Продолжение таблицы 6

Расшифровка блока данных A. Проверка блока данных A (аутентификация B).		
	 Пересылка данных с указанием имени сервиса.	

В табл. 6 представлен также порядок работы криптографических серверов A и B при обращении сервера B в локальную область A, закрытую сервером A. При повторном обращении сервера B к серверу A сервер A принимает решение о генерации новых параметров сессии и взаимной аутентификации, а также о временном интервале доверия к сертификату.

V Заключение

Протоколы передачи данных в защищенном режиме SSL, TLS, PCT и другие в общем случае предназначены для использования западных стандартов на криптографические преобразования над данными. Кроме того, реализации этих протоколов содержат экспортные ограничения на длину ключей, а поэтому не могут быть использованы для защиты передаваемых данных на уровне конфиденциальной связи. Кроме того, протоколы SSL, TLS, PCT необходимы для интеграции различных программных продуктов, зачастую выполненных различными производителями. Предложенный Протокол защищенной передачи данных предназначен для использования любой длины ключей, базируется на использовании отечественных стандартов криптографии и предназначен для использования в однородных *криптографических серверах*.

УДК 681.3.06:006.354

ИССЛЕДОВАНИЕ СВОЙСТВ ПОДСТАНОВОК ГОСТ 28147-89, ПОСТРОЕННЫХ НА ОСНОВЕ АНАЛИЗА СВОЙСТВ КООРДИНАТНЫХ ФУНКЦИЙ

Роман Олейников, Ирина Лисицкая, Александр Шумов
Харьковский национальный университет радиоэлектроники

Аннотация: **Показано, что известные требования к подстановкам ГОСТ 28147-89 позволяют использовать заполнение узлов замены, при которых шифр является уязвимым к дифференциальному криптоанализу.**
Summary: **It is shown, that known requirements to S boxes of GOST 28147-89 allow to use permutations, which make cipher vulnerable to differential cryptanalysis.**
Ключевые слова: **ГОСТ 28147-89, заполнение узлов замены, дифференциальный криптоанализ.**

В настоящее время в Украине официально рекомендован к применению только один блочный симметричный алгоритм шифрования – ГОСТ 28147-89. Его особенностью является отсутствие стандартного заполнения узлов замены (S-блоков). Разработчики шифра не определили долговременный ключ, также как и не опубликовали в открытой печати правила его построения. Тем не менее, известно, что именно свойства подстановок в значительной мере определяют криптостойкость всего шифра [1].

К нынешнему моменту опубликованы несколько подходов к обоснованию требований отбора подстановок ГОСТ 28147-89, один из которых основан на анализе криптографических свойств координатных (булевых) функций, образующих S-блок [2]. В работе предлагается использование четырёх требований, первое из которых определяет формирование перестановки, а три остальных определяют свойства булевых функций, отображающих входные биты S-блока в выходные. Кратко напомним эти требования:

1) все преобразования π_i ($i = \overline{1,8}$), образующие блок замены π, должны быть перестановками;

2) у каждой из координатных функций $f_j^{(i)}$ перестановок π_i ($i = \overline{1,8}$, $j = \overline{1,4}$) должен отсутствовать аффинный статистический аналог, совпадающий с ней с вероятностью большей, чем $3/4$:

$$\left|\Delta_a^f\right| \le 4,$$

где Δ_a^f – коэффициент статистической структуры булевой функции $f_j^{(i)}$ подстановки π_i, $a = \overline{0,15}$;

3) корреляционные коэффициенты 1-го и 2-го порядка подстановок π_i должны удовлетворять условиям

$$c_{i,j}^{\alpha} = \frac{1}{2} + \frac{h}{8},\ h = -1,0,1\ (j = 1,...,4,\ i = 1,...,4),$$

$$c_{i_1,i_2,j}^{\alpha_1,\alpha_2} = \frac{1}{4} + \frac{h}{8},\ h = -1,0,1\ (j = 1,...,4,\ i_1, i_2 : 1 \le i_1 < i_2 \le 4);$$

4) коэффициенты размножения ошибки координатных функций должны удовлетворять условию

$$\frac{1}{4} \le \frac{1}{2^4} \sum_{x \in V_4(2)} \left(f\left(x_1,...,x_i,...,x_4\right) \oplus f\left(x_1,...,\overline{x_i},...,x_4\right) \right) \le \frac{3}{4} \quad (i = 1,...,4).$$

Подчеркнём, что кроме первого требования, определяющего биективность преобразования, все остальные относятся только к координатным функциям, задающим значения отдельных битов S-блока. Из этого следует, что несмотря на выполнение требования 2, для линейной комбинации булевых функций $f_j^{(i)}$ подстановки возможно существование аффинного статистического аналога с вероятностью, превышающей значение $3/4 = 12/16$.

