15. *C. De Canni`ere & B. Preneel*. TRIVIUM Specifications. eSTREAM, ECRYPT Stream Cipher Project [электронный ресурс]. Available at: http://www.ec rypt.eu.org/stream/p3ciphers/ trivium/trivium_p3.pdf (Accessed: 14 February 2014).
16. *Yun Tian, Gongliang Chen, Jianhua Li.* Quavium - A New Stream Cipher Inspired by Trivium, *JCP journal of computers*, 2012, Vol. 7, No. 5, pp. 1278-1283.
17. *Varfolomeev A.A., Zhukov A.E., Pudovkina M.A.* Potochnye kriptosistemy. Osnovnye svoystva i metody analiza stoykosti. Uchebnoe posobie [Stream cryptosystem. Basic properties and methods of strength analysis. Tutorial]. Moscow: PAIMS, 2000, 272 p.
18. Shifrovanie dannykh v Perl programmakh (crypt perl howto). Available at: http://www.opennet.ru/base/dev/perl_crypt.txt.html.
19. *Babilo P.N.* Osnovy yazyka VHDL [The basics of the language VHDL]. 2 nd ed. Moscow: Solon–R, 2002, 218 p.
20. *Sergienko A.M.* VHDL dlya proektirovaniya vychislitel'nykh ustroystv [VHDL for the design of computing devices]. Izd-vo: TID DS, 2003, 208 p.
21. VHDL: A logic synthesis approach Hardcover: D. Naylor, S. Jones. Cambridge University Press, July 31, 199, 324 p.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Голотин Денис Владимирович – e-mail: ww.golotin@mail.ru; тел.: +79514944226; кафедра безопасности информационных технологий; студент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@tsure.ru; Block “I”, 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of information technologies security; professor.

Golotin Denis Vladimirovich – e-mail: ww.golotin@mail.ru; phone: +79514944226; the department of information technologies security; student.

УДК 004.853

С.В. Поликарпов, К.Е. Румянцев, А.А. Кожевников

ИССЛЕДОВАНИЕ ЛИНЕЙНЫХ ХАРАКТЕРИСТИК ПСЕВДОДИНАМИЧЕСКИХ ПОДСТАНОВОК*

Одним из эффективных путей нейтрализации целого пласта методов криптоанализа блочных криптоалгоритмов является применение динамически изменяющихся подстановок. Подход на основе псевдодинамических 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 псевдодинамических подстановок требуется детальное исследование их криптографических свойств. Цель исследования – разработать методику определения линейных характеристик псевдодинамических подстановок для дальнейшего подтверждения их целевого применения в блочных криптоалгоритмах. В работе получены выражения для определения линейных свойств псевдодинамических подстановок PD-sbox для двух случаев: 1) когда значения состояния S фиксированы и задаются криптографическим ключом; 2) когда значения состояния S динамически изменяются под воздействием энтропии входной информации и результатов предшествующих преобразований. Первичный анализ выражения позволил сделать вывод, что сама структура псевдодинамической подстановки PD-sbox*

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

значительно затрудняет определение её линейных характеристик и, тем самым, препятствует осуществлению линейного криптоанализа. Предложенная методика определения линейных характеристик позволяет оценить линейные свойства всего ансамбля порождаемых при помощи PD-sbox подстановок. Это выгодно отличает данную работу от большинства работ по применению ключезависимых и динамических подстановок в криптографических криптоалгоритмах.

