УДК 621.3.06

Лисицкий К. Е.

Аспирант Харьковского национального университета имени В. Н. Каразина

ВЫРОЖДЕННЫЕ S-БЛОКИ

Актуальность. S-блоки являются одним из основных преобразований многих шифров, и поиску S-блоков с улучшенными криптографическими показателями уделяется громадное внимание в литературе этого направления. Тем самым полагается, что есть подстановки (S-блоки), которые следует считать плохими, т.е. такие, которые не подходят для построения надежных шифров. С другой стороны, одно из направлений совершенствования конструкций шифров, которое развивается в последнее время, связано с построением шифров, в которых могут применяться S-блоки случайного типа. Возникает важный вопрос. А какие же S-блоки не подходят для построения шифрующих преобразований? В этой связи большую актуальность приобретает изучение свойств и особенностей формирования S-блоков вырожденных конструкций, под которыми понимаются подстановки, ухудшающие криптографические показатели шифров.

Цель. Изучение свойств и особенностей формирования подстановок вырожденного типа, оценка вероятности их порождения с помощью генератора случайных подстановок. Определение признаков, по которым можно отличить вырожденные подстановки.

Метод. Построение поцикловых законов распределения максимумов таблиц дифференциальных разностей и таблиц линейных аппроксимаций для уменьшенных моделей шифров, при использовании в них разных (вырожденных) конструкций S-блоков. Определение закона распределения максимумов XOR таблиц и смещений таблиц линейных аппроксимаций байтовых подстановок.

Результаты. Изучены ансамблевые характеристики множества байтовых подстановок. На основе изучения дифференциальных и линейных свойств уменьшенных моделей шифров определены признаки, по которым можно выявить вырожденные подстановки. Вычислительным и экспериментальным путем определена вероятность случайного порождения (выбора) байтовой подстановки вырожденного типа.

Выводы. Результатами работы подтверждено, что получение вырожденных байтовых S-блоков при случайном их порождении является маловероятным событием. Это означает, что практически без ограничений в шифрах могут использоваться S-блоки, порождения с помощью генератора случайных подстановок.

Научная новизна состоит в том, что изучено влияние вырожденных подстановок на эффективность шифрующих преобразований. Впервые установлено, что использование в шифрах S-блоков, порожденных случайным образом, с очень большой вероятностью не приводит к ухудшению показателей стойкости шифров к атакам дифференциального и линейного криптоанализа.

Практическая значимость результатов работы заключается в получении конкретных данных, подтверждающих основное положение развиваемой новой методики оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа о независимости показателей стойкости шифров от применяемых S-блоков, в том числе и S-блоков случайного типа.

Ключевые слова: методология оценки стойкости, вырожденные подстановки, дифференциальные показатели, линейные показатели.

НОМЕНКЛАТУРА

π – нелинейное подстановочное преобразование (S-блок);

ЛАТ – линейная аппроксимационная таблица подстановки;

ТР – таблица разностей подстановки;

ТД – таблица дифференциалов подстановки;

$\Pr(\Lambda_\pi(\Delta X, \Lambda Y) = 2k^*)$ – вероятность порождения подстановки с максимальным значением XOR разности;

k^* – половинное значение максимума XOR перехода дифференциальной таблицы;

$\Pr\left(\lambda^*(\alpha,\beta) = \left|2l^*\right|\right)$ – вероятность порождения подстановки с максимальным значением смещения ЛАТ;

l^* – половинное значение максимума смещения таблицы ЛАТ;

$D_{\max}(X)$ – закон распределения максимумов таблицы XOR разностей байтовой подстановки;

$D_{\max}(Y)$ – закон распределения максимумов смещений линейной аппроксимационной таблицы байтовой подстановки;

$DP^{\pi}_{\max}$ – максимальное значение дифференциальной вероятности таблицы подстановки π;

$LP^{\pi}_{\max}$ – максимальное значение линейной вероятности подстановки π.

ВВЕДЕНИЕ

Одним из основных положений, развиваемых в новой методологии оценки показателей стойкости блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа [1], является положение, состоящее в том, что все БСШ после определенного индивидуального для каждого БСШ числа циклов приходят по дифференциальным и линейным показателям к свойствам случайных подстановок соответствующих степеней (значения максимальных дифференциальных и линейных вероятностей совпадают с соответствующими показателями случайных подстановок).

Проведенные многочисленные эксперименты, свидетельствуют о том, что сформулированное положение выполняется практически для всех известных шифров, а подстановки, его не подтверждающие – это весьма ограниченное множество по сравнению с общим числом возможных подстановок, существенно не влияющее на достоверность сформулированного утверждения.

Это означает, что предлагаемая методология работает для произвольных S-блоковых конструкций, исключая так называемые вырожденные подстановки, которые в современных шифрах не используются. Возникает воп-

DOI 10.15588/1607-3274-2018-1-15

рос, а какие же S-блоки считать вырожденными? И насколько вероятно попасть при случайном выборе на вырожденную подстановку?

Одним из простых ответов на этот вопрос может стать такой: вырожденными S-блоками следует считать те, которые либо не позволяют шифру в пределах ограниченного числа циклов, однозначно определенного для каждого шифра, достичь показателей случайной подстановки соответствующей степени, либо стационарное значение, к которому приходит шифр, не соответствует ожидаемому, свойственному случайной подстановке.

Объектом исследования является процесс прихода шифров к состоянию случайной подстановки (к стационарному значению поцикловых значений максимумов дифференциальных и линейных вероятностей).

Предмет исследований составляют байтовые подстановки вырожденного типа, определение которых приведено выше.

Целью данной работы является изучение свойств и особенностей формирования подстановок вырожденного типа. Оценивается вероятность порождения байтовых S-блоков с помощью генератора случайных подстановок. Определяются признаки, по которым можно отличить вырожденные подстановки.

1 ПОСТАНОВКА ЗАДАЧИ

Пусть мы имеем выборку из случайно сгенерированных байтовых (размера 8×8) подстановок: π_1, π_2, . . ., π_n. Для симметрической группы S_n полное множество таких подстановок будет содержать $n!$ различных представителей. Каждое из этих преобразований характеризуется своими значениями максимальной дифференциальной $DP^{\pi}_{\max}$ и линейной $LP^{\pi}_{\max}$ вероятностей. Необходимо определить, какие из полного множества таких подстановок и сколько являются вырожденными в определенном выше смысле?

