УДК 004.853

С.В. Поликарпов, А.А. Кожевников

ПСЕВДО-ДИНАМИЧЕСКИЕ ПОДСТАНОВКИ: ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ СВОЙСТВ*

Применение в симметричных криптоалгоритмах псевдо-динамических подстановок PD-sbox позволяет совместить сильные стороны фиксированных подстановок (высокая скорость работы и эффективность использования вычислительных ресурсов) и динамических подстановок (нейтрализация статистических методов криптоанализа). Для оптимального применения псевдо-динамических подстановок требуется детальное исследование и обоснование их криптографических свойств. Цель исследования – приблизительное определение линейных свойств полноразмерных псевдо-динамических подстановок на основе экстраполяции вычисленных линейных свойств малоразмерных псевдо-динамических подстановок, сформированных случайным образом. Исследованы линейные свойства малоразмерных псевдо-динамических подстановок, формируемых случайным образом. Для этого определены максимальные значения смещения вероятности аппроксимации подстановки линейными функциями $\max bias(\alpha, \beta)$ *по каждому заданному наборов параметров PD-sbox. С целью упрощения анализа полученных результатов определены усреднённые значения максимумов смещения* $avg\,(\max bias(\alpha, \beta))$*. Это позволило определить простую закономерность между параметрами PD-sbox и вероятностью получения максимальных значений смещения* $\max bias(\alpha, \beta)$ *при случайном формировании PD-sbox. Выявленная закономерность позволила приблизительно экстраполировать линейные свойства малоразмерных псевдо-динамических подстановок на линейные свойства полноразмерных псевдо-динамических подстановок. Проведённая оценка сложности линейного криптоанализа, выраженного в количестве необходимых пар «открытый текст – шифротекст», показала, что имеется потенциальная возможность по синтезу симметричных блочных криптоалгоритмов на основе псевдо-динамических подстановок PD-sbox с экстремально низкими значениями смещения* $bias(\alpha, \beta)$*, для которых можно обосновать нижний порог сложности линейного криптоанализа.*

Линейный криптоанализ; динамические подстановки; псевдо-динамические подстановки PD-sbox.

S.V. Polikarpov, A.A. Kozhevnikov

PSEUDO-DYNAMIC SUBSTITUTIONS: RESEARCH OF LINEAR PROPERTIES

Use of the pseudo-dynamic substitutions PD-sbox in symmetric cryptoalgorithms allows to combine the strengths of the fixed substitutions (high speed and efficient use of computational resources) and dynamic substitutions (neutralization of statistical methods of cryptanalysis). For optimal use of the pseudo-dynamic substitutions is necessary a detailed investigation and study of cryptographic properties. The purpose of the study – an approximate determination of the linear properties of full-size pseudo-dynamic substitutions based on the extrapolation of the linear properties of small pseudo-dynamic substitutions. Linear properties for small-sized pseudo-dynamic substitutions (that are generated randomly) are investigated. For this were determined the maximum values for the bias of probability approximation of investigated substitutions by linear functions. To simplify the analysis of the results were determined average values of the maxima for bias. This allowed to determine a simple relationship between the parameters of PD-sbox and the probability of obtaining maximum values for bias. The revealed dependence allowed to extrapolate linear properties of small-size pseudo-dynamic substitutions to linear properties of full-size

* Работа выполнена на основе гос. задания Минобрнауки РФ № 213.01-11/2014-9.

pseudo-dynamic substitutions. The evaluation of the complexity of linear cryptanalysis, defined in the amount of required pairs of "plaintext – ciphertext", showed that there is potential for the synthesis of symmetric block encryption algorithms with extremely low values of bias, for which can be proved the lower threshold of the complexity of linear cryptanalysis.

Linear cryptanalysis; dynamic substitution; pseudo-dynamic substitution PD-sbox.

Введение. Для оценки стойкости современных вычислительно стойких блочных криптоалгоритмов широко применяются методы линейного и дифференциального криптоанализов, а так же их производные [13]. Отметим, что рассмотрении линейного и дифференциального криптоанализов используют статистические свойства криптографических операций, что наиболее эффективно при **фиксированных** подстановках и раундовых ключах [2, 3]. В блочных криптоалгоритмах основным способом нейтрализации линейного и дифференциального криптоанализов является применение более 8 раундов шифрования, более эффективных операций перемешивания и подбор подстановок с максимальными характеристиками: максимальной нелинейностью, минимальными автокорреляционными характеристиками и другие [4–7].

Несмотря на существование стандартов блочного шифрования – ГОСТ 28147-89 (Российский стандарт шифрования) [8] и AES (стандарт шифрования в США) [9], методам синтеза фиксированных подстановок (блоков замены) уделяется пристальное внимание, поскольку они должны одновременно удовлетворять ряду криптографических свойств [1, 10–12]. Типичный случай заключается в том, что синтезированная подстановка по одним характеристикам может имеет высокие показатели, а по другим – низкие [6, 10].

Проблема усугубляется тем, что даже теоретически не может быть фиксированных подстановок, обладающих идеальными линейными и дифференциальными свойствами [13].

Однако, другим очевидным приёмом нейтрализации линейного и дифференциального криптоанализов является применение динамических подстановок, которые могут менять своё содержимое в зависимости от значения ключа или в процессе шифрования [14–16]. Но это решение сталкивается с необходимостью обеспечения:

- однозначности и обратимости криптографических преобразований для законных пользователей;
- обоснования криптографических свойств предлагаемых решений;
- обеспечения приемлемой сложности реализации и скорости шифрования информации.