Рассмотрим вариант долговременного ключа ГОСТ 28147-89, каждая подстановка которого удовлетворяет требованиям 1–4 (табл. 1).

Таблица 1 – Долговременный ключ π, соответствующий требованиям 1–4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	11	4	2	13	1	8	5	7	3	14	12	0	6	9	15	10
2	8	14	1	0	4	9	15	2	6	5	3	13	11	10	12	7
3	8	12	4	3	7	5	10	1	15	2	14	9	0	13	11	6
4	6	3	0	13	4	10	11	2	14	1	7	8	9	5	12	15
5	3	6	13	2	14	1	7	8	9	5	0	15	10	11	4	12
6	5	8	1	3	6	9	15	14	7	12	10	13	11	2	4	0
7	3	5	1	14	11	0	6	13	12	7	15	10	4	8	9	2
8	12	8	7	0	1	11	13	14	5	6	10	3	2	15	9	4

Для поиска высоковероятных аффинных статистических аналогов линейных комбинаций булевых функций S-блока можно воспользоваться его таблицей линейной аппроксимации. Для первой подстановки, входящей в рассмотренный долговременный ключ, линейная аппроксимация приведена в табл. 2 (пустые ячейки означают нулевые элементы). Каждый элемент вычислен по формуле [3]:

$$NS_i(\alpha,\beta) = \#\left\{ x \;\middle|\; 0 \le x \le 15, \left(\bigoplus_{s=1}^{4} (x_s \cdot \alpha_s) \right) = \left(\bigoplus_{t=1}^{4} (\pi_i(x) \cdot \beta_t) \right) \right\} - 8. \qquad (1)$$

Таблица 2 – Линейная аппроксимация подстановки π_1 из табл. 1

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

Продолжение таблицы 2

A		2	2	4	2			-2	-2		4	-2		-2	2	
B		-4			-2	-2	2	-2	-4				2	2	2	-2
C			-2	-2			-2	-2	-2	6			-2	-2		
D		2	-4	2		2	4	2		2		-2		2		-2
E			2	2	-2	-2			2	2			-4	4	2	2
F		2		-2	-2		-2	4	-4	-2		-2	-2		2	

Как следует из (1), таблица линейной аппроксимации $NS_i(\alpha,\beta)$ подстановки π_i, $0 \le \alpha,\beta \le 15$, $1 \le i \le 8$, является более общей конструкцией для описания аффинных свойств S-блока, а колонки с индексами 1, 2, 4 и 8 совпадают со статистическими структурами булевых функций $f_1^{(i)}$, $f_2^{(i)}$, $f_3^{(i)}$ и $f_4^{(i)}$ соответственно. Заметим, что в таблице 2 значения $\left|NS_1(\alpha,\beta)\right| \le 4$ для $0 \le \alpha \le 15$ и $\beta \in \{1,2,4,8\}$, поэтому $\left|\Delta_a^f\right| \le 4$, и для π_1 соблюдается требование 2. Тем не менее, в $NS_1(\alpha,\beta)$ присутствуют значения, чей модуль превышает 4. Например, $NS_1(C,9) = 6$, что определяет существование линейной аппроксимации $f_1^{(1)} \oplus f_4^{(1)} = x_1 \oplus x_2$ с вероятностью $p_{C9}^{(1)} = 1/2 + 6/16 = 14/16$.

Отсюда следует, что вероятность совпадения аффинного статистического аналога линейной комбинации булевых функций подстановки π_1 выше, чем пороговое значение для одной координатной функции, определённое в требовании 2. Полученное значение вероятности показывает снижение стойкости алгоритма шифрования к линейному криптоанализу в случае применения таких S-блоков.