2 ЛИТЕРАТУРНЫЙ ОБЗОР

В криптографической литературе уделяется просто огромное внимание построению подстановочных конструкций (S-блоков) для блочных симметричных шифров [2–10 и мн. мн. др.], так как считается, что показатели стойкости шифров непосредственно связаны с криптографическими свойствами входящих в них S-блоков. Наши исследования [11–14 и мн. др.], однако, показали, что это не совсем так. Подстановочные преобразования, используемые в современных шифрах, не влияют на итоговые показатели стойкости шифров. Они влияют (не всегда) на динамику прихода шифров к состоянию случайной подстановки [15, 16] и то лишь в пределах одного цикла. Другое дело, что в принципе существуют конструкции S-блоков, которые ухудшают или просто разрушают криптографическое преобразование, применение которых для построения шифров просто недопустимо. Такие S-блоки в [1] названы вырожденными.

В работах [1, 17–19 и др.] пропагандируется использование для построения шифров случайно сконструированных S-блоков. Такие S-блоки нашли уже использование в современных шифрах, правда с дополнительным отбором по определенным критериям [20]. Возникает задача насколько важно выполнять проверку криптографических показателей S-блоков, предполагаемых к использованию в конкретном шифре, и если использовать случайные конструкции, как защититься от использования слабых (вырожденных) S-блоков?

В интернете нам не удалось найти материалов по вырожденным подстановкам. В этом направлении нашлась только одна опубликованная работа [21], в которой обсуждаются непосредственно понятия и подходы, связанные с вырожденными подстановками. Сегодня, возвращаясь к затронутым в работе [21] вопросам, хочется отметить, что обоснование мощности подстановок, названных в работе вырожденными, выполненное на основе формул для законов распределения переходов XOR таблиц и таблиц линейных аппроксимаций представляется не совсем аккуратным. Более последовательным и правильным следует считать использование для оценки множества вырожденных подстановок законов распределения максимумов переходов соответствующих таблиц, рассчитанных в нашей работе [22]. В этой работе можно найти и дополнительные аргументы, относящиеся к обоснованию математической модели случайной подстановки. Далее в рамках введенного в работе [22] понятия математической модели случайной подстановки обсуждаются свойства и особенности подмножества подстановок вырожденного типа.

3 МАТЕРИАЛЫ И МЕТОДЫ

Общим подходом, который развивается в этой работе, является построение поцикловых распределений максимумов таблиц дифференциальных разностей и таблиц линейных аппроксимаций для уменьшенных моделей шифров, в качестве которых рассматривается шифр из работы Хеуса и шифр Rijndael [1] (первый шифр имеет слабое линейное преобразование, а второй – сильное линейное преобразование). Многочисленные исследования уменьшенных моделей современных шифров [11–16 и мн. др.] показали, что с S-блоками, построенными по предложениям разработчиков шифра, Rijndael приходит к состоянию случайной подстановки по дифференциальным показателям за три цикла, а по линейным показателям – за четыре. С другими конструкциями S-блоков (из других шифров, в том числе и случайных S-блоков) приход Rijndael-я к случайной подстановке по дифференциальным показателям затягивается до 5-ти циклов. Шифру Хеуса для прихода к состоянию случайной подстановки для различных S-блоков (от рекомендованных конструкций до случайных S-блоков) достаточно выполнить от 6-ти до 9-ти циклов шифрования.

Нам потребуются и материалы из работы [21], приведенные далее в разделе эксперименты, в которой обсуждаются подходы к обоснованию модели случайной подстановки. Заодно мы выполним уточнение некоторых моментов.

Мы будем интересоваться числом циклов шифрования, после которого шифр приходит к показателям случайной подстановки, т.е. основным методом исследований будет построение для шифров с разными S-блоками поцикловых законов распределения максимумов полных дифференциалов и линейных корпусов. Основным инструментом исследований будет изучение законов рас-

пределения максимумов переходов дифференциальных и линейных таблиц постановок. Будет выполнена оценка доли вырожденных байтовых подстановок в общем множестве подстановок симметрической группы.

В данном случае вырожденными случайными подстановками будут считаться подстановки, которые не укладываются в рамки приведенных в работе [1 и др.] подстановок, примененных в ряде современных шифров, и модели случайной подстановки, обоснованной в работе [22].

4 ЭКСПЕРИМЕНТЫ

Здесь, как уже было отмечено выше, представляются результаты экспериментов с малыми (16-битными) моделями шифров. Соответственно разговор будет идти о полубайтовых S-блоках, изученных наиболее всесторонне и глубоко [23, 24]. Для каждого шифра с фиксированным числом циклов шифрования выполнялся расчет поцикловых распределений максимумов переходов XOR таблиц и смещений таблиц линейных аппроксимаций для 30 различных ключей зашифрования, сгенерированных случайным образом, а потом результаты усреднялись.

Мы здесь воспользуемся примерами вырожденных подстановок и результатами экспериментов из работы [21] с полубайтовыми S-блоками. Эксперименты показывают, что к вырожденным подстановкам (S-блокам) следует отнести, прежде всего, подстановки с предельными (максимальными) значениями дифференциальных переходов и (или) смещений (полубайтовые подстановки имеют максимальное значение дифференциального перехода равное 16 (2^n) для XOR таблиц и значение 8 (2^{n-1}) для таблиц линейных аппроксимаций). В табл. 1 и табл. 2, заимствованных из работы [21], мы представляем поцикловое поведение значений максимумов полных дифференциалов и значений максимумов смещений ЛАТ 16-ти битного шифра Хеуса из работы [25] (шифра со слабым линейным преобразованием).

В качестве первого примера взята тождественная подстановка (единичная подстановка симметрической группы). Эта подстановка имеет максимально возможное значение перехода дифференциальной таблицы равное 16 и максимально возможное значение смещения таблицы линейных аппроксимаций равное 8-ми (нелинейность равна нулю!). Результаты ее применения для построения процедуры зашифрования (шифра) приведены в верхней части таблицы 1 (первый пример). Этот пример ярко свидетельствует, что без применения подстановочной нелинейной операции шифр (любой) просто разваливается.

Второй и третий примеры подстановок свидетельствуют, что действительно существуют и не тождественные подстановки со значением показателя максимума смещения линейной аппроксимационной таблицы (ЛАТ) равному 8 (максимально возможному значению для полубайтовой подстановки), которые также не позволяют реализовать эффективную процедуру зашифрования. Заметим, что вторая подстановка приходит к асимптотическому значению максимума таблицы дифференциалов (ТД) равному 24, отличающемуся от теоретического значения максимума дифференциала для случайной подстановки (18–20).