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

S.V. Polikarpov, K.E. Rumyantsev, A.A. Kozhevnikov

RESEARCH OF LINEAR CHARACTERISTICS OF PSEUDO-DYNAMIC SUBSTITUTIONS

One of effective ways of neutralization of the whole layer of methods of cryptanalysis of block cryptoalgorithms is application of dynamically changing substitutions. Approach on the basis of pseudo-dynamic substitutions (PD-sbox) allows to combine strengths of the fixed substitutions (high speed of work and efficiency of use of computing resources) and dynamic substitutions (neutralization of statistical methods of cryptanalysis). The purpose of research – to develop a technique of determination of linear properties of pseudo-dynamic substitutions for further confirmation of their target application in block cryptoalgorithms. In the work expressions for determination of linear properties of pseudo-dynamic substitutions (PD-sbox) for two cases are obtained: 1) when values of a condition of S are fixed and are set by a cryptographic key; 2) when values of a condition of S dynamically change under the influence of entropy of entrance information and results of the previous transformations. Primary analysis of expression allowed to draw conclusions, fair for a case of the fixed values of a condition of S: 1) at real application of PD-sbox with parameters of bits and complexity of a problem of obtaining a full matrix of values can exceed complexity of full search of keys of cryptoalgorithm; 2) the complexity of a set of the demanded statistics for determination of values of a condition of S at linear cryptanalysis as the quantity of the entrance combinations given on PD-sbox input is limited to dimension of an input of X and makes against possible conditions of S; 3) partial or complete masking of a contribution of input values X in values matrixes at its calculation. The offered method of calculation of linear properties allows to estimate linear properties of all ensemble of the generated substitutions. This favourably distinguishes this work from most of work on the application of key-depended substitutions and dynamic substitutions in cryptographic algorithms.

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

Введение. В качестве инструмента оценки стойкости современных вычислительно стойких блочных криптоалгоритмов широко применяются методы линейного и дифференциального криптоанализов, а также их производные [13]. При рассмотрении линейного и дифференциального криптоанализов можно отметить, что эти методы используют статистические свойства криптографических операций и наиболее эффективны при **фиксированных** подстановках и раундовых ключах [2, 3]. В существующих блочных криптоалгоритмах основным способом нейтрализации указанных атак является применение значительного количества раундов шифрования (обычно более 8), более эффективных операций перемешивания и подбор подстановок с максимальными характеристиками: максимальной нелинейностью, минимальными автокорреляционными характеристиками и другие [4–7].

Несмотря на существование двух, проверенных временем 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, так как они должны одновременно удовлетворять целому ряду криптографических свойств [1, 10–12]. Типичным является случай, когда синтезированная подстановка по одним характеристикам имеет высокие показатели, но по другим – низкие [6, 10].

Проблема усугубляется тем, что фиксированных подстановок, обладающих идеальными линейными и дифференциальными характеристиками, не может быть даже теоретически [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 основными проблемами построения блочных шифров:

1) обеспечение однозначности и обратимости криптографических преобразований для законных пользователей;

2) обоснование криптографических свойств предлагаемых решений;

3) обеспечение 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], но это не дало им значительных преимуществ перед 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 псевдодинамической подстановки (*Pseudo-Dynamical Sbox* или *PD-sbox*) [25, 26]. Предлагаемый подход позволяет совместить сильные стороны фиксированных подстановок (высокая скорость работы и эффективность использования вычислительных ресурсов) и динамических подстановок (нейтрализация статистических методов криптоанализа).

Цель исследования – разработать методику определения линейных характеристик псевдодинамических подстановок для дальнейшего подтверждения их целевого применения в качестве замены обычных фиксированных подстановок в блочных криптоалгоритмах (для снижения угрозы линейного криптоанализа).

2. Псевдодинамические подстановки. Структура псевдодинамической подстановки (рис. 1) основана на базе обычных фиксированных подстановок (узлов замены) *sbox*. 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*.

Предполагается, что значения состояния *S* не обязательно являются фиксированными и могут динамически изменяться в процессе шифрования, а вероятностные свойства соответствуют равномерному закону распределения.

Общий вид выражения, описывающего структуру псевдодинамической подстановки *PD-sbox,* имеет вид

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

где *sbox* – фиксированные подстановки; *K* – количество фиксированных подстановок; *X* – входные биты; *Y* – выходные биты; *S* – биты состояния псевдодинамической подстановки; $\bigoplus$ – операция сложения по модулю 2.