Большинство исследований по применению динамических подстановок рассматривают вариант ключезависимых подстановок (Key-Dependent Sbox) – формирование подстановок в зависимости от значения криптографического ключа [14–16]. Известен ряд криптографических алгоритмов, использующих данный вариант [17–19]. Однако, это не даёт им значительных преимуществ перед известными аналогами [4, 20]. Мало того, появились техники восстановления содержимого ключезависимых подстановок [20].

Исследования последних лет сосредоточены на доработке криптоалгоритма AES и его модификаций путём ввода ключезависимых подстановок. Основной такого подхода является следующее предположение — если криптоаналитику не известно точное содержимое подстановок, то сложность криптоанализа значительно увеличивается. В основном, в исследованиях приводят свойства *отдельных* формируемых ключезависимых подстановок и по оценке их криптографических свойств делается вывод о положительном эффекте от их применения. Недостатком

такого подхода является отсутствие теоретического обоснования или результатов моделирования, показывающих криптографические свойства *ансамбля* формируемых подстановок в целом [14–16].

Наиболее сложным подходом является обеспечение полноценного динамизма – когда содержимое подстановки изменяется как от значения криптографического ключа, так и от энтропии шифруемой информации. Ярким примером является известный криптоалгоритм RC4 [21], который из-за слабых криптографических свойств [22, 23] не рекомендуется к использованию [24]. Пример криптоалгоритма RC4 наглядно показывает, что применение динамических подстановок не делает автоматически криптоалгоритм стойким к криптографическим атакам.

Таким образом, само по себе применение динамических подстановок не гарантирует значительного снижения эффективности линейного и дифференциального криптоанализов. Эффект может быть достигнут только при достижении динамическими подстановками статистических характеристик, приближающихся к идеальным (в условиях равновероятного динамического изменения подстановки).

Для обхода ограничений, присущих известным динамическим подстановкам, авторами предложена структура псевдо-динамической подстановки (*Pseudo-Dynamical Sbox* или *PD-sbox*) [25–27]. Предлагаемый подход позволяет совместить сильные стороны фиксированных подстановок (высокая скорость работы и эффективность использования вычислительных ресурсов) и динамических подстановок (нейтрализация статистических методов криптоанализа).

Для эффективного применения *PD-sbox* в криптографических алгоритмах необходимо досконально знать их линейные и дифференциальные свойства. Без методов точного определения линейных и дифференциальных свойств *PD-sbox* затруднительно разработать алгоритм оптимального выбора фиксированных подстановок, составляющих *PD-sbox* и, в дальнейшем, оценить результирующую стойкость криптоалгоритма.

Предполагается, что размерность *PD-sbox* для реальных криптоалгоритмов с учётом значения состояния *S* будет превышать 64 бит. Однако, при такой размерности точно определить линейные и дифференциальные свойства *PD-sbox* с использованием известных методов не представляется возможным.

Известным *частичным* решением такой проблемы является исследование функций с небольшими размерностями входов и выходов с последующей экстраполяцией полученных свойств на полноразмерные функции.

Цель исследования – *приблизительное* определение линейных свойств полноразмерных псевдо-динамических подстановок на основе экстраполяции вычисленных линейных свойств малоразмерных псевдо-динамических подстановок, сформированных случайным образом.

1. Используемые термины и определения

Псевдо-динамическая подстановка PD-sbox – структура из фиксированных подстановок и операций сложения по модулю 2 (побитового XOR), обладающая свойствами как динамических, так и фиксированных подстановок. Выходное значение *PD-sbox* описывается выражением:

$$Y = \bigoplus_{i=0}^{K-1} sbox_i(X \oplus S^i),$$

где *sbox* – фиксированные подстановки с размерностью входа *M* бит; *K* – количество фиксированных подстановок; *X* – входные биты; *Y* – выходные биты; *S* – биты состояния псевдо-динамической подстановки; $\oplus$ – операция сложения по модулю 2.

Входное значение каждой фиксированной подстановки параметризуется своим индивидуальным значением состояния S^i (state), где i – номер фиксированной подстановки (от *0* до *K-1*). Текущее значение состояния $S = \{S^0, S^1, S^2, \ldots, S^{K-1}\}$

задаёт одну подстановку из всего множества возможных подстановок *PD-sbox*. Подстановку, получаемую путём задания конкретного значения состояния *S*, будем называть эквивалентной (порождаемой) подстановкой для *PD-sbox*. Соответственно, количество различных эквивалентных подстановок для *PD-sbox* определяется количеством состояний *S*.

Полноразмерная псевдо-динамическая подстановка PD-sbox – псевдо-динамическая подстановка, предназначенная для применения в полноценных криптографических преобразованиях. Значение $S = K \cdot M$ составляет не менее 64-х бит. Таки образом, размерность входа и выхода фиксированных подстановок *M* составляет от 4-х до 16-и бит и количество фиксированных подстановок превышает 16-и ($K \geq 16$). Конкретные значения этих параметров определяются при синтезе криптоалгоритма с учётом необходимой стойкости и эффективности программной или аппаратной реализаций.

Малоразмерная псевдо-динамическая подстановка PD-sbox – псевдо-динамическая подстановка, предназначенная для детального исследования её криптографических свойств путём численных расчётов, с последующей экстраполяцией полученных свойств на полноразмерную псевдо-динамическую подстановку. Значение $S = K \cdot M$ составляет не более 24-х бит и ограничивается возможностями применяемых вычислительных средств.