В таблице 2 представлены результаты поцикловой оценки максимумов смещений таблиц линейных аппроксимаций (линейных оболочек) шифра Хеуса с этими же подстановка ми, которые рассматривались выше. И в этом случае результаты свидетельствуют о практической непригодности рассмотренных первых двух подстановок для построения шифрую щих преобразований. Последняя подстановка приходит к показателям случайной подстановки после 7-ми циклов, однако, для достижения необходимых дифференциальных свойств (см. табл. 1) ей требуется более 11-ти циклов зашифрования. В то же время здесь можно сослаться на результаты работ [26, 27 и др.], из которых следует, что случайно взятые подстановки с одновременно не максимальными значениями дифференциальных и линейных переходов с большой вероятностью приводят к эффективному шифрующему преобразованию. Число циклов, необходимое для перехода к случайной подстановке, например, для шифра Хеуса, не превышает 6-ти.

Таблица 1 – Поцикловые значения максимумов полных дифференциалов (XOR таблиц) шифра Хеуса с вырожденными S-блоками

№ п/п	Подстановка	Значения максимумов ТР в зависимости от числа циклов					
1	Тождественная подстановка	Число циклов					
	1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15)	1	2	3	4	5	6
		57617,1	50364,4	45675,6	40971,4	37338,8	39267,0
		Число циклов					
		7	8	9	10	11	12
		41487,8	43386,5	44803,1	46411,4	47075,4	47872,9
2	Подстановка 14 из работы [22]	Число циклов					
	5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12)	1	2	3	4	5	6
		32768	16384	5043,2	1327,87	369,60	151,07
		Число циклов					
		7	8	9	10	11	12
		61,53	32,60	24,20	23,87	23,93	24,13
3	Подстановка 1 из работы [5]	Число циклов					
	C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3)	1	2	3	4	5	6
		49152,0	27648,0	15552,0	3616,00	1016,0	451,27
		Число циклов					
		7	8	9	10	11	12
		209,27	106,60	53,07	27,53	20,07	19,07

Далее мы опять напоминаем результаты из работы [21].

В табл. 3 приведены поцикловые распределения максимумов числа переходов XOR таблиц для шифров с сильным линейным преобразованием. Они вычисляются с помощью уменьшенной (16-битной) конструкции шифра Rijndael, в котором используются те же

S-блоки, что и в предыдущих экспериментах. Первая вырожденная подстановка (тождественная) конечно и в этом случае приводит к развалу процедуры шифрования. В тоже время другие две подстановки (по крайней мере, последняя) на 11-ти циклах выходят к свойствам случайной. Однако, это все равно плохие подстановки.

Таблица 4 иллюстрирует. поцикловые значения максимумов смещений ЛАТ для уменьшенной модели Rijndael с вырожденными S-блоками. По данным этой таблицы вторая подстановка повторяет показатели, продемонстрированные шифром Хеуса (см. табл. 3). Она явно не подходит для построения шифра. В целом, все три подстановки (с показателями нелинейности равными 8-ми) следует отнести к вырожденным подстановкам.

Вырожденными могут быть подстановки и с не максимальными значениями дифференциальных и (или) линейных показателей (близкими к предельным). Пример такой подстановки представлен в табл. 5 и табл. 6.

В этом случае шифр пришел к другому стационарному значению равному 24. Это второй пример подстановки с таким свойством (см. табл. 1). Заметим, что при другой конструкции линейного преобразования (линейным преобразованием MixColumn и ShiftRows $GF(2^8)$) шифр приходит к асимптотическому значению, соответствующему случайной подстановке. Нам пока не удалось объяснить этого эффекта. Табл. 6 демонстрирует линейные показатели уменьшенной модели шифра Rijndael с этим же S-блоком (S-блоками). Результат говорит сам за себя. Этот S-блок нельзя применять для построения шифра.

Таблица 2 – Поцикловые значения максимумов смещений ЛАТ для шифра Хеуса с вырожденными S-блоками

№ п/п	Подстановка	Значения максимумов ЛАТ в зависимости от числа циклов					
1	Тождественная подстановка	Число циклов					
	0,1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15)	1	2	3	4	5	6
		32768	32768	32768	32768	32768	32768
		Число циклов					
		7	8	9	10	11	12
		32768	32768	32768	32768	32768	32768
2	Подстановка 14 из работы [22]	Число циклов					
	5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12)	1	2	3	4	5	6
		32768	32768	32768	32768	32768	32768
		Число циклов					
		7	8	9	10	11	12
		32768	32768	32768	32768	32768	32768
3	Подстановка 1 из работы [5]	Число циклов					
	C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3)	1	2	3	4	5	6
		32768	24576	12288	5233,1	2040,2	1077,7
		Число циклов					
		7	8	9	10	11	12
		839,7	821,7	830	811,3	834,4	806,6

Таблица 3 – Поцикловые значения максимумов полных дифференциалов (XOR таблиц) для уменьшенной модели шифра Rijndael с вырожденными S-блоками

№ п/п	Подстановка	Значения максимумов ТР в зависимости от числа циклов					
1	Тождественная подстановка	Число циклов					
	1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15)	1	2	3	4	5	6
		57617,1	50364,4	45675,6	40971,4	37338,8	39267,0
		Число циклов					
		7	8	9	10	11	12
		41487,8	43386,5	44803,1	46411,4	47075,4	47872,9
2	Подстановка 14 из работы [22]	Число циклов					
	5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12)	1	2	3	4	5	6
		32768	16384	5043,20	1327,87	369,60	151,07
		Число циклов					
		7	8	9	10	11	12
		61,53	32,60	24,20	23,87	23,93	24,13
3	Подстановка 1 из работы [5]	Число циклов					
	C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3)	1	2	3	4	5	6
		49152	15552,0	1686,6	500,00	70,00	19,253
		Число циклов					
		7	8	9	10	11	12
		19,07	19,613	18,80	19,527	19,61	19,37

Таблица 4 – Поцикловые значения максимумов смещений ЛАТ для уменьшенной модели Rijndael с вырожденными S-блоками.