При исследовании линейных свойств случайных S-блоков ГОСТа установлено, что существует большое количество перестановок, для которых модули значений в таблице линейной аппроксимации не превышают 4. Согласно статистическим данным вероятность генерации такого S-блока равна $p_4^L = 0{,}088 \approx 2^{-3{,}5}$. Однако экспериментальные попытки построить подстановку, для которой $\left|NS(\alpha,\beta)\right| \le 4$, $0 \le \alpha,\beta \le 15$ и при этом удовлетворяющую критериям [2], показали, что требование 3 не допускает использование таких подстановок. В результате можно предположить, что таблица линейной аппроксимации S-блока, удовлетворяющего всем требованиям [2], будет содержать элемент $NS(\alpha,\beta)$, по модулю не меньший 6 для $\alpha,\beta = 1,...15$, т. е. что аффинность такой подстановки будет достаточно высокой.

Тем не менее, благодаря переносам между разрядами, возникающими в ключевом сумматоре цикловой функции ГОСТ 28147-89, использование леммы М. Матсуи невозможно [4]. Поэтому при использовании сеансовых ключей, вызывающих появление большого количества переносов при шифровании, линейный криптоанализ [3] неприменим к ГОСТ 28147-89 при любых перестановках, используемых в составе долговременного ключа. Отсюда можно сделать вывод, что для подавляющего большинства сеансовых ключей ГОСТ 28147-89 с S-блоками, построенными в соответствии с требованиями [2], является защищённым от линейного криптоанализа, несмотря на возможность построения высоковероятной линейной аппроксимации подстановок.

Кроме линейного криптоанализа, для нападения на блочные симметричные шифры может быть использован и дифференциальный криптоанализ. Несмотря на большое количество циклов шифрования и использование модульного сложения для введения подключей, ГОСТ 28147-89 может быть уязвим для такой атаки [1]. В связи с этим возникает вопрос о стойкости алгоритма шифрования при использовании для построения S-блоков требований работы [2].

Долговременный ключ в атаке [1] состоит из подстановок, для которых некоторая входная разность $\Delta_{вх}^{(i)}$ всегда преобразовывается в выходную $\Delta_{вых}^{(i)}$, причем во входной и выходной разности активным является только один бит:

$$\pi : \pi_{1..8} \in \left\{ \pi_i \;\middle|\; P\left(\Delta_{вых}^{(i)} \Big/ \Delta_{вх}^{(i)} \right) = 1 \text{ для } w_T\left(\Delta_{вых}^{(i)}\right) = w_T\left(\Delta_{вх}^{(i)}\right) = 1 \right\}. \qquad (2)$$

Здесь $w_T(x)$ обозначает вес Хемминга четырёхбитового вектора x, при этом входные и выходные разности связаны соотношением $\Delta_{вых}^{(i)} = 2^{1+\log_2 \Delta_{вх}^{(i)} (\mathrm{mod}\, 4)}$.

Можно убедиться, что для таких подстановок

$$\left\| f_j^{(i)}(x_1,...,x_k,...,x_4) \oplus f_j^{(i)}(x_1,...,\overline{x_k},...,x_4) \right\| = 16, \qquad (3)$$

где $k = 5 - \log_2 \Delta_{вх}^{(i)}$ – номер активного бита во входной разности, $j = 5 - \log_2 \Delta_{вых}^{(i)}$ – номер активного бита в выходной разности подстановки π_i. Свойство (3) противоречит требованию к коэффициентам размножения ошибки координатных функций, поэтому подстановки (2) не удовлетворяют рассматриваемым критериям. Отметим также, что при проведении экспериментов не удалось построить S-блоки вида (2), соответствующие требованиям корреляционной иммунности. Отсюда следует, что подстановки [2] невозможно использовать в атаке, описанной в [1].

Тем не менее, при $P\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right) \geq \frac{6}{16}$ возможно проведение дифференциального криптоанализа ГОСТ 28147-89. Аналогично можно ослабить и второе условие: $w_T\left(\Delta_{вых}^{(i)}\right) = w_T\left(\Delta_{вх}^{(i)}\right) \leq 3$, что уменьшит количество сеансовых ключей, при которых возможно проведение атаки (ограничение на активизацию только 3 битов следует из требования к нераспространению активизации за пределы одного S-блока).