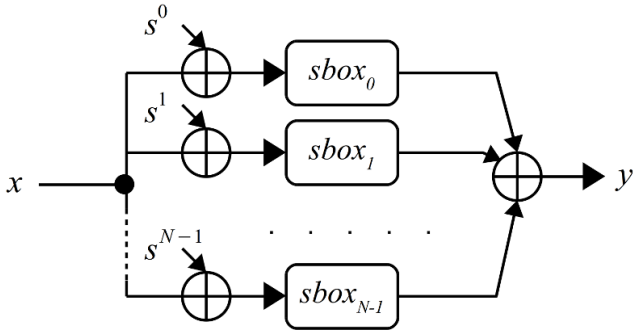

Рис. 1. Структура псевдодинамической подстановки

Для применения в криптографических алгоритмах необходимо определить следующие основные свойства формируемых эквивалентных (порождаемых) подстановок в зависимости от вида и количества фиксированных подстановок:

- линейные свойства;
- дифференциальные свойства;
- дистанция (степень различия или корреляция) между эквивалентными подстановками;
- алгебраические свойства и другие.

При этом необходимо дополнительно исследовать вопросы выбора количества и значений фиксированных подстановок.

3. Линейный криптоанализ. Основная цель линейного криптоанализа – снизить сложность (нелинейность) криптоалгоритма путём замены (аппроксимации) нелинейных подстановок наиболее вероятным набором линейных функций [2, 5].

Линейные характеристики функции, заданной в виде подстановки, показывают, насколько функция отличается от набора линейных функций (аффинных преобразований) [7]. В качестве метрики используют расстояние Хэмминга – ко-

личество отличающихся бит в двух строках одинаковой длины, где строками выступают значения таблиц истинности сравниваемых булевых функций. Наличие сильного соответствия между подстановкой и любой из линейных функций позволяет криптоаналитику с высокой вероятностью заменить подстановку на статистический аналог в виде линейной функции и тем самым значительно снизить сложность криптоанализа. Если подстановка и линейная функция отличаются в половине случаев, то замена статистическим аналогом неэффективна в случае равновероятности входных значений X.

В соответствии с определением [2], линейные характеристики определяются количеством совпадений подстановки с набором линейных (аффинных) функций:

$$\mathrm{NSbox}(\alpha,\beta) \stackrel{\mathrm{def}}{=} \{X|0 \le X < 2^M, (\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha[i])) = (\bigoplus_{j=0}^{N-1}(\mathrm{Sbox}(X)[j]\cdot\beta[j]))\}, \quad (2)$$

где $Sbox()$ – выходное значение подстановки; $[j]$ – конкретный бит выходного значения подстановки; x – входные значения подстановки; $[i]$ – конкретный бит входного значения подстановки; 2^M – количество входных комбинаций; M – количество входных бит; N – количество выходных бит; α – битовая маска для входного значения; β – битовая маска для выходного значения; $\cdot$ – операция побитового логического умножения. Фактически α и β задают вариант линейной функции.

Вероятность аппроксимации линейной функцией заданной подстановки определяется выражением

$$\mathrm{p}(\alpha,\beta) = \frac{\mathrm{NSbox}(\alpha,\beta)}{2^M}. \quad (3)$$

Эффективность аппроксимации часто представляют в виде смещения

$$\mathrm{bias}(\alpha,\beta) = \left|\mathrm{p}(\alpha,\beta) - \frac{1}{2}\right|, \quad (4)$$

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

С точки зрения криптографической стойкости идеальным случаем будет $bias(\alpha, \beta) = 0$ при всех значениях α и β, кроме $\alpha = 0$ и $\beta = 0$. Однако фиксированных подстановок с такими идеальными свойствами не существует [7]. Наихудшим вариантом является $bias(\alpha, \beta) = 0,5$ – что означает полное совпадение аппроксимируемой подстановки с линейной функцией или её инверсией.

4. Методика определения линейных характеристик для псевдодинамической подстановки. Методика определения линейных характеристик для фиксированных подстановок, приведённая в [2], требует модификации в случае анализа псевдодинамических подстановок. Действительно, при анализе линейных характеристик фиксированных подстановок подразумевается наличие типовой конструкции в блочном криптоалгоритме, показанной на рис. 2.