№ п/п	Подстановки	Число циклов					
1	Тождественная подстановка	Значения максимумов ЛАТ в зависимости от числа циклов					
	1,2,3,4,5,6,7,8,9,1A,B,C,D,E,F ЛАТ – 8, ДТ – 16 (15)	1	2	3	4	5	6
		32768	32768	32768	32768	32768	32768
		Число циклов					
		7	8	9	10	11	12
		32768	32768	32768	32768	32768	32768
2	Подстановка 14 из работы [22]	Число циклов					
	5,A,C,6,0,F,3,9,8,D,B,1,7,2,E,4 ЛАТ – 8, ДТ – 8 (12)	1	2	3	4	5	6
		32768	32768	32768	32768	32768	32768
		Число циклов					
		7	8	9	10	11	12
		32768	32768	32768	32768	32768	32768
3	Подстановка 1 из работы [5]	Число циклов					
	C,D,5,1,A,B,6,2,E,3,7,F,4,0,8,9 ЛАТ – 8, ДТ – 12 (3)	1	2	3	4	5	6
		32768	24576	12288	5244	2044	1080
		Число циклов					
		7	8	9	10	11	12
		792	872	826	816	842	816

Таблица 5 – Поцикловые значения максимумов полных дифференциалов (XOR таблиц) уменьшенной версии шифра Rijndael с вырожденными S-блоками

№ п/п	Подстановки	Число циклов					
4	Подстановка	Значения максимумов ТДР в зависимости от числа циклов					
	C,9,4,6,8,E,D,5,3,F,B,0,A,2,1,7 ЛАТ – 6, ДТ – 8 (5)	1	2	3	4	5	6
		32768,0	1536,0	139,07	23,53	24,20	23,73
		Число циклов					
		7	8	9	10	11	12
		23,80	24,07	23,80	23,93	24,00	23,80

Таблица 6 – Поцикловые значения максимумов смещений ЛАТ для уменьшенной модели шифра Rijndael с вырожденными S-блоками

№ п/п	Подстановка	Значения максимумов ЛАТ в зависимости от числа циклов					
4		Число циклов					
	C,9,4,6,8,E,D,5,3,F,B,0,A,2,1,7 ЛАТ – 6, ДТ – 8 (5)	1	2	3	4	5	6
		32768,0	32768,0	32768,0	32768,0	32768,0	32768,0
		Число циклов					
		7	8	9	10	11	12
		32768,0	32768,0	32768,0	32768,0	32768,0	32768,0

Многочисленные эксперименты с уменьшенными моделями шифров [1, 11–15, 25, 27 и др.] (и с полноцикловыми версиями шифров в режиме их активизации 16-битными входными и выходными блоками данных) свидетельствуют о том, что если в шифрах используются S-блоки не с максимальными значениями дифференциальных и линейных переходов, все шифры приходят к одним и тем же средним значениям максимумов дифференциальной и линейной вероятностей, характерными для случайных подстановок соответствующей степени [1]. Результаты свидетельствуют, что по всем рассмотренным шифрам для перехода к асимптотическому значению смещения требуется 4-5 циклов. Видно также, что использование S-блоков с высокими показателями нелинейности дает выигрыш в динамике выхода к асимптотическому значению в пределах одного цикла.

5 РЕЗУЛЬТАТЫ

Оценка доли вырожденных подстановок среди подстановок симметрической группы. Вторая часть работы посвящена оценке доли вырожденных подстановок среди подстановок симметрической группы

Здесь мы покажем, что вероятность попасть на вырожденную подстановку при их случайном формировании весьма мала.

Приведем здесь расчеты закона распределения максимумов XOR переходов байтовой подстановки, полученного в работе [19]. Напомним, что в этом случае сам закон распределения максимумов переходов XOR таблицы имеет вид

$$D_{\max}(X) \approx e^{-e^{\frac{10-2\cdot X}{0,87}}}. \quad (1)$$

При выводе этой формулы полагалось, что переходы таблицы XOR разностей байтовой подстановки представляют собой выборку (набор) из случайных значений, распределенных по Пуассоновскому закону. Результаты расчетов иллюстрирует табл. 7.

Из представленных результатов следует, что распределение сосредоточено в двух целочисленных значениях 10 и 12. При этом в более половины случаев на выходе генератора случайных подстановок формируются подстановки со значением максимума 12, далее, более 30% подстановок имеют максимумом значение 10. На остальные значения максимумов дифференциальных переходов приходится около 10% подстановок [28].

Вероятность получить подстановки со значениями максимумов равными 8-ми близка к 0,00004 и резко уменьшается при дальнейшем уменьшении значения максимума. Соответственно увеличенные до 20 расчетные значения максимума также получаются малыми (менее 10^{-5}) и резко уменьшаются при дальнейшем увеличении максимума.

Аналогичным путем можно выполнить оценку вероятности порождения случайной подстановки с теоретически максимально возможным значением перехода линейной аппроксимационной таблицы подстановки. Для этого случая в работе [19] получен закон распределения максимумов смещений байтовой случайной подстановки в виде

$$D_{\max}(Y) \approx e^{-e^{\frac{32-X}{2}}}. \qquad (2)$$

В табл. 8 представлены результаты расчетов по определению распределения значений максимумов смещений линейной аппроксимационной таблицы байтовой подстановки на основе интегрального закона распределения вероятностей (2).

Заметим, что по результатам ранее выполненной теоретической и экспериментальной оценки, значения максимумов смещений линейной аппроксимационной таблицы случайной подстановки степени 2^8 равны 32 (расчет) и 34 (эксперимент) [29]. В нашем случае расчетные максимумы и максимумы, полученные в экспериментах, совпадают и равны 34-м.

Вырожденные подстановки и в первом и во втором случаях попадают в хвосты максимальных значений законов распределений максимумов (1) и (2).

О подстановке под номером 6. В качестве эксперимента мы взяли хорошую полубайтовую подстановку шифра Rijndael [25], и с помощью двух транспозиций воспроизвели в ней переходы 2→4, 3→6 и 4→8 (последний переход уже был в исходной подстановке), имеющиеся в подстановке под номером 6. Полученная в результате этого подстановка (A, 3, 4, 6, B, E, F, 0, 1, 9, D) повторила по своим свойствам подстановку под номером 6 (она имеет максимальный дифференциальный переход равный 8-ми и максимальный линейный переход равный 6-ти, а шифр Rijndael приходит с такой подстановкой к асимптотическому значению максимума дифференциала равному 24), т.е. стала вырожденной. В то же время одна транспозиция в подстановке под номером 6 в цикле, не содержащем отмеченных выше переходов, сделала подстановку невырожденной. Нам не удалось найти признаков, по которым можно делить подстановки на вырожденные и невырожденные для этого случая, однако, нам не удалось найти невырожденные подстановки среди наиболее вероятного множества подстановок, приближающихся по линейным и дифференциальным показателям к показателям случайной подстановки, определяемой законами распределения вероятностей (1) и (2).

