17. *Gorbunov P.A., Fokht I.A.* Problemy informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh – teoreticheskie resheniya i prakticheskie razrabotki. Programmnye sistemy: teoriya i prilozheniya [Information security problems in medical information systems - theoretical solutions and practical developments. Software systems: theory and applications], ed. by S.M. Abramova. In 2nd vol. Vol. 1. Moscow: Fizmatlit, 2006, pp. 107-112.
18. *Nazarenko G.I, Guliev Ya.I., Ermakov. D.E.* Meditsinskie informatsionnye sistemy: teoriya i praktika [Medical information systems: theory and practice], ed. by G.I. Nazarenko, G.S. Osipova. Moscow: Fizmatlit, 2005, 320 p.
19. *Mikheev V.A.* Osnovy postroeniya podsistemy zashchity informatsii mnogofunktsional'noy informatsionnoy sistemy [Fundamentals of building a subsystem of information security for a multifunctional information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 165-167.
20. *Klepikov E.A., Yas'ko A.O.* Voprosy zashchity konfidentsial'noy meditsinskoy informatsii o patsiente v meditsinskikh informatsionnykh sistemakh [Issues of protecting confidential medical information about a patient in medical information systems], *Simvol nauki* [Symbol of Science], 2016, No. 9-1. Available at: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

Статью рекомендовал к опубликованию д.э.н. Е.Н. Тищенко.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: +79054530191; д.т.н.; профессор.

Шумилин Александр Сергеевич – e-mail: ashumilin@sfedu.ru; тел.: +79081773495; м.н.с.

Алексеев Дмитрий Михайлович – e-mail: dalekseev@sfedu.ru; тел.: +79515069532; ассистент.

Babenko Lyudmila Klimentievna – Southern Federal University; e-mail: lkbabenko@sfedu.ru, 2, Chekhov street, Taganrog, 347922, Russia; phone: +79054530191; dr. of eng. sc.; professor.

Shumilin Alexander Sergeevich – e-mail: ashumilin@sfedu.ru; phone: +79081773495; junior researcher.

Alekseev Dmitry Mikhailovich – e-mail: dalekseev@sfedu.ru; phone: +79515069532; assistant.

УДК 004.056.55 DOI 10.18522/2311-3103-2020-5-16-30

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

ВЫЧИСЛИТЕЛЬНО ЭФФЕКТИВНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ УСРЕДНЁННЫХ ЛИНЕЙНЫХ СВОЙСТВ ПСЕВДО-ДИНАМИЧЕСКИХ ПОДСТАНОВОК

Псевдо-динамические подстановки PD-sbox могут стать эффективной заменой фиксированных подстановок в псевдо-случайных функциях, так как обладают положительными свойствами как фиксированных подстановок (малый расход вычислительных ресурсов), так и динамических подстановок (способных кардинально усложнять применение статистических методов криптоанализа). Проблемой активного внедрения псевдо-динамических подстановок является, в том числе, отсутствие вычислительно эффективного метода определения усреднённых линейных свойств для всего множества генерируемых при помощи PD-sbox эквивалентных подстановок, при этом в большинстве случаев интересует только определение максимальных значений преобладания (смещения) bias(α, β) от идеального значения 1/2. Для решения этой проблемы предлагается оригинальный метод, состоящий в том, что максимальные значения преобладания рассчитываются только для относительно небольших фиксированных подстановок, входящих в состав PD-sbox, а результирующие максимальные значения преобладания получаются путём итерационного вычисления с использованием логико-вероятностного выражения для операции Исключаю-

щего ИЛИ-НЕ (XNOR). Эффектом применения предложенного метода является кардинальное снижение вычислительных операций и, соответственно, возможность определения на типовом персональном компьютере максимальных значений преобладания bias(α, β) для 16-элементных PD-sbox, состоящих из 8-битовых фиксированных подстановок (что является недостижимым при использовании тривиального метода).

Псевдо-случайные функции; линейный криптоанализ; псевдо-динамические подстановки.