Представление PD-sbox в виде большой эквивалентной фиксированной подстановки – представление описания *PD-sbox* в виде большой эквивалентной подстановки с размерностью входа $S = K \cdot M$ бит, где *K* – количество фиксированных подстановок в составе *PD-sbox* и *M* – размерность входа каждой фиксированной подстановки. Данное представление позволяет оценить свойства всего ансамбля формируемых *PD-sbox* эквивалентных подстановок. На рис. 1 показан пример большой эквивалентной подстановки при $K = 2$. Данная подстановка имеет вход размерностью $2 \cdot M$, значения которого получаются конкатенацией отдельных входов $X \oplus S^0$ и $X \oplus S^1$ с размерностью *M* бит.

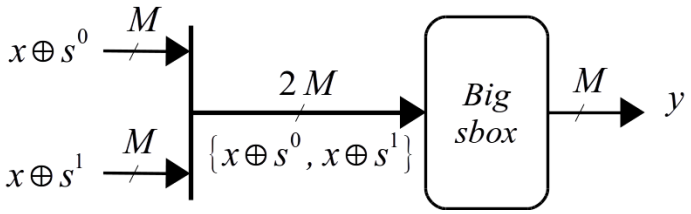

Рис. 1. Представление PD-sbox в виде большой эквивалентной фиксированной подстановки

Значения указанной большой фиксированной эквивалентной подстановки получаются путём перебора всех возможных входных комбинаций $\{X \oplus S^0, X \oplus S^1\}$ и получением выходных значений *Y* на выходе *PD-sbox*.

2. Этапы определения линейных свойств PD-sbox. Основная цель линейного криптоанализа – снизить сложность (нелинейность) криптоалгоритма путём замены (аппроксимации) нелинейных подстановок наиболее вероятным набором линейных функций [2, 5]. Эффективность аппроксимации часто представляют в виде смещения вероятности аппроксимации подстановки линейными функциями

$$\mathrm{bias}(\alpha,\beta) = |\mathrm{p}(\alpha,\beta) - \frac{1}{2}|,$$

которое показывает, на сколько отличается вероятность аппроксимации от равновероятного (идеального с точки зрения стойкости) значения 0,5.

Осуществим приблизительную оценку линейных свойств полноразмерных *PD-sbox* (с размерностью состояния более 64 бит), путём экстраполяции линейных свойств, полученных для малоразмерных *PD-sbox*. Для этого выполним следующие этапы:

- Вычисление матрицы значений $bias(\alpha, \beta)$ малоразмерных *PD-sbox*, состоящих из биективных подстановок и имеющих размерности состояния *S* от 3 до 16 бит.
- Определение максимальных (наихудших) значений смещения $max\ bias(\alpha, \beta)$ в матрице значений $bias(\alpha, \beta)$.
- Оценка распределения максимальных значений смещения $max\ bias(\alpha, \beta)$ для случайно формируемых *PD-sbox.*
- Определение усреднённых значений максимумов смещения *avg (max* $bias(\alpha, \beta)$*).*
- Поиск функции экстраполяции усреднённых значений максимумов смещения *avg (max* $bias(\alpha, \beta)$*)* малоразмерных *PD-sbox* на полноразмерные *PD-sbox.*

Расчёт значений $bias(\alpha, \beta)$ будем осуществлять по приведённому ранее алгоритму [27], используя представление *PD-sbox* в виде большой эквивалентной фиксированной подстановки. Для обеспечения достоверности результатов вычисления значений $bias(\alpha, \beta)$ осуществим набор статистики для каждой комбинации параметров используя $n = 100$ малоразмерных *PD-sbox*, сформированных случайным образом.

3. Результаты определения линейных свойств малоразмерных PD-sbox. В табл. 1 приведены результаты вычисления максимальных значений смещения $max\ bias(\alpha, \beta)$ для случаев $K = 1$, $K = 2$, $K = 3$, $K = 4$ и $K = 5$ при размерности входа $M = 3$ бит. Размерность большой эквивалентной фиксированной подстановки составила от 3 до 15 бит.

Таблица 1

Распределение максимальных значений смещения $max\ bias(\alpha, \beta)$ для случаев $K = 1$, $K = 2$, $K = 3$, $K = 4$ и $K = 5$ при размерности входа $M = 3$ бит

	Количество значений max bias(α, β) при разном количестве *K* фиксированных подстановок в составе PD-sbox				
Значения max bias(α, β)	$K = 1$	$K = 2$	$K = 3$	$K = 4$	$K = 5$
0,03125	-	-	-	1	16
0,0625	-	-	2	29	58
0,125	-	7	55	51	20
0,25	28	81	37	17	6
0,5	72	12	6	2	-

В табл. 2 приведены результаты вычисления максимальных значений смещения $max\ bias(\alpha, \beta)$ для случаев $K = 1$, $K = 2$, $K = 3$ и $K = 4$ при размерности входа $M = 4$ бит. Размерность большой эквивалентной фиксированной подстановки составила от 4 до 16 бит. Для примера приведены значения $max\ bias(\alpha, \beta)$ для случайно формируемых биективных подстановок с размерностями входа и выхода 8 бит (random sbox 8x8).

Таблица 2

Распределение максимальных значений смещения $max\ bias(\alpha, \beta)$ для случаев $K = 1$, $K = 2$, $K = 3$ и $K = 4$ при размерности входа $M = 4$ бит.