Таблица 7 – Распределение максимумов выборки переходов таблицы XOR разностей для подстановок степени 2^8, полученных расчетным путем и результаты эксперимента

k^* (X_1, X_2)	$\Pr(\Lambda_\pi(\Delta X, \Lambda Y) = 2k^*)$	Число максимумов (расчет)	Эксперимент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	111
12 (12,10)	0,905 – 0,368 = 0,537	137	130
14 (14, 12)	0,9901 – 0,905 = 0,008	22	15
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	1
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0
20 (20,18)	$0,9999999999999 – 0,9999 = 9,99999999\times10^{-5}$	0,0256	0

Таблица 8 – Распределение значений максимумов смещений для множества из 2^8 подстановок, полученных расчетным путем и результаты экспериментов

k^* (X_1, X_2)	$\Pr(\lambda(\alpha,\beta) = \lvert 2k^* \rvert)$	Число значений	Эксперимент
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5,6\ 10^{-4} – 3,4110^{-7} = 5,6\ 10^{-4}$	0,14	0
30 (30,28)	$0,064 – 5,6\ 10^{-4} = 0,0638$	16	14
32 (32,30)	0,368–0,064 = 0,304	78	67
34 (34,32)	0,692 – 0,304 = 0,388	99	108
36 (36,34)	0,874 – 0,692 = 0,181	46	37
38(38,36)	0,9518 – 0,874 = 0,078	19	22
40 (40,38)	0,9821 – 0,9518 = 0,03	8	8
42 (42,40)	0,9933 – 0,9821 = 0,011	3	1
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

6 ОБСУЖДЕНИЕ

Предложен метод теоретической и практической оценки и определения эффективности используемых в шифрах подстановочных преобразований позволяющий проверить пригодность подстановок для построения эффективного шифрующего преобразования.

По сравнению с известными подходами и результатами развиваемый метод оценки эффективности шифрующих преобразований на основе экспериментов с использованием уменьшенных моделей шифров позволяет получить такие оценки при ограниченных вычислительных ресурсах и в приемлемые сроки.

Здесь можно согласиться с тем, что множество допустимых подстановок можно ограничить подстановками, которые укладываются в рамки математической модели случайной подстановки, предложенной в работе [22]. Вырожденных подстановок мало. Основная масса подстановок позволяют реализовать эффективное шифрующее преобразование.

Байтовая подстановка является случайной, если одновременно выполняются два условия [22]:

1) Значение максимума ее XOR таблицы находится в границах 10–12;

2) Значение максимума смещения ее таблицы линейных аппроксимаций находится в границах 32–36.

Эффективность применения разработанного метода подтверждается представленными результатами вычислительных экспериментов и состоит в реализации простой процедуры проверки пригодности S-блоков для применения в БСШ на основе оценки значений максимумов их XOR таблиц и максимумов смещений таблиц линейных аппроксимаций.

К вырожденным S-блокам следует отнести подстановки, попадающие в хвосты максимальных значений законов распределений максимумов (1) и (2).

Представленные примеры вырожденных подстановок ярко свидетельствуют, что S-блоки в шифрах играют весьма важную роль. Существуют подстановки (вырожденного типа), с которыми построить хорошего криптографического преобразования нельзя. С другой стороны, подстановки являются одним из основных элементов шифрующего преобразования. Они реализуют один из важных для шифра механизмов – механизм нелинейного перемешивания (перестановки) битов блоков данных, с помощью которого удается наиболее просто добиться эффекта хаотичности в преобразовании битов данных.

ВЫВОДЫ

В работе решена задача уточнения понятия вырожденной подстановки, и выполнена оценка мощности множества таких подстановок.

К вырожденным S-блокам мы отнесли подстановочные конструкции с дифференциальными и линейными показателями (максимумами XOR таблиц и смещений таблиц линейных аппроксимаций), относящимися к хвостам законов распределений максимумов (близкими к предельно возможным как с одной, так и с другой стороны).

Следует отметить, что на протяжении всех экспериментов нам так и не удалось сгенерировать байтовую вырожденную подстановку.

Научная новизна представленных результатов состоит в том, что изучено влияние вырожденных подстановок на эффективность шифрующих преобразований. Впервые установлено, что использование в шифрах S-блоков, порожденных случайным образом, с очень большой вероятностью не приводит к ухудшению показателей стойкости шифров к атакам дифференциального и линейного криптоанализа.

Практическая значимость результатов работы заключается в получении конкретных данных, подтверждающих основное положение развиваемой новой методики оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа о независимости показателей стойкости шифров от применяемых случайно сгенерированных S-блоков, которые с очень большой вероятностью являются невырожденными.

Подводя итоги приведенным результатам, можно отметить следующие моменты.

Результатами работы подтверждено, что получение вырожденных S-блоков при случайном порождении подстановок является маловероятным событием. Особенно это относится к байтовым S-блокам. Для этих S-блоков получение подстановок с максимумами XOR таблиц и смещений таблиц линейных аппроксимаций, близкими к предельно достижимым, является практически невозможным событием. Реальные наиболее вероятные значения максимумов, которые удается получить в экспериментах для байтовых подстановок это 32–34 для таблиц линейных аппроксимаций и 10-12 для таблиц XOR разностей. Они оказываются далекими от предельных значений $2^{8-1}=128$ (для ЛАТ) и $2^{8}=256$ (для таблиц разностей), характерных для вырожденных подстановок. При этом с увеличением значений максимумов линейных и дифференциальных показателей (переходов) вероятности отбора подстановок с такими значениями очень быстро уменьшаются. Таким образом, доля вырожденных подстановок в общем множестве подстановок симметрической группы оказывается весьма малой.

Это значит, что положение, сформулированное в начале работы, состоящее в том, что все шифры независимо от используемых в них S-блоков после небольшого начального числа циклов шифрования становятся случайными подстановками, выполняется с весьма высоким уровнем доверия. Порождение вырожденных S-блоков является очень маловероятным событием, и самое главное они всегда могут быть обнаружены и исключены на основе результатов экспериментов.

Перспективы дальнейших исследований состоят в дальнейшем изучении механизмов формирования переходов таблиц XOR разностей и таблиц линейных аппроксимаций при использовании вырожденных S-блоков, приводящих к нарушению показателей прихода шифров к состоянию случайной подстановки, и, в частности, появления для некоторых S-блоков второго стационарного значения максимумов дифференциальных вероятностей, отличающегося от показателей случайных S-блоков, а также разработка принципов проектирования блочных симметричных шифров, не зависящих от применяемых в них S-блоков.