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

COMPUTATIONALLY EFFICIENT METHOD FOR DETERMINING THE AVERAGE LINEAR PROPERTIES OF PSEUDO-DYNAMIC SUBSTITUTIONS

Pseudo-dynamic substitutions PD-sbox can become an effective replacement for fixed substitutions in pseudo-random functions, since they have the positive properties of both fixed substitutions (low consumption of computational resources) and dynamic substitutions (which can radically complicate the application of statistical cryptanalysis methods). The problem of active implementation of pseudo-dynamic substitutions is, inter alia, the absence of a computationally efficient method for determining the averaged linear properties for the entire set of equivalent substitutions generated using PD-sbox, while in most cases, only the determination of the maximum values of the prevalence (bias) bias (α, β) from the ideal value 1/2. To solve this problem, an original method is proposed, which consists in the fact that the maximum dominance values are calculated only for relatively small fixed substitutions included in the PD-sbox, and the resulting maximum dominance values are obtained by iterative calculation using a logical-probabilistic expression for the Exclusive OR operation -NO (XNOR). The effect of using the proposed method is a dramatic reduction in computational operations and, accordingly, the possibility of determining on a typical personal computer the maximum values of the prevalence bias (α, β) for 16-element PD-sboxes consisting of 8-bit fixed substitutions (which is unattainable when using a trivial method).

Pseudo-random functions; linear cryptanalysis; pseudo-dynamic substitutions.

Введение. Одной из серьёзных проблем при создании симметричных криптографических алгоритмов является удовлетворение требований их устойчивости к статистическим методам криптоанализа, среди которых наиболее опасными и часто используемыми являются линейный и дифференциальный криптоанализ (и их производные) [1–8]. Если рассматривать линейный криптоанализ, то его целью является попытка упрощения сложности криптографического преобразования путём замены (аппроксимации) нелинейных элементов на линейные функции. В качестве нелинейных элементов, в большинстве случаев, выступают операции подстановки (замены), имеющие небольшую размерность (обычно 4 или 8 бит).

Как известно [9], реальные фиксированные подстановки не могут обладать идеальными свойствами и имеют ограниченный предел нелинейности (для своей размерности). По этой причине симметричные криптоалгоритмы имеют итерационную структуру, позволяющую «накопить» необходимую нелинейность за счёт количества итераций (раундов) преобразования и, тем самым, противодействовать статистическим методам криптоанализа.

Одним из известных и практически нереализованных путей противодействия статистическим методам криптоанализа является использование динамических подстановок. Однако, динамические подстановки не нашли широкого применения. Исключением является криптоалгоритм RC4, но и он переведён в разряд устаревших и ненадёжных [10]. Недостатками динамических подстановок являются: кардинальное увеличение затрачиваемых ресурсов и малое количество исследований по принципам обновления содержимого подстановок.

Возможным решением проблемы удовлетворения требованиям по одновременной минимизации затрачиваемых аппаратных ресурсов и минимизации задержки при преобразовании информации является применение псевдо-динамических подстановок *PD-sbox* [11–18].

Проведённые ранее исследования, на основе вычислительного эксперимента, показали [11, 14], что псевдо-динамические подстановки при работе в динамическом режиме (когда изменяются значения на управляющем входе) обладают идеальными усреднёнными линейными и дифференциальными свойствами (при усреднении свойств по всему множеству эквивалентных подстановок). Однако, при работе в статическом режиме (когда значение на управляющем входе фиксировано, но зависит от секретного параметра) псевдо-динамические подстановки, в общем случае, не обладают идеальными усреднёнными линейными и дифференциальными характеристиками.

Так, в [12, 13] осуществлено первичное исследование линейных характеристик псевдо-динамических подстановок *PD-sbox*. Предложена методика расчёта линейных свойств псевдо-динамических подстановок *PD-sbox*, позволяющая исследовать линейные свойства в зависимости от свойств и количества составляющих её фиксированных подстановок. Предложенная методика позволяет фактически оценить линейные свойства всего множества порождаемых при помощи *PD-sbox* подстановок. Это выгодно отличает данную работу от большинства работ, по применению зависимых от ключа и динамических подстановок.

В [13] приведены результаты, показывающие, что путём случайного формирования можно получить полноразмерные псевдо-динамические подстановки *PD-sbox*, обладающие экстремально низкими значениями смещения (преобладания) вероятности линейной аппроксимации $bias(\alpha,\beta)$. Стоит отметить, что в работе осуществлялась оценка *среднего* значения преобладания для большого количества *PD-sbox* и эта оценка производилась на основе *экстраполяции* результатов малоразмерных псевдо-динамических подстановок. Приведённый метод *не позволяет* осуществлять точное определение линейных свойств конкретных полноразмерных псевдо-динамических подстановок.

