: Mask A = de51, Mask B = 9bc7. Здесь использовано свойство закона распределения смещений таблицы линейных аппроксимаций, заключающееся в независимости (а точнее, в слабой зависимости) закона распределения смещений таблицы линейных аппроксимаций $LAT_\pi^*(\alpha,\beta)$ от значений пары масок α,β, для которых он определен [7, 8].

В табл. 12 представлены значения максимумов смещений LAT, полученные для разных фиксированных значений пар масок, выбранных случайно. Видно, что значения максимумов смещений таблиц LAT для шифров ГОСТ и DES являются достаточно близкими друг к другу и хорошо согласуются с результатами, следующими из теоретических расчетов [9].

На рис. 2 представлены несколько в ином изображении линейные свойства шифра DES. Здесь уже приведено семейство (множество) законов распределения смещений таблицы линейных аппроксимаций $LAT_\pi^*(\alpha,\beta)$, вычисленных

Таблица 9

Дифференциальные свойства шифра ГОСТ

Cycles: 4 Key Expansion: 0 1 2 3 KEY: 89 e7 cb43	Cycles: 6 Key Expansion: 0 1 2 3 0 1 KEY: 89 e7 cb 43	Cycles: 8 Key Expansion: 0 1 2 3 0 1 2 3 KEY: 89 e7 cb 43	Cycles: 10 Key Expansion: 0 1 2 3 0 1 2 3 0 1 KEY: 89 e7 cb 43	Cycles: 12 Key Expansion: 0 1 2 3 0 1 2 3 3 2 1 0 KEY: 89 e7 cb 43
#2: 1122601344 #4: 331369798 #6: 77742211 #8: 19814042 #10: 4723044 #12: 1611350 #14: 520212 #16: 375091 . . . #1476: 1 #1500: 1 #1596: 1 #2048: 1 #2484: 1 #2688: 2	#2: 1294452922 #4: 325890171 #6: 55603179 #8: 7283017 #10: 811089 #12: 95427 #14: 20876 #16: 10177 . . . #302: 2 #330: 1 #336: 1 #372: 1 #374: 1 #408: 1	#2: 1301957485 #4: 325620217 #6: 54368219 #8: 6823824 #10: 687733 #12: 59514 #14: 5301 . . . #62: 1 #64: 3 #66: 1 #76: 2 #80: 1 #82: 1 #90: 1	#2: 1302414806 #4: 325648076 #6: 54280774 #8: 6783192 #10: 678604 #12: 56844 #14: 4061 #16: 260 #18: 20 #20: 5 #22: 1	#2: 1302542964 #4: 325616922 #6: 54261128 #8: 6781276 #10: 679189 #12: 56481 #14: 4081 #16: 254 #18: 16 #20: 1

Таблица 10

Зависимость значений максимумов полных дифференциалов
от числа циклов для мини шифров

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
ГОСТ			2688		408		90
DES	12288	3584	334,4	123,3	30,2	19,2	19,6

Таблица 11

Линейные свойства шифра ГОСТ

Cycles: 6 Key Expansion: 0 1 2 3 0 1 Mask A = de51 Mask B = 9bc7 KEYS: 2^16	Cycles: 8 Key Expansion: 0 1 2 3 0 1 2 3 Mask A = de51 Mask B = 9bc7 KEYS: 2^16	Cycles: 10 Key Expansion: 0 1 2 3 0 1 2 3 0 1 Mask A = de51 Mask B = 9bc7 KEYS: 2^16	Cycles: 12 Key Expansion: 0 1 2 3 0 1 2 3 3 2 1 0 Mask A = de51 Mask B = 9bc7 KEYS: 2^16
#2: 907 #4: 909 #6: 890 #8: 896 #10: 867 #12: 872 #14: 867 #16: 862 #18: 850 #20: 889 . . . #558: 1 #562: 1 #566: 1 #618: 1 #644: 1 #756: 1	#2: 865 #4: 853 #6: 840 #8: 875 #10: 839 #12: 833 #14: 821 #16: 771 #18: 821 . . . #490: 1 #494: 1 #498: 1 #508: 1 #512: 1 #588: 1	#2: 873 #4: 825 #6: 770 #8: 781 #10: 778 #12: 797 #14: 803 #16: 765 #18: 802 . . . #544: 1 #568: 1 #570: 1 #572: 1 #576: 1 #576: 1	#2: 813 #4: 796 #6: 804 #8: 802 #10: 826 #12: 815 #14: 841 . . . #474: 1 #490: 1 #492: 1 #498: 1 #510: 1 #518: 1 #552: 1 #572: 1 #600: 1