БЛАГОДАРНОСТИ

Работа выполнена в рамках госбюджетной научно-исследовательской темы Харьковского национального университета им. В. Н. Каразина «Аналіз стану, обґрунтування вимог та напрямків розвитку, стандартизація розробка та впровадження криптографічних систем для надання електронних довірчих послуг» (номер гос. регистрации 0116U000810). Приказ МОН Украины № 158 от 26.02.2016 г.

СПИСОК ЛИТЕРАТУРЫ

1. Долгов В. И. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа: монография / В. И. Долгов, И. В. Лисицкая. – Харьков : Издательство «Форт», 2013. – 420 с.
2. Saier W. Nonlinearity criteria for cryptographic functions / W. Saier, O. Staffelbach // In Advances in Cryptology. – EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag. – 1990. – Vol. 434. – P. 549–562.
3. Pasalic E. Further Results on the Relation between Nonlinearity and Resiliency for BF / E. Pasalic, T. Johansson // IEEE Trans. on Information Theory. – 2002. – Vol. 48, No. 7, July. – P. 1825–1834.
4. Sillan W. An effective genetic algorithm for finding highly nonlinear Boolean functions / W. Sillan, A. Clark and E. Dawson // In First International Conference on Information and Communications Security, in Lecture Notes in Computer Science, Springer Verlag. – 1997. – Number 1334. – P. 149–158.
5. Sillan W. Smart Hill Climbing Finds Better Boolean Functions / W. Sillan, A. Clark and E. Dawson // Workshop on Selected Areas in Cryptography (SAC'97) Workshop Record. – 1997. – P. 50.
6. Seberry J. Hadamar Matrices, Bent Functions and Cryptography / J. Seberry and X. Zhang. // In J. H. Dinitz and D. R. Stinson, editors, Contemporary Design Theory: A Collection of Surveys, chapter 11, John Wiley and Sons, Inc. – 1995. – P. 431–559.
7. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197) / [И. Д. Горбенко, А. В. Потий, Ю. А. Избенко и др.] // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2004. – № 126. – С. 132–138.
8. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity / [E. Pasalic, T. Johansson, S. Saitra et al.] // In Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.
9. Sillan W. Heuristic Design of Cryptographically Strong Balanced Boolean Functions / W. Sillan, A. Clark and E. Dawson. // In Advances in Cryptology EUROCRYPT'98 Springer Verlag LNCS 1403. – 1998. – P. 489–499.
10. Saity S. Construction of Cryptographically Important Boolean Functions / S. Saity and T. Johansson // In INDOCRYPT 2002, Volume 2551 in Lecture Notes in Computer Science, Springer Verlag – 2002.– P. 234–245.
11. Лисицкая И. В. Методология оценки стойкости блочных симметричных криптопреобразований на основе уменьшенных моделей: дис. … докт. техн. наук: 05.13.05 / Лисицкая Ирина Викторовна. – Харьков, 2012. – 293 с.
12. Долгов В. И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. / В. И. Долгов, А. А. Кузнецов, С. А. Исаев. // Электронное моделирование. – 2011.– Т. 33, № 6. – С. 81–99.
13 Кузнецов А. А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс / А. А. Кузнецов, И. В. Лисицкая, С. А. Исаев // Прикладная радиоэлектроника. – 2011. – Т.10, №2 – С. 135–140.
14. Криптографичекие свойства уменьшенной версии шифра «Калина» / [В. И Долгов, Р. В Олейников, А. Ю. Большаков и др.] // Прикладная радиоэлектроника. – 2010. – № 3. – С. 349–354.
15. Gorbenko I. D. On Ciphers Coming to a Stationary State of Random Substitution / I. D. Gorbenko, K. E. Lisickiy, D. S. Denisov // Universal Journal of Electrical and Electronic Engineering, 2, P. 206–215. DOI. 10.13189/ujeee. 2014.020409.
16. Лисицкий К. Е. Динамические показатели прихода блочных шифров к состоянию случайной подстановки / К. Е. Лисицкий / / Издательский дом LAP LAMBERT Academic Publishing, 2014. – 60 с. ISBN-13. 978-3-659-28919-4.
17. Долгов В. И. Шифры со случайными подстановками / В. И. Долгов, И. В. Лисицкая, К. Е. Лисицкий // Труды международной научно-технической конференции «Компьютерное моделирование в наукоемких технологиях», Харьков, 28–31 мая 2014 г. – С. 120–123.
18. Лисицкий К. Е. Снова об оптимальных S-блоках / К. Е. Лисицкий // Прикладная радиоэлектроника. – 2014. – Том. 13, № 3.– С. 208–212.
19. Горбенко И. Д. Уточненные показатели прихода шифров к состоянию случайной подстановки / И. Д. Горбенко, И. В. Лисицкая, К. Е. Лисицкий // Прикладная радиоэлектроника. – 2014. – Том. 13, № 3.– С. 213–216.
20. Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К. : Держспоживстандарт України, 2015. – 238 с. – (Національний стандарт України).
21. Лисицкая И. В. Вырожденные подстановки / И. В. Лисицкая // Радиотехника. – 2012. – Вып. 171 – С. 31–38.
22. Лисицкая И. В. Уточненная математическая модель случайной подстановки / И. В. Лисицкая, Е. В. Мельничук // Автоматизированные системы управления и приборы автоматики – 2013.– Вып. 162. – С. 22–34.
23. Juhani M. Cryptographic Analysis of All 16-Bit S-Boxes / Markku-Juhani O. Saarinen // Volume 7118 of the series Lecture Notes in Computer Science. – 2008. – P. 118–133.
24. Токарева Н. Н. Квадратичные аппроксимации специального вида для четырехразрядных подстановок в S-блоках / Н. Н. Токарева // Прикладная дискретная математика. – 2008. – Т. 1, № 1. – С. 50–54.
25. Heys H. M. A Tutorial on Linear and Differential Cryptanalysis / H. M. Heys // CRYPTOLOGIA. – 2002. – 26, № 3. – P. 189–221.
26. Лисицкая И. В. Об участии S-блоков в формировании максимальных значений линейных вероятностей блочных симметричных шифров / И. В. Лисицкая, В. В. Ковтун // Межведомственный научн. технический сборник «Радиотехника». – 2011. – Вып. 166. – С. 17–25.
27. Лисицкая И. В. Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / И. В. Лисицкая, А. В. Казимиров // Proceedings International Conference SAIT 2011, Kyiv, Ukraine, May 23–28. – 2011. – P. 459.
28. Дифференциальные свойства подстановок / [Р. В., Олейников, О. И. Олешко, К. Е. Лисицкий и др.] // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 326–333.
29. Долгов В. И. Свойства таблиц линейных аппроксимаций случайных подстановок / В. И. Долгов, И. В. Лисицкая, О. И. Олешко // Прикладная радиоэлектроника. – 2010. – №3. – С. 334–340.