В противовес этому, для определения усреднённых дифференциальных характеристик был найден способ, позволяющий осуществлять исследование таких свойств на обычном персональном компьютере. Приведённый в [15] вычислительно-эффективный метод показывает, что существует *принципиальная* возможность определения усреднённых дифференциальных свойств для полноразмерных псевдо-динамических подстановок, используя только дифференциальные свойства маленьких фиксированных подстановок, входящих в состав *PD-sbox*. Кроме того, в [16] показано существование класса псевдо-динамических подстановок *PD-sbox*, которые в статическом режиме работы имеют идеальное усреднённое распределение дифференциалов.

Таким образом, существует актуальная проблема поиска вычислительно-эффективного метода определения линейных характеристик псевдо-динамических подстановок.

В данной работе предлагается вычислительно-эффективный метод определения линейных свойств (усреднённых по всему множеству эквивалентных подстановок) полноразмерных псевдо-динамических подстановок. Что позволяет закрыть пробел в наличии эффективных средств анализа линейных параметров и, соответственно, синтеза псевдо-динамических подстановок.

Существующие подходы. Метод линейной аппроксимации подстановок был предложен в [19]. В соответствии с определением, линейные свойства определяются количеством совпадений подстановки с набором линейных (аффинных) функций:

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

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; $\oplus$ – операция сложения по модулю 2. Фактически α и β задают вариант линейной функции.

Вероятность аппроксимации линейной функцией заданной подстановки определяется выражением:

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

Эффективность аппроксимации часто представляют в виде смещения (преобладания):

$$bias(\alpha,\beta) = \left|p(\alpha,\beta) - \frac{1}{2}\right|, \quad (3)$$

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 [9].

Таким образом, данный метод требует вычисления количества совпадений всех возможных комбинаций линейных функций с оцениваемой подстановкой. Размерность результирующей таблицы для $NSbox$ будет составлять 2^M строк и 2^N столбцов.

В [12] приведённый метод был расширен для исследования псевдо-динамических подстановок [11].

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 (рис. 1).

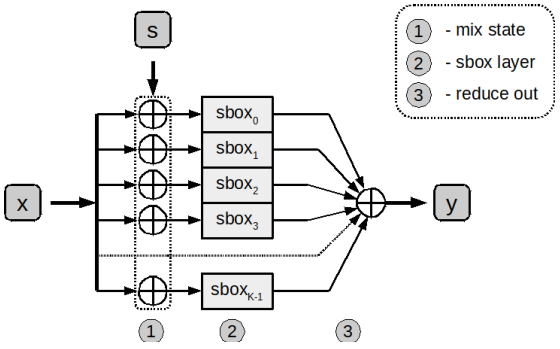

Рис. 1. Структура PD-sbox

Выражение, описывающее псевдо-динамическую подстановку:

$$Y = \bigoplus_{i=0}^{K-1} Sbox_i(X \oplus S^i), \quad (4)$$

где $Sbox$ – фиксированные подстановки; K – количество фиксированных подстановок; X – входные биты; Y – выходные биты; S – биты состояния псевдо-динамической подстановки; M – размерность фиксированных подстановок, входа x и выхода y.

Задавая конкретное значение состояния S – задаём одну эквивалентную подстановку. Всего будет 2^{MK} эквивалентных подстановок (M – размерность входа).

Как было указано [12–14], псевдо-динамические подстановки в динамическом режиме работы обладают идеальными усреднёнными линейными и дифференциальными свойствами (происходит взаимная компенсация значений $bias(\alpha,\beta)$ при усреднении по всему множеству формируемых эквивалентных подстановок).

Поэтому, интерес представляет исследование линейных свойств для статического режима работы псевдо-динамических подстановок *PD-sbox* –когда значения состояния S фиксированы и задаются криптографическим ключом.

Тривиальный метод. Для этого случая тривиальным методом оценки линейных свойств является представление *PD-sbox* в виде *большой* эквивалентной подстановки, заменяющая собой все параллельно включенные фиксированные подстановки из состава *PD-sbox*. Например, *большая* эквивалентная подстановка для *PD-sbox* из двух фиксированных подстановок получается перебором всех возможных входных комбинаций $\{X \oplus S^0, X \oplus S^1\}$ и вычислением соответствующих выходных значений Y (рис. 2.).