	Количество значений max bias(α, β) при разном количестве K фиксированных подстановок в составе PD-sbox				
Значения max bias(α, β)	$K = 1$	$K = 2$	$K = 3$	$K = 4$	random sbox 8x8 бит
0,046875	-	-	-	17	-
0,0625	-	-	-	1	-
0,0703125	-	-	-	69	-
0,09375	-	-	34	-	-
0,105469	-	-	-	13	-
0,125	-	1	3	-	12
0,132812	-	-	-	-	38
0,140625	-	-	57	-	30
0,148438	-	-	-	-	15
0,15625	-	-	-	-	4
0,164062	-	-	-	-	1
0,1875	-	60	2	-	-
0,210938	-	-	4	-	-
0,25	-	8	-	-	-
0,28125	9	29	-	-	-
0,375	87	2	-	-	-
0,5	4	-	-	-	-

На рис. 2 приведено распределение максимальных значений смещения $max\ bias(\alpha, \beta)$.

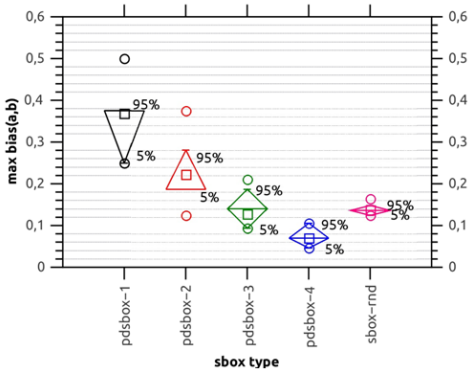

Рис. 2. Ящичковая диаграмма распределения максимальных значений смещения $max\ bias(\alpha, \beta)$ при $M = 4$ бит для разного количества фиксированных подстановок в PD-sbox

Приведённые в табл. 2 результаты показывают, что уже при $K = 4$ и $M = 4$ максимальные значения смещения $max\ bias(\alpha, \beta)$ псевдо-динамических подстановок, формируемых случайным образом, в среднем значительно лучше (меньше) значений смещений $max\ bias(\alpha, \beta)$ для случайных подстановок размерностью 8 бит. Эти значения сопоставимы со значениями $max\ bias(\alpha, \beta)$ специально подобранных 8-ми битных подстановок. Например, значение $max\ bias(\alpha, \beta)$ для подстановки из криптоалгоритма AES составляет 0,0625.

Приведённая ящичковая диаграмма (рис. 2) наглядно показывает динамику уменьшения разброса максимальных значений смещения $max\ bias(\alpha, \beta)$ при увеличении количества фиксированных подстановок в составе *PD-sbox*. Для упрощения анализа получаемых результатов в таблице 3 приведена обобщённая информация по *усреднённым* значениям максимумов смещения *avg (max* $bias(\alpha, \beta)$*)*. Задача оценки отклонения (девиации) значений максимумов смещения в данном исследовании не ставилась.

Таблица 3

Обобщённая информация по усреднённым значениям максимумов смещения *avg (max* $bias(\alpha, \beta)$*)*

	Количество фиксированных подстановок в составе *PD-sbox*			
	$K = 1$	$K = 2$	$K = 3$	$K = 4$
Размерность входа	**3 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,43	0,27125	0,1925	0,1346875
Размерность входа	**4 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,36875	0,2228125	0,12796877	0,070820345
Размерность входа	**5 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,28875	0,14609375	0,067402349	0,030593269
Размерность входа	**6 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,2321875	0,088828104	0,031413568	0,0113983876*
Размерность входа	**7 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,18171875	0,052299787	0,014705499	0,003893524*
Размерность входа	**8 бит**			
Среднее значение $max\ bias(\alpha, \beta)$	0,13781238	0,030178229	0,0062695695*	0,0012979218*

4. Интерпретация полученных результатов. В результате анализа представленных результатов (табл. 3) было получено выражение, позволяющее *приблизительно* определить усреднённые значения максимумов смещения *avg (max* $bias(\alpha, \beta)$*)* для полноразмерных *PD-sbox*, сформированных случайным образом:

$$avg(max\ bias(\alpha,\beta))_K = \frac{avg(\max bias(\alpha,\beta))_{K=3}}{C^K},$$

где

$$C = \frac{avg(max\ bias(\alpha,\beta))_{K=3}}{avg(max\ bias(\alpha,\beta))_{K=4}},$$

отношение между средними значениями *max* $bias(\alpha, \beta)$ *при K= 3 и K= 4.*

В табл. 4 приведены результаты расчёта *приблизительных* усреднённых значений максимумов смещения *avg (max* $bias(\alpha, \beta)$*)* для полноразмерных *PD-sbox* в зависимости от количества *K* фиксированных подстановок в их составе (размерности входов *M* равны 4, 6 и 8 бит).

Таблица 4

Результаты расчёта *приблизительных* усреднённых значений максимумов смещения *avg (max* $bias(\alpha, \beta)$*)* для полноразмерных *PD-sbox*

K	*avg (max* $bias(\alpha, \beta)$*)*		
	M = 4 бит	*M* = 6 бит	*M* = 8 бит
	C = 1,81	*C* = 2,76	*C* = 4,83
4	7,070E-02	1,138E-02	1,298E-03
5	3,906E-02	4,124E-03	2,687E-04
6	2,158E-02	1,494E-03	5,564E-05
7	1,192E-02	5,414E-04	1,152E-05
8	6,587E-03	1,961E-04	2,385E-06
9	3,639E-03	7,107E-05	4,938E-07
10	2,011E-03	2,575E-05	1,022E-07
11	1,111E-03	9,329E-06	2,117E-08
12	6,138E-04	3,380E-06	4,382E-09
13	3,391E-04	1,225E-06	9,073E-10
14	1,873E-04	4,437E-07	1,879E-10
15	1,035E-04	1,608E-07	3,889E-11
16	5,719E-05	5,825E-08	8,052E-12

Соответствующая диаграмма приведена на рис. 3.