Статья поступила в редакцию 25.01.2017.
После доработки 01.03.2017.

Лисицький К. Є.
Аспірант Харківського національного університету імені В. Н. Каразіна

ВИРОДЖЕНІ S-БЛОКИ

Актуальність. S-блоки є одним з основних перетворень багатьох шифрів, і пошуку S-блоків з удосконаленими криптографічними показниками приділяється величезна увага в літературі цього напряму. Тим самим припускається, що є підстановки (S-блоки), які слід вважати плохими, тобто такі, які не підходять для побудови надійних шифрів. З іншого боку, один з напрямків вдосконалення конструкцій шифрів, який розвивається в останній час, пов'язаний з побудовою шифрів, в яких можуть застосовуватися S-блоки випадкового типу. Виникає важливе питання. А які ж S-блоки не підходять для побудови шифруючих перетворень? У цьому зв'язку велику актуальність набуває вивчення властивостей та особливостей формування S-блоків вироджених конструкцій, під якими розуміються підстановки, що погіршують криптографічні показники шифрів.

Мета. Вивчення властивостей та особливостей формування підстановок виродженого типу, оцінка ймовірності їх породження за допомогою генератора випадкових підстановок. Визначення ознак, за якими можна виділити вироджені підстановки.

Метод. Побудова поциклових законів розподілу максимумів таблиць диференціальних різниць і таблиць лінійних апроксимацій для зменшених моделей шифрів, при використанні в них різних (вироджених) конструкцій S-блоків. Визначення закону розподілу максимумів XOR таблиць і зміщення таблиць лінійних апроксимацій байтових підстановок.

Результати. Вивчені ансамблеві характеристики множини байтових підстановок. На основі вивчення диференціальних та лінійних властивостей зменшених моделей шифрів визначені ознаки, за допомогою яких виявляються вироджені підстановки. Обчислювальним і експериментальним шляхом визначається ймовірність випадкового породження (вибору) байтової підстановки виродженого типу.

Висновки. Результатами роботи підтверджено, що отримання вироджених байтових S-блоків при випадковому їх породженні є малоймовірною подією. Це означає, що практично без обмежень у шифрах можуть використовуватися S-блоки, породжені з допомогою генератора випадкових підстановок.

Наукова новизна міститься в тому, що вивчений вплив вироджених підстановок на ефективність шифруючих перетворень. Вперше встановлено, що використання в шифрах S-блоків, породжених випадковим чином, з дуже великою ймовірністю не призводить до погіршення показників стійкості шифрів до атак диференціального та лінійного криптоаналізу.

Практична значимість результатів роботи скадається в отриманні конкретних даних, що підтверджують основне положення розробленої нової методики оцінки стійкості блочних симетричних шифрів до атак диференціального та лінійного криптоаналізу про незалежність показників стійкості шифрів від використовуваних S-блоків, у тому числі й S-блоків випадкового типу.

Ключові слова: методологія оцінки стійкості, вироджені підстановки, диференціальні показники, лінійні показники.

Lisickiy K. E.
Post-graduate student of Kharkiv National University named by V. N. Karazina

DEGENERATE S-BOXES

Context. S-blocks are one of the main transformations of many ciphers, and the search for S-boxes with improved cryptographic indices a great deal of attention in the literature of this direction is paid. Thus, it that there are permutations (S-blocks), which should be considered bad is assumed, i.e. those that are not suitable for building reliable ciphers. On the other hand, one of the directions for improving the design of ciphers, which has been developing recently, with the construction of ciphers is connected, in which S-blocks of random type can be used. There is an important question. Which S-boxes are not suitable for building encryption transformations? In this connection, the study of the properties and features of the formation of S-blocks of degenerate structures, which are interpretations that degrade the cryptographic exponents of ciphers, is becoming increasingly important.

Objective. A study of the properties and features of the formation of permutations of a degenerate type, an estimate of the probability of their generation with the aid of a random permutation generator. Determination of the characteristics by which degenerate substitutions can distinguished.

Method. Construction of the piecemeal laws of the distribution of the maxima of tables of differential differences and tables of linear approximations for reduced models of ciphers, using different (degenerate) S-block constructions in them. Determination of the law of distribution of maxima of XOR tables and shifts of tables of linear approximations of byte permutations.

Results. The ensemble characteristics of the set of byte substitutions are studied. Based on the study of the differential and linear properties of the reduced models of ciphers, the characteristics by which degenerate substitutions can identified are determined. The probability of random generation (by choice) of a byte substitution of a degenerate type is determined computationally and experimentally.

Conclusions. The results of the work confirmed that obtaining degenerate byte S-blocks for their random generation is an unlikely event. This means that almost without restrictions in the ciphers, S-blocks can used, generating with the help of the generator of random substitutions.

The scientific novelty of the presented results is that the influence of degenerate permutations on the efficiency of encryption transformations has studied. For the first time it established that, the use of S-blocks generated randomly in ciphers with a very high probability does not lead to a deterioration in the ciphers' resistance to differential and linear cryptanalysis attacks.

The practical significance of the results of the work seen in the receipt of specific data confirming the main position of the new technique developed to assess the stability of block symmetric ciphers to attacks of differential and linear cryptanalysis on the independence of cipher strength indicators from the applied S-blocks, including S-blocks of random type.

Keywords: methodology of evaluation of resistance, degenerate substitution, differential indicators, linear indicators.

REFERENCES

1. Dolgov V. I., Lisickaya I. V. Metodologiya ocenki stojkosti blochnyh simmetrichnyh shifrov k atakam differencial'nogo i linejnogo kriptoanaliza: monografiya. Har'kov, Izdatel'stvo "Fort", 2013, 420 p.
2. Saier W., Staffelbach O. Nonlinearity criteria for cryptographic functions, *In Advances in Cryptology – EUROCRYPT'89, Lecture Notes in Computer Science*. Springer-Verlag, 1990, Vol. 434, pp. 549–562.
3. Pasalic E., Johansson T. Further Results on the Relation between Nonlinearity and Resiliency for BF, *IEEE Trans. on Information Theory*, 2002, Vol. 48, No. 7, July, P. 1825–1834.
4. Sillan W., Clark A. and Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean functions, *In First International Conference on Information and Communications Security, in Lecture Notes in Computer Science,* Springer Verlag, 1997, Number 1334, pp. 149–158.