Таблица 12

Максимумы *LAT* для фиксированных масок по числу раундов шифра DES

Число циклов															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	256	486	596	574	534	522	534	548	548	514	528	640	534	556	492
0	0	490	538	550	496	562	528	518	460	536	512	542	524	554	508
0	192	492	566	626	552	562	586	572	514	558	508	582	512	562	524
0	392	500	566	516	498	530	534	522	582	510	560	512	616	524	482
0	96	536	490	502	476	504	546	536	508	514	558	538	480	568	532
0	480	510	502	510	512	538	554	550	504	552	516	500	492	510	502
0	160	446	494	530	554	554	566	550	586	544	536	570	550	568	584
0	0	442	542	528	544	512	498	484	506	554	508	606	500	578	632
0	0	248	588	522	548	516	556	510	498	526	522	560	530	502	472
0	0	512	510	458	478	524	530	516	588	578	484	526	534	528	504

для различного числа циклов алгоритма шифрования. Видно, что значение максимума таблиц линейных аппроксимаций получается в районе 500-600, что совпадает с асимптотическими показателями шифра ГОСТ и значениями, следующими из теоретического закона распределения вероятностей линейных аппроксимаций случайного S блока [7].

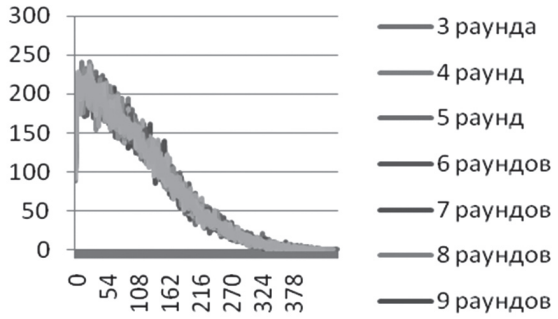

Рис. 2. Линейные свойства шифра DES

6. ПРОВЕРКА СТАТИСТИЧЕСКИХ СВОЙСТВ С ПОМОЩЬЮ НАБОРА ТЕСТОВ NIST STS

Одною из популярных методик статистических исследований шифрующих преобразований является тестирование выходного потока битов, полученных после зашифрования с помощью тестов NIST STS, используемых для выяснения наличия признаков псевдослучайности.

Набор тестов NIST STS был предложен в ходе проведения конкурса на новый национальный стандарт блокового шифрования США. Это набор тестов использовался и для исследования статистических свойств кандидатов на новый блоковый шифр в ходе конкурса, проводимого и в Украине. На сегодня методика тестирования, предложенная NIST, является наиболее распространенной у разработчиков криптографических средств защиты информации. Мы здесь не будем подробно излагать сущность этой методики, которую можно найти во многих источниках, а приведем сразу результаты ее применения для анализа показателей статистической безопасности шифров DES и ГОСТ.

Как видно из результатов тестирования 8-ми цикловый DES уже проходит 86% уровень [см. рис. 3, 4], в то время как у ГОСТ-а один из тестов остается ниже 50%-го уровня. Для 12 циклов шифрования оба шифра уже проходят для всех тестов 96% уровень (рис. 5, 6). Близкие к приведенным здесь показатели прохождения тестов имеют и большие прототипы рассмотренных шифров.