Объём информации для успешного осуществления линейного криптоанализа, выражаемый количеством пар «открытый текст – шифротекст», приблизительно можно определить по формуле (при вероятности успеха 97,7 %) [2]:

$$N = \frac{1}{bias(\alpha,\beta)^2}.$$

Следовательно, уменьшение смещения вероятности линейной аппроксимации $bias(\alpha, \beta)$ в 2 раза приводит к увеличению объёма необходимой для успешного криптоанализа информации в 4 раза. При определённом уровне значения смещения $bias(\alpha, \beta)$ необходимое количество пар «открытый текст-шифротекст» будет превышать доступное количество входных-выходных комбинаций блочного преобразования, что сделает этот вид криптоанализа неэффективным.

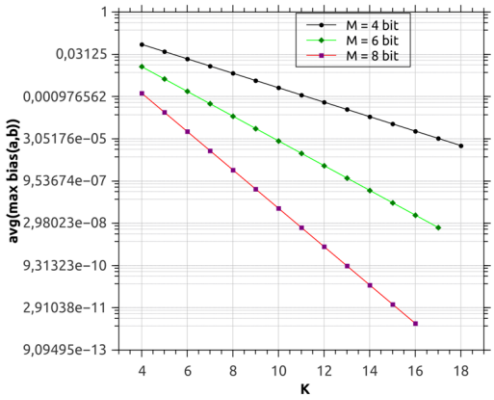

Рис. 3. Результаты расчёта приблизительных усреднённых значений максимумов avg (max bias(α, β)) для полноразмерных PD-sbox

В табл. 5 приведена оценка сложности линейного криптоанализа, полученная на основе результатов из табл. 4.

Таблица 5

Оценка сложности линейного криптоанализа при использовании *PD-sbox*

K	Требуемое количество пар «открытый текст – шифротекст» (при вероятности успеха 97,7 %)		
	M = 4 бит	M = 6 бит	M = 8 бит
4	$> 2^{7}$	$> 2^{12}$	$> 2^{19}$
8	$> 2^{14}$	$> 2^{24}$	$> 2^{37}$
12	$> 2^{21}$	$> 2^{36}$	$> 2^{55}$
16	$> 2^{28}$	$> 2^{48}$	$> 2^{73}$

Выводы. Представление псевдо-динамических подстановок *PD-sbox* виде большой эквивалентной подстановки позволяет учесть вклад управляющего входа *S*, задаваемого секретным криптографическим ключом и определяющего конкретный вид подстановки, что даёт возможность оценить линейные свойства всего ансамбля порождаемых при помощи *PD-sbox* подстановок. Это выгодно отличает псевдо-динамические подстановки *PD-sbox* от ключезависимых и динамических подстановок [14–16, 18].

Результаты, приведённые в табл. 4 и 5, показывают, что путём случайного формирования можно получить полноразмерные псевдо-динамические подстановки *PD-sbox*, обладающие экстремально низкими значениями смещения вероятности линейной аппроксимации $bias(\alpha, \beta)$ и требующие при линейном криптоанализе значительного количества пар «открытый текст-шифротекст».

Стоит отметить, что полноразмерные блочные симметричные криптоалгоритмы обычно имеют раундовую (итерационную) структуру, содержащую в каждом раунде блок подстановочных операций. Знание линейных свойств отдельных подстановок, учитывая размерность обрабатываемого блока информации, не позволяет напрямую определить линейные свойства всего блочного преобразования в целом. Однако, объединяя пораундово в цепочки линейные аппроксимации отдельных подстановок можно экстраполировать линейные свойства подстановок в итоговую линейную характеристику всего блочного преобразования [2].

Линейные характеристики, полученные путём объединения в цепочки линейных аппроксимаций раундовых подстановок обычно не являются самыми оптимальными для линейного криптоанализа. Процесс поиска наилучшего варианта объединения линейных аппроксимаций раундовых подстановок в цепочку является нетривиальной задачей, особенно в условиях значительного (более 8) количества раундов шифрования. Поэтому, ведётся постоянный поиск способов наилучшего объединения в цепочки линейных аппроксимаций раундовых подстановок и совершенствование методов криптоанализа. Этим предопределяется отсутствие для известных симметричных криптоалгоритмов гарантированного нижнего порога сложности для линейного криптоанализа и его производных.

В противовес этому, появляется потенциальная возможность по синтезу симметричных блочных криптоалгоритмов на основе псевдо-динамических подстановок *PD-sbox* с экстремально низкими значениями смещения $bias(\alpha, \beta)$, для которых можно обосновать нижний порог сложности линейного криптоанализа. Например, наличие в цепочке хотя-бы двух *PD-sbox* с максимальным смещением $bias(\alpha, \beta) = 8{,}052E\text{-}12$ (при $M = 8$ бит, $K = 16$ и $S = K \cdot M = 128$ бит), получаемым в среднем при **случайной** генерации фиксированных подстановок, требует набора более $2^{(73+73)}$ или 2^{146} пар «открытый текст – шифротекст». Это существенно превышает количество комбинаций для криптографического ключа длиной 128 бит и делает линейный криптоанализ неэффективным (при данной длине ключа).