Для получения наиболее эффективной атаки необходимо использование наибольшего значения для $P\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right)$, а для увеличения количества сеансовых ключей, при которых возможен криптоанализ, необходимо уменьшение $w_T\left(\Delta_{вх}^{(i)}\right)$, при этом $w_T\left(\Delta_{вх}^{(i)}\right) \geq 1$.

Первоначально, по аналогии с [1], производился поиск перестановок, для которых возможно преобразование $w_T\left(\Delta_{вх}^{(i)}\right) = 1$ с высокой вероятностью. Были построены S-блоки, удовлетворяющие требованиям к корреляционной иммунности и коэффициентам размножения ошибки, для которых вероятность $P\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right) = \frac{8}{16}$, однако в статистической структуре координатных функций таких подстановок всегда находился коэффициент $\left|\Delta_a^f\right| > 4$. При выполнении и этого требования удалось найти S-блоки с максимальным значением $P_{\max}\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right) = \frac{4}{16}$, чего недостаточно для проведения атаки. Таким образом, при однобитовой входной разности подстановки ($w_T\left(\Delta_{вх}^{(i)}\right) = 1$) требования [2] не допускают использование S-блоков, при которых ГОСТ 28147-89 будет уязвимым для известного варианта дифференциального криптоанализа.

В связи с этим были исследованы S-блоки, для которых возможно преобразование разностей с $w_T\left(\Delta_{вх}^{(i)}\right) = 2$. Было обнаружено, что в этом случае требования 3 и 4 допускают использование подстановок с $P_{\max}\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right) = \frac{12}{16}$. Тем не менее, при использовании ограничения на коэффициенты статистической структуры наибольшее допустимое значение вероятности снижается до $P_{\max}\left(\Delta_{вых}^{(i)} \middle/ \Delta_{вх}^{(i)}\right) = \frac{8}{16}$. Однако, такое значение позволяет реализовать дифференциальную атаку. В частности, был построен долговременный ключ (см. табл. 1), каждый из S-блоков которого выполняет преобразование входной разности $\Delta_{вх}^{(i)} = 3$ в выходную $\Delta_{вых}^{(i)} = 6$ с вероятностью $8/16$:

$$\pi : \pi_{1..8} \in \left\{ \pi_i \;\middle|\; P\left(\Delta^{(i)}_{вых} = 6 \middle/ \Delta^{(i)}_{вх} = 3 \right) = \frac{8}{16} \right\}. \qquad (4)$$

Отметим, что в соответствии с эмпирическими данными, вероятность того, что случайная подстановка π_i, удовлетворяющая требованиям [2], одновременно будет обладать свойством $P_{\max}\left(\Delta^{(i)}_{вых} \middle/ \Delta^{(i)}_{вх} \right) = \frac{8}{16}$, равна $p_w = 8{,}2 \cdot 10^{-4} \approx 2^{-10{,}25}$ (при проведении эксперимента были исследованы свойства 277134253 случайных перестановок, из которых 211068 прошли ограничения [2], из них соответственно 173 выполняли преобразование $\left(\Delta^{(i)}_{вх} = 3\right) \to \left(\Delta^{(i)}_{вых} = 6\right)$ с вероятностью $P_{\max} = \frac{8}{16}$). Отсюда вероятность генерации долговременного ключа, удовлетворяющего условию (4), и при этом состоящего из перестановок, соответствующих критериям [2], равна $p_8^G = \left(p_w\right)^8 \approx 2^{-82}$.

Распределение разностей первого S-блока π_1 построенного долговременного ключа приведено в табл. 3. Как можно видеть, для входной разности $\Delta^{(1)}_{вх} = 3$ вероятность преобразования в выходную $\Delta^{(1)}_{вых} = 6$ равна $\frac{8}{16}$, при этом $w_T\left(\Delta^{(1)}_{вых} = 6\right) = w_T\left(\Delta^{(1)}_{вх} = 3\right) = 2$.