ЗАКЛЮЧЕНИЕ

Представленные в работе результаты анализа криптографических свойств уменьшенных моде-

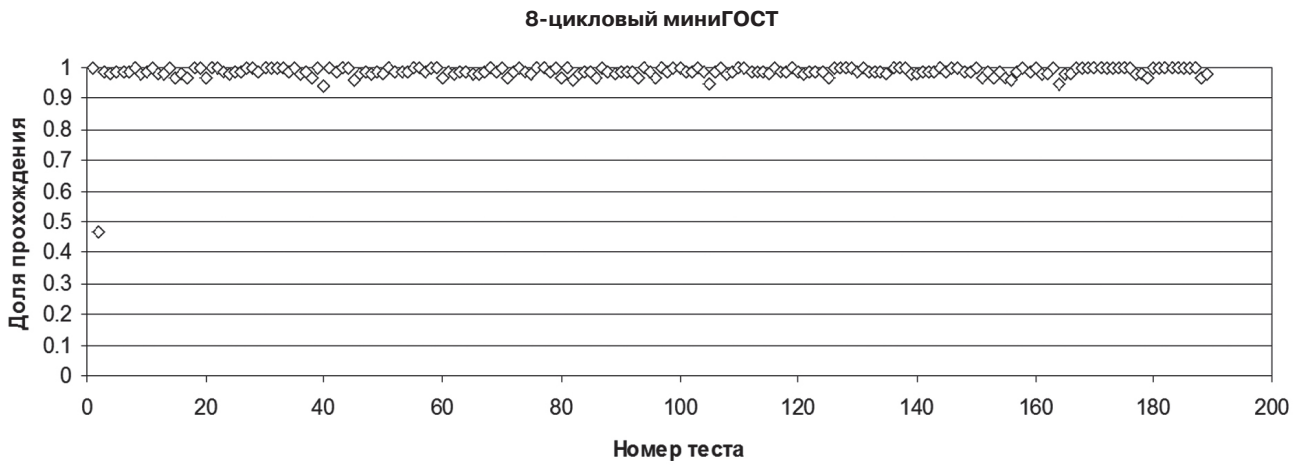

Рис. 3. Прохождение тестов 8-ми цикловым шифром ГОСТ

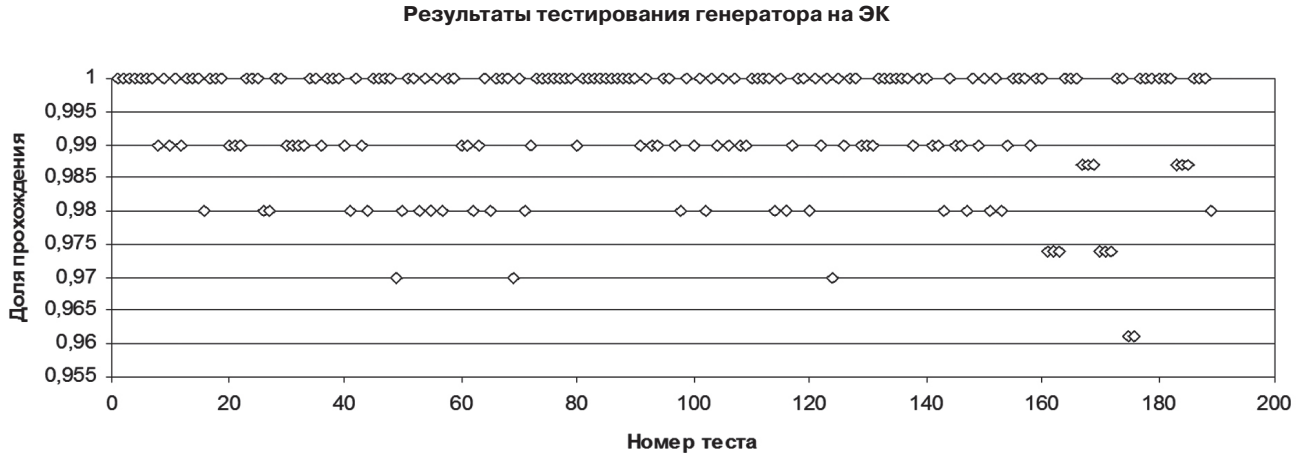

Рис. 4. Прохождение тестов 8-ми цикловым шифром DES

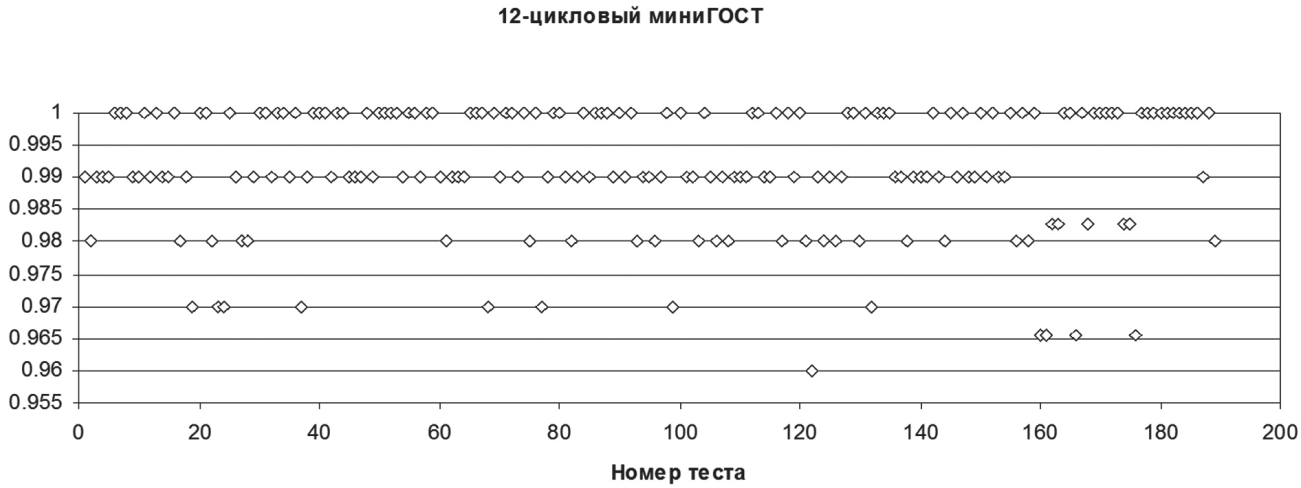

Рис. 5. Прохождение тестов 12-ти цикловым шифром ГОСТ

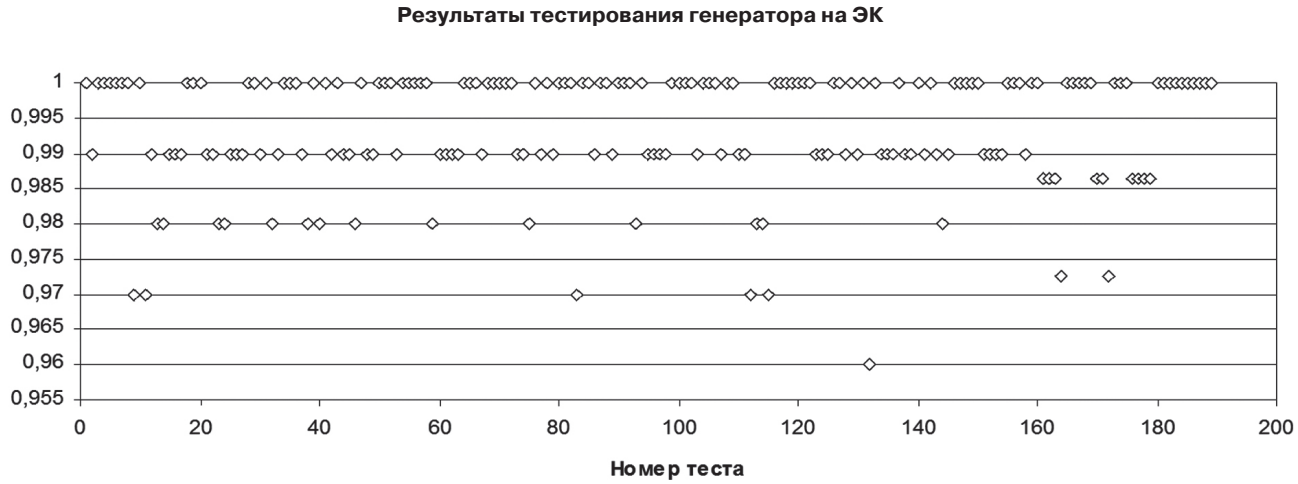

Рис. 6. Прохождение тестов 12-ти цикловым шифром DES

лей шифров ГОСТ и DES в целом подтвердили, что они отражают свойства своих прототипов. Тем самым косвенным путем подтверждена адекватность подхода к анализу свойств больших прототипов на основе использования показателей и характеристик их уменьшенных моделей.

Литература

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

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

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

[4] Judy Moore Cycle Structure of the DES with Weak and Semi-Weak Keys / Judy Moore and Gustavus Sianons. // Sandia National Laboratories Albuquerque, NM 87165, Copyright © Springer-Verlag, 1998, pp. 11-32.

[5] *Долгов В.И.* Принципы защиты алгоритма DES от атак дифференциального криптоанализа. "Секреты" *S* блоков стандарта / Долгов В.И., Лисицкая И.В., Головашич С.А., Олейников Р.В. // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2000. Вып. 113. – С. 148-157.