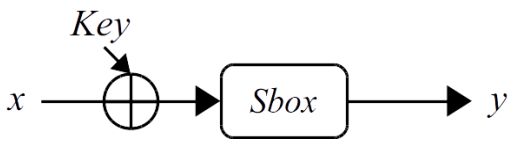

Рис. 2. Типовое включение фиксированной подстановки в блочном криптоалгоритме

Данная конструкция описывается выражением

$$Y = Sbox(X \oplus Key). \quad (5)$$

Так как значение ключа *Key* фиксировано и смешивается с входным значением *X* при помощи сложения по модулю 2 (XOR), то достаточно в соответствии с выражением (2) определить линейные свойства непосредственно фиксированной подстановки (без учёта вклада значения ключа *Key*):

$$Y = Sbox(X). \quad (6)$$

Последнее выражение пытаются аппроксимировать линейной функцией вида

$$\bigoplus_{j=0}^{N-1} (Y[j] \cdot \beta[j]) = \bigoplus_{i=0}^{M-1} (X[i] \cdot \alpha[i]), \quad (7)$$

где значения битовых масок α и β задают конкретный вариант линейной функции.

Таким образом, алгоритм определения линейных свойств для выражения (5) выглядит следующим образом:

1. Задаются значения параметров α и β.

2. Последовательно перебираются все варианты значений *X* и по выражению (6) определяются соответствующие значения выходов *Y*.

3. Полученные значения *X* и *Y* подставляются в выражение (7) и, в случае верности данного равенства, значение $NSbox(\alpha, \beta)$ увеличивается на единицу.

4. После завершения пунктов 1–3 для всех значений α и β формируется результирующая матрица значений $NSbox(\alpha, \beta)$.

5. Вычисляется вероятность аппроксимации линейной функцией $p(\alpha, \beta)$ и смещение $bias(\alpha, \beta)$.

В матрице значений $bias(\alpha, \beta)$ осуществляется поиск наибольших значений, соответствующих линейным функциям, максимально приближающихся к аппроксимируемой функции.

Значение ключа *Key* можно ввести в аппроксимирующее выражение уже после расчёта линейных свойств, что позволяет значительно снизить количество вычислений при определении матрицы значений $NSbox(\alpha, \beta)$. Ввод значения ключа *Key* осуществляется в соответствии со следующей заменой

$$Y = Sbox(X \oplus Key) \Rightarrow \bigoplus_{j=0}^{N-1} (Y[j] \cdot \beta[j]) = \bigoplus_{i=0}^{M-1} ((X[i] \oplus Key) \cdot \alpha[i]).$$

После этого значения битов ключа *Key* можно определить (с определённой вероятностью) при помощи выражения

$$\bigoplus_{i=0}^{M-1} (Key \cdot \alpha[i]) = \left(\bigoplus_{i=0}^{M-1} (X[i] \cdot \alpha[i])\right) \oplus \left(\bigoplus_{j=0}^{N-1} (Y[j] \cdot \beta[j])\right). \quad (8)$$

Для случая с псевдодинамической подстановкой *PD-sbox* необходимо дополнительно учитывать значение состояния *S*, задающее порождаемую подстановку и имеющее значительно большую размерность, чем у *X* и *Y*. Для криптографических операций, с точки зрения стойкости, важны любые особенности преобразований, так как они могут приводить к значительному снижению стойкости криптоалгоритмов в целом. Поэтому, для всестороннего изучения линейных свойств псевдодинамической подстановки необходимо рассмотреть два случая:

1. Значения состояния *S* фиксированы и задаются криптографическим ключом. Для этого случая псевдодинамическая подстановка *PD-sbox* представляется в виде большой эквивалентной фиксированной подстановки, с размерностью входа, соответствующей размерности состояния *S*.

2. Значения состояния *S* динамически изменяются под воздействием энтропии входной информации и результатов предшествующих преобразований. Для этого случая псевдодинамическая подстановка *PD-sbox* представляется в виде динамически изменяемой подстановки с размерностями входа и выхода, соответствующих размерностям *X* и *Y*, где конкретная подстановка задаётся значением состояния *S*.

4.1. Представление PD-sbox в виде большой эквивалентной фиксированной подстановки. Данный случай предполагает, что значения состояния *S* фиксированы и задаются криптографическим ключом.