Таблица 3 – Распределение разностей подстановки π_1 из табл. 1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16															
1			2			2				2			2	2		6
2				2	2					6					2	4
3			2	2			8						2	2		
4				2		2		4			6		2			
5				2		4	2		4		2					2
6				4	2	2				2	2		2		2	
7		4				2	2			2	2		4			
8		2						2	2		4			4	2	
9		2	2			2		2	4						2	2
A		2	2	4	2			2							4	
B		2						2	2			4	4		2	
C			2				2	4		2				6		
D			6			2			2			4				2
E					6		2		2	2				2	2	
F		4			4							8				

Преобразование разностей на S-блоке $\left(\Delta^{(i)}_{вх} = 3\right) \to \left(\Delta^{(i)}_{вых} = 6\right)$ обладает свойством, заключающемся в том, что активизация подстановки не выходит за её пределы в ходе преобразования внутри цикловой функции ГОСТа, что позволяет строить дифференциальные характеристики с малым количеством активных S-блоков; в этом случае распространение активизации обуславливается только конструкцией цепи Фейстеля и искажениями разностей на ключевом сумматоре, что в некоторых случаях позволяет вообще избежать лавинного эффекта.

Для заполнения узлов замены, приведенного в табл. 1, была построена 32-цикловая характеристика Ω с $r = 45$ активными S-блоками. Маски подключей M_Ω для неё приведены в табл. 4, а сама характеристика Ω – в табл. 5 (маски и разности представлены в шестнадцатеричной системе счисления, вероятность преобразования в последней колонке табл. 5 вычислена с учётом предположения об отсутствии искажений на ключевом сумматоре).

Таблица 4 – Маски разности подключей M_Ω для построенной характеристики с 45-ю активными S-блоками

K_0	K_1	K_2	K_3
00330300	30030303	30033000	03030003
K_4	K_5	K_6	K_7
00030030	33030003	30033300	00330303

Вероятность характеристики в случае отсутствия искажений на ключевом сумматоре может быть получена из количества активных подстановок: $p_\Omega^{K^w} = 2^{-r} = 2^{-45}$. Это свойство выполняется для сеансовых ключей шифрования, у которых в 0 сброшены все биты подключей, за исключением старшего: $K \in K^w = \left\{\left(k_l 0^{31}\right)^8, 0 \le l \le 7, k_l \in GF(2)\right\}$, где значения из K^w представлены в двоичной системе счисления. Очевидно, что $\left|K^w\right| = 2^8 = 256$.

Тем не менее, верные пары для характеристики Ω существуют и при $K \notin K^w$, однако для таких ключей её вероятность ниже: $p_\Omega^{K \notin K^w} < p_\Omega^{K^w}$. Поскольку нижним порогом вероятности характеристики ГОСТ 28147-89 является значение $p^{\min} = 2^{-64}$, интерес представляет оценка мощности множества ключей K^E, для которых $p_\Omega^{K^E} > p^{\min}$, и, соответственно, дифференциальный криптоанализ является эффективным.

Для верной пары характеристики Ω (табл. 6) все разности проходят через сумматор без искажения. Это условие выполняется, если каждая активная тетрада без изменения будет передана со входа цикловой функции на S-блоки. Известно, что возможность (и вероятность) прохождения тетрады разности через сумматор зависит от соответствующих четырёх битов подключа на рассматриваемом цикле. Анализ таблиц распределения разностей для 4-битового сумматора показал, что прохождение разности вида $\Delta_{вх}^{(i)} = 3$ возможно при условии, что младшие два бита ключевой тетрады равны нулю, т. е.

$$K_j^{(i)} \in \left\{k \,\middle|\, k \equiv 0 (\mathrm{mod}\, 4), k \in GF(2)^4\right\} = \{0,4,8,12\}, \qquad (5)$$

где j – номер активной тетрады в 32-битовой разности, $0 \le j \le 7$. Отсюда получается, что для каждой активной тетрады разности возможно использование 4 значений ключа из 16 возможных.

Таблица 5 – Характеристика Ω с 45 активными S-блоками для долговременного ключа π из табл. 1

Номер цикла	Левая половина входного значения	Правая половина входного значения	Вероятность преобразования
1	30303	300000	2^0
2	300000	30300	2^{-1}
3	30300	30000000	2^{-3}
4	30000000	30000	2^{-4}
5	30000	0	2^{-5}
6	0	30000	2^{-5}
7	30000	30000000	2^{-6}
8	30000000	30300	2^{-7}
9	30300	300000	2^{-9}
10	300000	30303	2^{-10}
11	30303	30003000	2^{-13}
12	30003000	3030003	2^{-15}
13	3030003	30	2^{-18}
14	30	3000003	2^{-19}
15	3000003	3000	2^{-21}
16	3000	3	2^{-22}
17	3	0	2^{-23}
18	0	3	2^{-23}
19	3	3000	2^{-24}
20	3000	3000003	2^{-25}