Увеличением параметра K (количества фиксированных подстановок в составе *PD-sbox*) можно обеспечить устойчивость к линейному криптоанализу всего криптоалгоритма за счёт линейных свойств только **отдельной** псевдо-динамической подстановки *PD-sbox,* без необходимости поиска наилучшего варианта цепочки линейных аппроксимаций.

Проведённые предварительные исследования показали, что имеется потенциальная возможность **точного расчёта** смещения $bias(\alpha, \beta)$ для полноразмерных *PD-sbox* на основе линейных свойств отдельных фиксированных подстановок, что позволит синтезировать *PD-sbox* с **гарантированным** нижним порогом сложности линейного криптоанализа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Preneel B., Biryukov A. De C.* Canniere et al. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. – Berlin Heidelberg NewYork London Paris Tokyo Hong Kong Barcelona Budapest: Springer-Verlag, 2004.
2. *Matsui Mitsuru*. Linear Cryptoanalysis Method for DES Cipher // Advances in Cryptology – EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. – 1993. – P. 386-397. – URL: http://dx.doi.org/10.1007/3-540-48285-7_33.
3. *Biham Eli, Shamir Adi.* Differential Cryptanalysis of DES-like Cryptosystems // J. Cryptology. – 1991. – Vol. 4, No. 1. – P. 3-72. – URL: http://dx.doi.org/10.1007/BF00630563.
4. *Долгов В.И., Кузнецов А.А., Исаев С.А.* Дифференциальные свойства блочных симметричных шифров // Электронное моделирование. – 2011. – Т. 33, № 6. – С. 81-99.
5. *Горбенко И.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В*. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 312-320.
6. *Kazymyrov O., Oliynykov R.* Application of vectorial Boolean functions for substitutions generation used in symmetric cryptographic transformation // In Systems of information processing. – 2012. – Vol. 6, No. 104. – P. 97-102.
7. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: Московский центр непрерывного математического образования, 2004. – 470 с.

8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов ИПК, 1996. – 28 с. – URL: http://protect.gost.ru/document.aspx?control=7&id=139177.
9. Standards Federal Information Processing. Advanced Encryption Standard (AES). – Publication 197, November 26, 2001.
10. *Ivanov Georgi, Nikolov Nikolay, Nikova Svetla*. Reversed Genetic Algorithms for Generation of Bijective S-boxes with Good Cryptographic Properties // IACR Cryptology ePrint Archive. – 2014. – Vol. 2014. – P. 801. – URL: http://eprint.iacr.org/2014/801.
11. *Beelen Peter, Leander Gregor.* A new construction of highly nonlinear S-boxes // Cryptography and Communications. – 2012. – Vol. 4, No. 1. – P. 65-77. – URL: http://dx.doi.org/10.1007/s12095-011-0052-4.
12. *Kazymyrov Oleksandr, Kazymyrova Valentyna, Oliynykov Roman.* A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent // IACR Cryptology ePrint Archive. – 2013. – Vol. 2013. – P. 578. – URL: http://eprint.iacr.org/2013/578.
13. *Tokareva N.N.* Generalizations of bent functions. A survey // Diskretn. Anal. Issled. Oper. – 2010. – Vol. 17, No. 1. – P. 34-64.
14. *Ahmad Musheer, Khan Parvez Mahmood, Ansari Mohd. Zeeshan*. A Simple and Efficient Key-Dependent S-Box Design Using Fisher-Yates Shuffle Technique // Recent Trends in Computer Networks and Distributed Systems Security – Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings. – 2014. – P. 540-550. – URL: http://dx.doi.org/10.1007/978-3-642-54525-2_48.
15. *Pradeep L.N., Bhattacharjya Aniruddha.* Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks // Security in Computing and Communications – International Symposium, SSCC 2013, Mysore, India, August 22-24, 2013. Proceedings. – 2013. – P. 63-69. – URL: http://dx.doi.org/10.1007/978-3-642-40576-1_7.
16. *Hosseinkhani Razi, Haj H., Javadi Seyyed et al*. Using Cipher Key to Generate Dynamic S-Box in AES Cipher System. – 2012.
17. *Schneier Bruce*. Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish) // Fast Software Encryption, Cambridge Security Workshop. – London, UK, UK: Springer-Verlag, 1994. – P. 191-204. – URL: http://dl.acm.org/citation.cfm?id=647930.740558.
18. *Кузнецов А.А., Сергиенко Р.В., Науско А.А*. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 241-249.
19. *Bogdanov A., Knudsen L.R., Leander G. et al.* PRESENT: An Ultra-Lightweight Block Cipher // Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems. – CHES '07. – Berlin, Heidelberg: Springer-Verlag, 2007. – P. 450-466. – URL: http://dx.doi.org/10.1007/978-3-540-74735-2_31.
20. *Borghoff Julia, LarsR. Knudsen, Leander Gregor, Søren S. Thomsen.* Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes // FSE / Ed. by Antoine Joux. – Vol. 6733 of Lecture Notes in Computer Science. – Springer, 2011. – P. 270-289.
21. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. – New York: John Wiley and Sons, 1996.
22. *Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson et al.*On the Security of RC4 in TLS // Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. – 2013. – P. 305-320. – URL: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/alFardan.
23. *Lv Jing, Zhang Bin, Lin Dongdai*. Distinguishing Attacks on RC4 and A New Improvement of the Cipher // IACR Cryptology ePrint Archive. – 2013. – Vol. 2013. – P. 176. – URL: http://eprint.iacr.org/2013/176.
24. Security Advisory 2868725: Recommendation to disable RC4. Security Research and Defense Blog. – URL: http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx.
25. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Псевдо-динамические таблицы подстановки: основа современных симметричных криптоалгоритмов // Научное обозрение. – 2014. – № 12. – С. 162-166.

26. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Псевдо-динамические таблицы подстановки: исследование дифференциальных характеристик // Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках: сборник материалов международного научного е-симпозиума. Россия, г. Москва, 27-28 декабря 2014 г. – Киров: МЦНИП, 2015. – С. 77-89. – URL: http://dx.doi.org/10.13140/2.1.2609.8723.
27. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Исследование линейных характеристик псевдодинамических подстановок // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 111-123.

REFERENCES

1. *Preneel B., Biryukov A., De C. Canniere et al.* Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. Berlin Heidelberg NewYork London Paris Tokyo Hong Kong Barcelona Budapest: Springer-Verlag, 2004.
2. *Matsui Mitsuru*. Linear Cryptoanalysis Method for DES Cipher, *Advances in Cryptology – EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, 1993, pp. 386-397. Available at: http://dx.doi.org/10.1007/3-540-48285-7_33.
3. *Biham Eli, Shamir Adi*. Differential Cryptanalysis of DES-like Cryptosystems, *J. Cryptology*, 1991, Vol. 4, No. 1, pp. 3-72. Available at: http://dx.doi.org/10.1007/BF00630563.
4. *Dolgov V.I., Kuznetsov A.A., Isaev S.A.* Differentsial'nye svoystva blochnykh simmetrichnykh shifrov [Differential properties of symmetric block ciphers], *Elektronnoe modelirovanie* [Electronic Modeling], 2011, Vol. 33, No. 6, pp. 81-99.
5. *Gorbenko I.D., Dolgov V.I., Lisitskaya I.V., Oleynikov R.V.* Novaya ideologiya otsenki stoykosti blochnykh simmetrichnykh shifrov k atakam differentsial'nogo i lineynogo kriptoanaliza [A new ideology of assessing resistance block symmetric ciphers to attacks of differential and linear cryptanalysis], *Prikladnaya radioelektronika* [Applied Radio Electronics], 2010, Vol. 9, No. 3, pp. 312-320.
6. *Kazymyrov O., Oliynykov R.* Application of vectorial Boolean functions for substitutions generation used in symmetric cryptographic transformation, *In Systems of information processing*, 2012, Vol. 6, No. 104, pp. 97-102.
7. *Logachev O.A., Sal'nikov A.A., Yashchenko V.V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean functions in coding theory and cryptology]. Moscow: Moskovskiy tsentr nepreryvnogo matematicheskogo obrazovaniya, 2004, 470 p.
8. GOST 28147-89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya [State Standard 28147-89. System of information processing. Cryptographic protection. Cryptographic transformation algorithm]. Moscow: Izd-vo standartov IPK, 1996, 28 p. Available at: http://protect.gost.ru/ document.aspx?control=7&id=139177.
9. Standards Federal Information Processing. Advanced Encryption Standard (AES). Publication 197, November 26, 2001.
10. *Ivanov Georgi, Nikolov Nikolay, Nikova Svetla*. Reversed Genetic Algorithms for Generation of Bijective S-boxes with Good Cryptographic Properties, *IACR Cryptology ePrint Archive*, 2014, Vol. 2014, pp. 801. Available at: http://eprint.iacr.org/2014/801.
11. *Beelen Peter, Leander Gregor.* A new construction of highly nonlinear S-boxes, *Cryptography and Communications*, 2012, Vol. 4, No. 1, pp. 65-77. Available at: http://dx.doi.org/10.1007/s12095-011-0052-4.
12. *Kazymyrov Oleksandr, Kazymyrova Valentyna, Oliynykov Roman.* A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent, *IACR Cryptology ePrint Archive*, 2013, Vol. 2013, pp. 578. Available at: http://eprint.iacr.org/2013/578.
13. *Tokareva N.N.* Generalizations of bent functions. A survey, *Diskretn. Anal. Issled. Oper.*, 2010, Vol. 17, No. 1, pp. 34-64.
14. *Ahmad Musheer, Khan Parvez Mahmood, Ansari Mohd. Zeeshan*. A Simple and Efficient Key-Dependent S-Box Design Using Fisher-Yates Shuffle Technique, *Recent Trends in Computer Networks and Distributed Systems Security – Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings*, 2014, pp. 540-550. Available at: http://dx.doi.org/10.1007/978-3-642-54525-2_48.