[6] *Горбенко И.В.* Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа / Горбенко И.В., Лисицкая И.В., Коряк А.С. // Радиоэлектроника и информатика. 1998. №1 (02). С. 39-43.

[7] *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И. // Прикладная радиоэлектроника. Харьков: ХНУРЭ. – 2010.

[8] Luke O'Connor. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995.

[9] *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И. // Прикладная радиоэлектроника. Харьков: ХНУРЭ. – 2010.

Поступила в редколлегию 19.04.2011

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Макарчук Ярослав Анатольевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптоанализ асимметричных криптографических схем с помощью аппаратных атак.

Григорьев Андрей Владимирович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: анализ криптографических свойств блочных симметричных и потоковых шифров, и их схем разворачивания ключей.

Дроботько Екатерина Викторовна, аспирантка кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров, анализ структурних элементов БСШ.

УДК 621.3.06

Дослідження криптографічних показників зменшених моделей шифрів ГОСТ та DES / В.І. Долгов, Я.А. Макарчук, А.В. Григор'єв, К.В. Дроботько // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 127–134.

Для обгрунтування правомірності оцінки властивостей та криптографічних показників блокових симетричних шифрів на основі вивчення і зіставлення властивостей їх зменшених моделей приводяться результати аналізу властивостей та криптографічних показників зменшених моделей добре відомих і детально вивчених шифрів DES і ГОСТ. На основі отриманих результатів роблять висновок про те, що зменшені моделі шифрів DES і ГОСТ практично повторюють характеристики своїх великих прототипів.

Ключові слова: зменшена версія шифру, що стискає перестановка, циклічні властивості, повний диференціал.

Табл. 12. Іл. 6. Бібліогр.: 9 найм.

UDC 621. 391:519.2:519.7

Researching cryptographic indeces of reduced models of GOST and DES ciphers / V.I. Dolgov, Ya.A. Makarchuk, A.V. Grigoriev, E.V. Drobot'ko // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 127–134.

For grounding legitimacy of estimation of properties and cryptographic indexes of block symmetric ciphers on the basis of study and comparison of properties of their diminished models results of analyzing the properties and cryptographic indexes of the diminished models of well known DES and GOST ciphers studied in detail are presented. On the basis of the results obtained a conclusion is drawn that the diminished models of DES and GOST codes practically repeat the characteristics of their big prototypes.

Keywords: reduced version of a cipher, compacting permutation, cyclic properties, total differential.

Tab. 12. Fig. 6. Ref.: 9 items.