Продолжение таблицы 5

21	3000003	30	2^{-27}
22	30	3030003	2^{-28}
23	3030003	30003000	2^{-31}
24	30003000	30303	2^{-33}
25	30303	300000	2^{-36}
26	300000	30300	2^{-37}
27	30300	30000000	2^{-39}
28	30000000	30000	2^{-40}
29	30000	0	2^{-41}
30	0	30000	2^{-41}
31	30000	30000000	2^{-42}
32	30000000	30300	2^{-43}
33	30300	300000	2^{-45}

Кроме того, необходимо учитывать возможность прихода переноса из младших тетрад в старшие. Приход синхронного переноса из предыдущей тетрады аналогичен прибавлению 1 к значению ключевых битов в текущей тетраде [1], что вызывает искажение разностей. Для снижения вероятности прихода переноса необходимо дополнительно установить в нуль ключевые биты, предшествующие активной тетраде на текущем цикле. При установке в нуль двух битов, предшествующих активной тетраде, получаем вероятность возникновения ситуации, благоприятствующей прохождению $\Delta_{вх}^{(i)}$ без искажения, не менее чем $p_{\Delta_{вх}^{(i)}}^{T} = 1 - p\left(a = a' = 11_2\right) = \frac{3}{4}$, где $a = a' = 11_2$ – значение, вызывающее транспортировку переноса (так как a и a' представляют собой два старших бита тетрады $j-1$ обрабатываемого блока, а разность характеристики Ω может принимать только значение $\Delta_{вх}^{(i)} = 3 = 0011_2$, то для верной пары всегда $a = a'$).

Каждый из подключей участвует в шифрующем преобразовании 4 раза. Разности соответствующих входов циклов для каждого из подключей, объединённые при помощи дизъюнкции, образуют маски разностей подключей M_Ω (табл. 4). Анализируя количество ненулевых тетрад в M_Ω можно найти мощность множества сеансовых ключей K^E, для которых возможно нахождение верной пары характеристики Ω, и, соответственно, выполнение дифференциального криптоанализа. Можно видеть, что в M_Ω присутствует $n_s = 23$ активные тетрады, в которые возможен перенос, и $n_j = 4$ младшие активные тетрады, приход переноса в которые невозможен (подключи K_1, K_3, K_5, K_7). Имеем, что для каждой из n_s тетрад необходимо установить в нуль 4 бита ключа, а для каждой из n_j – 2 бита. Получается, что после фиксации $n_{fx} = n_s \cdot (2+2) + n_j \cdot 2 = 100$ битов сеансового ключа существует верная пара для характеристики. Отсюда $\left|K^E\right| \geq 2^{256-n_{fx}} = 2^{256-100} = 2^{156}$, и при этом $K^w \subset K^E$. Отметим также, что ситуация, когда в n_s активных тетрадах четыре ключевых бита вместо нуля устанавливаются в единицу, также благоприятствует выполнению характеристики, что дополнительно увеличивает K^E.

Как уже было отмечено выше, для сеансовых ключей $K \in K^w$ вероятность характеристики Ω максимальна и равна $p_\Omega^{\max} = p_\Omega^{K^w} = 2^{-45}$. Оценим нижнее значение вероятности $p_\Omega^{\min}$ для $K \in K^E$. В худшем случае (с точки зрения поиска верной пары), перенос возникает в каждом разряде, предшествующем зафиксированному блоку ключевых битов для каждой из n_s^Ω активных тетрад, присутствующих в характеристике, и не являющихся самыми младшими. В характеристике Ω присутствуют $n_j^\Omega = 8$ активных тетрад в младших разрядах, и поскольку общее количество активных S-блоков равно $r = 45$, то $n_s^\Omega = r - n_j^\Omega$. В этом случае вероятность того, что перенос не транспортируется в активную тетраду, равна

$p^{T}_{\Delta^{(i)}_{вх}}$. Отсюда находим нижнее значение вероятности характеристики Ω для сеансовых ключей $K \in K^E$: $p^{\min}_{\Omega} = p^{\max}_{\Omega} \cdot \left(p^{T}_{\Delta^{(i)}_{вх}}\right)^{r-n^{\Omega}_{j}} = 2^{-45} \cdot \left(\frac{3}{4}\right)^{45-8} \approx 2^{-45} \cdot 2^{-15,4} = 2^{-60,4}$. Получается, что $p^{\min}_{\Omega} > p^{\min}$, и для любого $K \in K^E$ возможно выполнение дифференциального криптоанализа.