Рассмотрим вариант псевдодинамической подстановки, состоящей из 2-х фиксированных подстановок (рис. 3).

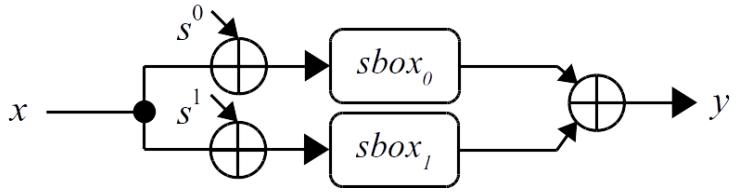

Рис. 3. Вариант PD-sbox, состоящей из двух фиксированных подстановок

В данном случае описание *PD-sbox* можно представить в виде большой эквивалентной подстановки, показанной на рис. 4. Данная подстановка имеет вход размерностью 2*M*, значения которого получаются конкатенацией отдельных входов $X \oplus S^0$ и $X \oplus S^1$ с размерностью *M* бит.

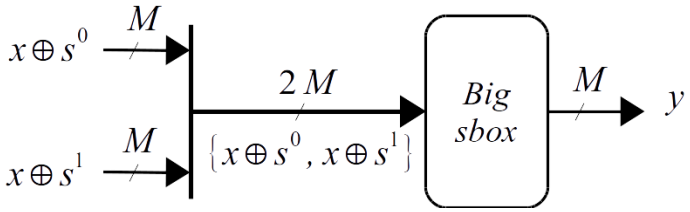

Рис. 4. Представление PD-sbox в виде большой эквивалентной подстановки

Перебирая все возможные водные комбинации $\{X \oplus S^0, X \oplus S^1\}$ и получая выходные значения *Y*, можно сформировать большую фиксированную эквивалентную подстановку, для которой применима ранее описанная методика определения линейных свойств. Однако для определения специфических свойств *PD-sbox* необходимо получить и проанализировать соответствующее аппроксимирующее выражение.

Выражение, описывающее выходное значение, будет иметь вид

$$Y = Sbox_0(X \oplus S^0) \oplus Sbox_1(X \oplus S^1). \quad (9)$$

При замене фиксированных подстановок *Sbox* линейными функциями получим выражение вида

$$\bigoplus_{j=0}^{N-1}(Y[j] \cdot \beta[j]) = \bigoplus_{i=0}^{M-1}((X[i] \oplus S^0[i]) \cdot \alpha^0[i]) \oplus \bigoplus_{i=0}^{M-1}((X[i] \oplus S^1[i]) \cdot \alpha^1[i]),$$

где *Y* – выходное значение; [*j*] – конкретный бит выходного значения подстановки; *X* – входное значение; S^0 и S^1 – значения состояния псевдодинамической подстановки; [*i*] – конкретный бит входного значения фиксированной подстановки; *M* – количество входных бит; *N* – количество выходных бит; α^0 и α^1 – битовые маски для входных значений фиксированных подстановок; β – битовая маска для выходного значения; • – операция побитового логического умножения, $\oplus$ – операция сложения по модулю 2.

После этого, значения битов состояния S^i можно определить (с определённой вероятностью) при помощи выражения

$$(\bigoplus_{i=0}^{M-1}(S^0[i]\cdot\alpha^0[i]))\oplus(\bigoplus_{i=0}^{M-1}(S^1[i]\cdot\alpha^1[i]))=$$
$$=(\bigoplus_{j=0}^{N-1}(Y[j]\cdot\beta[j]))\oplus(\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha^0[i]))\oplus(\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha^1[i])). \quad (10)$$

По сравнению с (8) в данном выражении больше переменных, что приводит к значительному увеличению размерности матрицы значений $NSbox(\alpha,\beta)$ и количества вычислений при её расчёте.

Таким образом, алгоритм определения линейных свойств для выражения (9) выглядит следующим образом:

1. Задаются значения параметров α^k и β.

2. Последовательно перебираются все варианты значений X и S^i и по выражению (9) определяются соответствующие значения выходов Y.

3. Полученные значения подставляются в выражение (10) и, в случае верности данного равенства, значение $NSbox(\alpha,\beta)$ увеличивается на единицу.