5. Sillan W., Clark A. and Dawson E. Smart Hill Climbing Finds Better Boolean Functions, *Workshop on Selected Areas in Cryptography (SAC'97) Workshop Record*, 1997, P. 50.
6. Seberry J., Zhang X. Hadamar Matrices, Bent Functions and Cryptography, *In J. H. Dinitz and D. R. Stinson, editors, Contemporary Design Theory: A Collection of Surveys, chapter 11, John Wiley and Sons, Inc*, 1995, pp. 431–559.
7. Gorbenko I. D., Potij A. V., Izbenko Yu. A. i dr. Issledovanie analiticheskih i statisticheskih svojstv bulevyh funkcij kriptoalgoritma Rijndael (FIPS 197), *Radiotehnika. Vseukr. Mejvedomstvenyj nauchno tehnicheskij sbornik*, 2004, No. 126, pp. 132–138.
8. Pasalic E., Johansson T., Saitra S. et al. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity, *In Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics*. Elsevier, January 2001.
9. Sillan W., Clark A. and Dawson E. Heuristic Design of Cryptographically Strong Balanced Boolean Functions, *In Advances in Cryptology EUROCRYPT'98 Springer Verlag LNCS 1403*, 1998, pp. 489–499.
10. Saity S., Johansson T. Construction of Cryptographically Important Boolean Functions, *In INDOCRYPT 2002, Volume 2551 in Lecture Notes in Computer Science, Springer Verlag*, 2002, pp. 234–245
11. Lisickaya I. V. Metodologiya ocenki stojkosti blochnyh simmetrichnyh kriptopreobrazovanij na osnove umen'shenyh modelej: dis. … doct. tehnich. nauk 05.13.05. Har'kov, 2012, 293 p.
12. Dolgov V. I., Kuznecov A. A., Isaev S. A. Differencial'nye svojstva blochnyh simmetrichnyh shifrov, predstavlennyh na ukrainskij konkurs, *Elektronnoe modelirovanie,* 2011, Vol. 33, No. 6, pp. 81–99.
13. Kuznecov A. A., Dolgov V. I., Isaev S. A. Linejnye svojstva blochnyh simmetrichnyh shifrov, predstavlennyh na ukrainskij konkurs, *Prikladnaya Radioelektronika*, 2011, Vol. 10, No. 2, pp. 135–140.
14. Dolgov V. I., Olejnikov R. V., Bolshakov A. UI. i dr Kriptograficheskie svojstva umen'shenoj versii shifra «Kalina», *Prikladnaya Radioelektronika*, 2010, Vol.10, No. 3, pp. 135–140.
15. Gorbenko I. D., Lisickiy K. E., Denisov D. S. On Ciphers Coming to a Stationary State of Random Substitution, *Universal Journal of Electrical and Electronic Engineering*, 2, pp. 206–215. DOI. 10.13189/ujeee. 2014.020409.
16. Lisickij K. E. Dinamicheskie pokazateli prihoda blochnyh shifrov k sostoyaniyu sluchajnoj podstanovki, *Izdatel'stvo dom LAP LAMBERT Academic Publishing,* 2014, 60 p. ISBN-13-978-3-659-28919-4.
17. Dolgov V. I., Lisickaya I. V., Lisickij K. E. Shifry so sluchajnumi podstanjvkami, *Trudy mejvedomstvennoj mejdynarodnoj nauchno tegnicheskoj konferencii "Komp'uiternoe modelirovanie v naukoiomkih tehnologiyah"*. Har'kov, 28–31 maua 2014 y, pp. 120–123.
18. Lisickij K. E. Snova ob optimal'nyh S-blokah, *Prikladnaya radioelektronika, HTURE*, 2014, Том. 13, No. 3, pp. 208–212.
19. Gorbenko I. D., Lisickaya I. V., Lisickij K. E. Utochneonnye pokazateli prihoda shifrov k sostoyaniyu sluchajnoj podstanovki, *Prikladnaya radioelektronika*, 2014, Том. 13, No. 3, pp. 213–216.
20. Informacijni tehnologii. Kriptografichnyj zahyst informacii. Algoritm symmetrichnogo blokovogo peretvorennya: ДСТУ 7624:2014. Kiev, Derzhspozhyvstandart Ukrainu, 2015, 238 p. (Nacional'nyj standart Ukrainy).
21. Lisickaya I. V. Vyrozhdennye podstanovki, *Radiotehnika,* 2012, Vyp. 171, pp. 31–38.
22. Lisickij K. E. On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers , *I. J. Computer Network and Information* Security, 2014, 1, 11–18 Published Online November 2013 in MECS (http://www.mecs-press.org/). DOI: 10.5815/ijcnis. 2014.01.02.
23. Markku-Juhani O. Saarinen Cryptographic Analysis of All 16-Bit S-Boxes, *Of the series Lecture Notes in Computer Science,* 2008, Volume 7118, pp. 118–133.
24. Tokareva N. N. Kvadratichnye approksimacii sgecial'nogo vida dlya cheturehrozryadneh podstanovok v S-blokah, *Prikladnaya diskretnaya matematika*, 2008, Vol. 1, No. 1, pp. 50–54.
25. Heys H. M. A Tutorial on Linear and Differential Cryptanalysis, *CRYPTOLOGIA*, 2002, Vol. 26, No. 3, pp. 189–221.
26. Lisickaya I. V., Kovtun V. V. Ob uchastii S-blokov v formirovanii maksimal'nyh znachenij linejnyh veroyatnostej blochnyh simmetrichnyh shifrov, *Mejvedomstvennyj nauchno tegnicheskoj sbornik "Radiotehnika"*, 2011, Vyp 166, pp. 17–25.
27. Lisickaya I. V., Kazimirov A. V. Ob uchastii S-blokov v formirovanii maksimal'nyh znachenij differencial'nyh veroyatnostej blochnyh simmetrichnyh shifrov, *Proceedings International Conference SAIT 2011, Kyiv, Ukraine, May 23–28*, 2011, P. 459.
28. Olejnikov R. V., Oleshko O. I., Lisickij K. E. i dr. Differencial'nye svojstva podstanovok, *Prikladnaya diskretnaya matematika*, 2010, Tom 9, No. 1, pp. 50–54.
29. Dolgov V. I., Lisickaya I. V., Oleshko O. I. Svojstva tablic linejnyh approksimacihj sluchajnyh podstanovok, *Prikladnaya Radioelektronika*, 2010, No. 3, pp. 334–340.