15. *Pradeep L.N., Bhattacharjya Aniruddha.* Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks, *Security in Computing and Communications – International Symposium, SSCC 2013, Mysore, India, August 22-24, 2013. Proceedings*, 2013, pp. 63-69. Available at: http://dx.doi.org/10.1007/978-3-642-40576-1_7.
16. *Hosseinkhani Razi, Haj H., Javadi Seyyed et al*. Using Cipher Key to Generate Dynamic S-Box in AES Cipher System. 2012.
17. *Schneier Bruce*. Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish), *Fast Software Encryption, Cambridge Security Workshop*. London, UK, UK: Springer-Verlag, 1994, pp. 191-204. Available at: http://dl.acm.org/citation.cfm?id=647930.740558.
18. *Kuznetsov A.A., Sergienko R.V., Nausko A.A.* Simmetrichnyy kriptograficheskiy algoritm ADE (Algorithm of Dynamic Encryption) [Symmetric cryptographic algorithm ADE (Algorithm of Dynamic Encryption)], *Prikladnaya radioelektronika* [Applied Radio Electronics], 2007, Vol. 6, No. 2, pp. 241-249.
19. *Bogdanov A., Knudsen L.R., Leander G. et al.* PRESENT: An Ultra-Lightweight Block Cipher, *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems. CHES '07*. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 450-466. Available at: http://dx.doi.org/10.1007/978-3-540-74735-2_31.
20. *Borghoff Julia, LarsR. Knudsen, Leander Gregor, Søren S. Thomsen.* Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes, *FSE*, Ed. by Antoine Joux, Vol. 6733 of Lecture Notes in Computer Science. Springer, 2011, pp. 270-289.
21. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. New York: John Wiley and Sons, 1996.
22. *Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson et al*.On the Security of RC4 in TLS, *Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013*, pp. 305-320. Available at: https://www.usenix.org/conference/usenixsecurity13 /technical-sessions/paper/alFardan.
23. *Lv Jing, Zhang Bin, Lin Dongdai*. Distinguishing Attacks on RC4 and A New Improvement of the Cipher, *IACR Cryptology ePrint Archive*, 2013, Vol. 2013, pp. 176. Available at: http://eprint.iacr.org/2013/176.
24. Security Advisory 2868725: Recommendation to disable RC4. Security Research and Defense Blog. Available at: http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx.
25. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A*. Psevdo-dinamicheskie tablitsy podstanovki: osnova sovremennykh simmetrichnykh kriptoalgoritmov [Pseudo-dynamic lookup table: the Foundation of modern symmetric cryptographic algorithms], *Nauchnoe obozrenie* [Scientific Review], 2014, No. 12, pp. 162-166.
26. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Psevdo-dinamicheskie tablitsy podstanovki: issledovanie differentsial'nykh kharakteristik [Pseudo-dynamic lookup table: a study of differential characteristics], *Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma. Rossiya, g. Moskva, 27-28 dekabrya 2014 g.* [Physico-mathematical methods and informational technologies in science, technology and the Humanities: proceedings of the international scientific e-Symposium. Russia, Moscow, 27-28 December 2014]. Kirov: MTsNIP, 2015, pp. 77-89. Available at: http://dx.doi.org/10.13140/2.1.2609.8723.
27. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A*. Issledovanie lineynykh kharakteristik psevdodinamicheskikh podstanovok [Research of linear characteristics of pseudo-dynamic substitutions], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 111-123.

Статью рекомендовал к опубликованию д.т.н., профессор О.И. Шелухин.

Поликарпов Сергей Витальевич – Южный федеральный университет; e-mail: polikarpovsv@gmail.com; 347922, г. Таганрог, ул. Чехова, 2; тел.: +78634371902; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; доцент.

Кожевников Алексеевич – e-mail: leha.kozhevnikov@gmail.com; кафедра информационной безопасности телекоммуникационных систем; ассистент.

Polikarpov Sergey Vitalievich – Southern Federal University; e-mail: polikarpovsv@gmail.com; 2, Chekhova street, Taganrog, 347922, Russia; phone: +78634371902; the department of Information security of telecommunication; cand. of eng. sc.; associate professor.

Kozhevnikov Aleksey Alekseevich – e-mail: leha.kozhevnikov@gmail.com; the department of Information security of telecommunication; assistant lecturer.

УДК 621.39

В.В. Котенко, С.В. Котенко

ИДЕНТИФИКАЦИОННЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ИДЕНТИФИКАТОРОВ*

На фоне значительных достижений в части идентификации пользователей в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация информационных процессов. Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях влияния идентификационных признаков на качество защиты информации. Цель исследования состоит в разработке и обосновании принципов идентификационного анализа криптографических алгоритмов. Фундаментальную основу предлагаемого подхода к идентификационному анализу составляют авторские методы теории виртуализации: метод формирования виртуальных информационных образов, метод моделирования оценок виртуальных информационных образов, методы виртуализации информационных процессов, методы виртуализации идентификаторов. Решения задачи идентификационного анализа криптографических алгоритмов включает два этапа: 1) идентификационный анализ с позиций виртуализации информационных идентификаторов ансамблей процесса шифрования; 2) идентификационный анализ с позиций информационных оценок эффективности шифрования. Полученные результаты открывают принципиально новую область исследований в направлении расширения возможностей управления защитой информации на основе интеллектуального анализа данных и поддержки принятия решения при ситуационном управлении в условиях угроз информационных вторжений с адаптацией к возможному изменению широкого спектра идентификаторов источников угроз.

Защита информации; идентификация; аутентификации; шифрование; виртуализация; оптимизация; информационный поток; информационная безопасность.

V.V. Kotenko, S.V. Kotenko

ANALYSIS OF CRYPTOGRAPHIC IDENTIFICATION ALGORITHMS WITH POSITIONS VIRTUALISATION IDENTIFIERS

Against the backdrop of significant advances in the identification of the user in tasks of processing, protection and transmission of information almost overlook the identification of information processes. The criticality of the situation is revealed in the recent patterns of influence on the quality of the identification features of data protection. The purpose of the study is to develop an identification and justification of the principles of the analysis of cryptographic algorithms. The fundamental basis for the proposed approach to the identification methods of analysis constitute the author's theory of virtualization: virtual information method of forming images, a method of modeling assessments virtual information, the method of information processes virtualization, virtualization techniques identifiers. Solving the problem identification analysis of cryptographic algorithms involves two stages: 1) identification analysis from the point of virtualization information encryption process identifiers ensembles; 2) identification information analysis from the standpoint of effectiveness evaluations encryption. These results open up an entirely new field of

* Работа выполнена на основе гос. задания Минобрнауки РФ № 213.01-11/2014-9.