4. После завершения пунктов 1–3 для всех значений α и β формируется результирующая матрица значений $NSbox(\alpha,\beta)$.

5. Вычисляется вероятность аппроксимации линейной функцией $p(\alpha,\beta)$ и смещение $bias(\alpha,\beta)$, при этом в выражении (3) для $p(\alpha,\beta)$ учитывается количество вариантов значений S^i:

$$p(\alpha,\beta)=\frac{NSbox(\alpha,\beta)}{2^M\cdot\prod_{i=0}^{(K-1)}2^M}=\frac{NSbox(\alpha,\beta)}{2^{M(1+K)}}, \quad (11)$$

где i – номер фиксированной подстановки, перед которой добавляется значение состояния S^i; M – количество бит в значении состояния S^i; K – количество фиксированных подстановок в *PD-sbox*.

Итоговое выражение, описывающее набор линейных функций, аппроксимирующих псевдо-динамическую подстановку *PD-sbox* с произвольным количеством K фиксированных подстановок, будет выглядеть следующим образом:

$$\bigoplus_{k=0}^{K-1}\left(\bigoplus_{i=0}^{M-1}\left(S^k[i]\cdot\alpha^k[i]\right)\right)=\left(\bigoplus_{j=0}^{N-1}(Y[j]\cdot\beta[j])\right)\oplus\bigoplus_{k=0}^{K-1}\left(\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha^k[i])\right), \quad (12)$$

где S^k – значение состояния псевдо-динамической подстановки для k-й фиксированной подстановки; K – количество фиксированных подстановок в *PD-sbox*; Y – выходное значение; $[j]$ – конкретный бит выходного значения подстановки; X – входное значение; $[i]$ – конкретный бит входного значения фиксированной подстановки; M – количество входных бит; N – количество выходных бит; α^k – битовые маски для входных значений фиксированных подстановок; β – битовая маска для выходного значения; • – операция побитового логического умножения; $\oplus$ – операция сложения по модулю 2.

4.2. Представление PD-sbox в виде динамически изменяемой подстановки. Данный случай предполагает, что значения состояния S динамически изменяются под воздействием энтропии входной информации и результатов предшествующих преобразований криптоалгоритма, в состав которого включена *PD-sbox*. Для этого случая псевдодинамическая подстановка *PD-sbox* представляется в виде динамически изменяемой подстановки с размерностями входа и выхода соответствующих размерностям X и Y, где конкретная подстановка задаётся значением состояния S размерностью $M{\cdot}K$ бит или $J{=}2^{M.K}$ комбинаций (рис. 5).

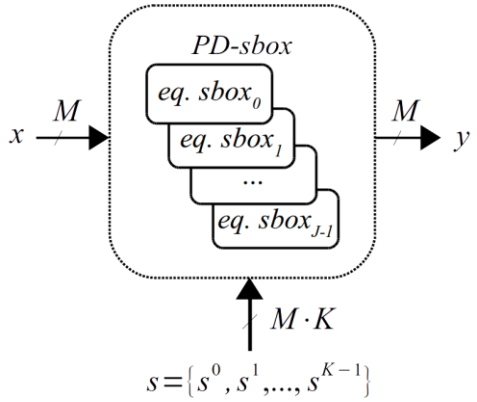

Рис. 5. Представление PD-sbox в виде динамически изменяемой подстановки

Так как по условию работы псевдодинамической подстановки *PD-sbox* предполагается равновероятность порождаемых подстановок (исходя из равновероятности значения параметра *S*), то необходимо усреднять значения для $NSbox(\alpha, \beta)$ по всему множеству порождаемых (эквивалентных) подстановок:

$$\overline{\mathrm{NSbox}}(\alpha,\beta) = \frac{\sum_{i=0}^{J-1} \mathrm{NSbox_i}(\alpha, \beta)}{J}, \quad , \tag{13}$$

где $J = 2^{M.K}$ – количество порождаемых подстановок; i – индекс порождаемой подстановки; $NSbox_i(\alpha, \beta)$ – матрица, содержащая количество совпадений с набором линейных функций для i-ой порождаемой подстановки; α – битовая маска для входного значения; β – битовая маска для выходного значения.