Для экспериментальной проверки полученных результатов была выбрана 16-цикловая характеристика, совпадающая с первой половиной Ω:

$$\Omega^{16} = \left(\Delta^{\Omega^{16}}_{вх} = 3\ 0303\ 0030\,0000, \Delta^{\Omega^{16}}_{вых} = 3\ 0000\,0000, \Delta^{\Omega^{16}}_{i} = \Delta^{\Omega}_{i}, 2 \le i \le 16\right). \quad (6)$$

С учетом маски подключей M_{Ω} (табл. 4) был сформирован сеансовый ключ $K^{э} \in K^E$ (табл. 6). После выполнения $2 \cdot 3{,}57 \cdot 10^{9}$ шифрований на сеансовом ключе $K^{э}$, было найдено 207 верных пар характеристики (6), что даёт экспериментальную вероятность $p^{э}_{\Omega^{16}} \approx 5{,}8 \cdot 10^{-8} = 2^{-24,04}$, находящуюся в пределах $p^{\min}_{\Omega} = p^{\max}_{\Omega^{16}} \cdot \left(\frac{3}{4}\right)^{23-n^{\Omega^{16}}_{j}} = 2^{-30,9} \le p^{э}_{\Omega^{16}} \le p^{\max}_{\Omega^{16}} = 2^{-r_{\Omega^{16}}} = 2^{-23}$. При этом $p^{э}_{\Omega^{16}}$ достаточно близко к теоретически полученному значению вероятности $p_{\Omega^{16}} = 2^{-(23+1.28)} = 2^{-24,28}$.

Отсюда следует, что экспериментальные данные полностью подтверждают приведенные выше оценки.

Таблица 6 – Пример сеансового ключа ГОСТ 28147-89, построенного с учётом масок разности M_{Ω}

K_0	K_1	K_2	K_3
F7C0080B	C0E81014	40D801B5	FC081290
K_4	K_5	K_6	K_7
9FA403C0	800C07D4	40E40009	E7C00408

Таким образом, требования [2] допускают использование заполнения узлов замены, при котором ГОСТ 28147-89 является уязвимым для дифференциального криптоанализа (сложность поиска верной пары составляет величину от 2^{45} до 2^{60} для не менее чем 2^{156} сеансовых ключей). Однако, из-за низкой вероятности получения таких подстановок, весьма жёстких условий проведения атаки и её высокой вычислительной сложности рассмотренная методика не может стать реальной угрозой безопасности алгоритма ГОСТ 28147-89. Вместе с тем факт наличия теоретической атаки актуализирует вопрос дальнейшего совершенствования критериев отбора подстановок для ГОСТ 28147-89.

Литература: 1. Олейников Р. В. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89. // Радиотехника. – 2001. – № 119. С. 146–152. 2 . Холоша А. А. Об одном подходе к анализу качества блока подстановки битовых векторов. // Збірник наукових праць інституту проблем моделювання в енергетиці НАНУ. Вип. 2. Львів: Світ. – 1998. с. 59–74. 3. M. Matsui. Linear Cryptanalysis Method for the DES Cipher. Lecture Notes in Computer Science, Advances in Cryptology, proceedings of Eurocrypt '93, 1993. pp. 27–41. 4. C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, Y. Zheng. Further comments on the Soviet Encryption Algorithm. Advances in Cryptology – EUROCRYPT'96, Springer-Verlag, Berlin, 1996, pp. 433–438.

УДК 681.3.067:681.3.016

ОСНОВНАЯ ПРОБЛЕМА ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Виктор Куценко, Тарас Левченко, Николай Миронов, Виктор Мясоедов
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Применяемые обычно критерии оценки псевдослучайных последовательностей приводят к отбраковке слишком большого числа последовательностей. Это приводит к усложнению схем генерации и замедляет шифрование. В статье предложен критерий оценки, аналогичный**