После вычисления $NSbox(\alpha, \beta)$ по формулам (3) и (4) определяются вероятность аппроксимации линейными функциями псевдодинамической подстановки $p(\alpha, \beta)$ и смещение $bias(\alpha, \beta)$.

Заключение. Получены выражения для определения линейных характеристик псевдодинамических подстановок *PD-sbox* для двух случаев:

1. Когда значения состояния *S* фиксированы и задаются криптографическим ключом – выражения (12) и (11).

2. Когда значения состояния *S* динамически изменяются под воздействием энтропии входной информации и результатов предшествующих преобразований – выражение (13).

Для полученных выражений предложена методика расчёта линейных характеристик псевдодинамических подстановок *PD-sbox*, позволяющая исследовать линейные свойства в зависимости от свойств и количества составляющих её фиксированных подстановок. Следует отметить, что предложенная методика позволяет фактически оценить линейные свойства всего *ансамбля* порождаемых *PD-sbox* подстановок. Это выгодно отличает данную работу от большинства работ по применению ключезависимых и динамических подстановок в криптоалгоритмах [14–16, 18].

Кроме того, первичный анализ выражения (12) позволил сделать важные выводы, справедливые для случая фиксированных значений состояния *S*, задаваемых криптографическим ключом:

1. Размерность полной матрицы значений $NSbox(\alpha, \beta)$ составляет $2^{M.K}$ строк и 2^M столбцов. В противовес этому, для обычных фиксированных биективных подстановок эта размерность составляет всего 2^M строк и 2^M столбцов. Учитывая, что для реальных криптоалгоритмов предполагаются значения $M \geq 8$ бит и $K \geq 16$, то сложность задачи получения полной матрицы значений $NSbox(\alpha, \beta)$ может превышать сложность полного перебора ключей криптоалгоритма.

2. Количество входных комбинаций, которые можно подать на вход *PD-sbox*, ограничено размерностью входа X и составляет 2^M против $2^{M.K}$ возможных состояний S. Поэтому у криптоаналитика возникает проблема набора требуемой статистики для определения значений состояния $S = \{S^0, S^1, S^2, \ldots, S^{K-1}\}$ по выражению (12). Появляющаяся неопределённость при определении значений состояния S значительно снижает эффективность линейного криптоанализа.

3. Частичное или полное маскирование вклада входных значений X в значения матрицы $NSbox(\alpha, \beta)$ при её расчёте по выражению (12). Например, при $K = 2$, $\alpha^0[i] = 1$ и $\alpha^1[i] = 1$ получаем $(X[i]\cdot\alpha^0[i]) \oplus (X[i]\cdot\alpha^1[i]) = 0$ на основе свойств операции сложения по модулю 2 (смотри правую часть выражения (10)). Данный эффект также снижает эффективность линейного криптоанализа и напрямую связан с предыдущим пунктом вывода.

Указанные особенности псевдодинамических подстановок *PD-sbox* потенциально могут значительно снизить эффективность линейного криптоанализа даже без учёта конкретных свойств входящих в её состав фиксированных подстановок.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Preneel B., Biryukov A., C. De 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. – ИПК Издательство стандартов, 1996. – С. 28. – 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. *Julia Borghoff, Lars R. Knudsen, Gregor Leander, 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.* Псевдодинамические 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.

REFERENCES

1. *Preneel B., Biryukov A., C. De 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 block symmetric 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 to assess the persistence of block symmetric ciphers to attacks, 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]. IPK Izdatel'stvo standartov, 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. *Julia Borghoff, Lars R. Knudsen, Gregor Leander, Søren S. Thomsen*. Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes, *FSE*, Under 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 basis 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: study the differential characteristics of], Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: Cbornik 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.

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.

Румянцев Константин Евгеньевич – e-mail: rke2004@mail.ru; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Кожевников Алексей 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.

Rumyantsev Konstantin Evgenievich – e-mail: rke2004@mail.ru; the department of information security of telecommunication; head of department; dr. of eng.. sc.; professor.

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