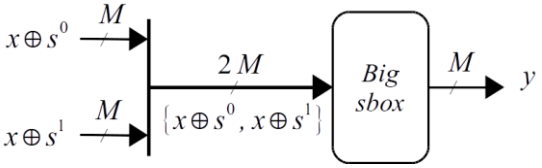

Рис 2. Представление PD-sbox в виде большой эквивалентной подстановки

После этого производится вычисление линейных свойств *большой* эквивалентной подстановки с использованием выражения из [19]. Недостаток метода – для полноразмерных *PD-sbox большая* эквивалентная подстановка будет иметь неприемлемую для вычислений размерность, так как размерность результирующей таблицы для $NSbox(\alpha,\beta)$ будет составлять 2^{MK} строк и 2^M столбцов. Например, 8-элементная *PD-sbox*, сформированная из 4-битных фиксированных подстановок, потребует вычисления таблицы для $NSbox(\alpha,\beta)$, состоящей из $2^{8\cdot4}$ или 2^{32} строк.

Метод на основе аналитического выражения. В работе [12] получены выражения для определения линейных свойств псевдо-динамических подстановок *PD-sbox* для случая, когда значения состояния S фиксированы и задаются криптографическим ключом:

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

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

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

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*.

Недостаток метода – аналогичен предыдущему случаю, определение таблицы $NSbox(\alpha,\beta)$ для полноразмерных *PD-sbox* будет иметь неприемлемую для вычислений размерность (размерность таблицы для $NSbox(\alpha,\beta)$ будет составлять 2^{MK} строк и 2^M столбцов).

Постановка задачи. Введём следующие обозначения:

K – количество фиксированных подстановок в составе *PD-sbox*;

M – размерность входа и выхода этих фиксированных подстановок;

N_{rows} – количество строк в таблице $P(\alpha,\beta)$;

$N_{columns}$ – количество столбцов в таблице $P(\alpha,\beta)$;

N_{count} – количество операций подсчёта совпадений *одной* линейной функции (задаваемой масками α и β) и исследуемой подстановки (на основе формулы (1)), соответствует количеству входных комбинаций.

Под вычислительной эффективностью будем понимать количество операций и объём памяти, затрачиваемых при определении (расчёте) линейных свойств подстановок.

Для тривиального метода (используя большую эквивалентную подстановку) получаем: $K \cdot M$ – размерность входа в битах; $N_{rows} = 2^{K \cdot M}$; $N_{columns} = 2^M$; $N_{count} = 2^{K \cdot M}$. Суммарное количество проходов в соответствии с формулой (1):

$$N_{bigSbox} = N_{rows} \cdot N_{columns} \cdot N_{count} = 2^{K \cdot M} \cdot 2^M \cdot 2^{K \cdot M} = 2^{M(2 \cdot K+1)}$$

Итогом вычислений будет таблица значений $NSbox(\alpha,\beta)$ размерностью $2^{K \cdot M} \times 2^M$ строк и столбцов. На основе этой таблицы рассчитываются таблицы $P(\alpha,\beta)$ и $bias(\alpha,\beta)$ с такой же размерностью. После чего по таблице $bias(\alpha,\beta)$ осуществляется поиск максимальных значений.

Например, для *PD-sbox* с $K = 8$ и $M = 4$ мы получим $N_{bigSbox} = 2^{4(2 \cdot 8+1)} = 2^{68}$ проходов в соответствии с формулой (1) и таблицу значений $NSbox(\alpha,\beta)$ размерностью $2^{32} \times 2^4$, что уже является непреодолимой задачей для типовых персональных компьютеров (не рассматривая последующие этапы расчёта).

Как показывает анализ публикаций по теме линейного криптоанализа [1, 8], в большинстве случаев для подстановок (и других нелинейных элементов) определяются только максимальные отклонения значений преобладания $bias(\alpha,\beta)$ от идеального значения $(1/2)$.

Таким образом, ставится задача поиска метода, позволяющего вычислять на типовых персональных компьютерах максимальные значения $bias(\alpha,\beta)$ для – элементных псевдо-динамических подстановок *PD-sbox* с $K \leq 16$ и $M \leq 8$.

Предлагаемый подход. Заключается в том, что оцениваются только максимальные значения преобладания $bias(\alpha,\beta)$ для каждого из вариантов битовой маски для выходного значения β (т. е., для каждого столбца $NSbox(\alpha,\beta)$ или $P(\alpha,\beta)$), при этом *не* рассчитываются все варианты битовой маски для входного значения α (имеющее 2^{MK} комбинаций). Вместо этого, вычисляются таблицы $P_i(\alpha^i,\beta)$ для отдельных фиксированных подстановок, а результирующие значения для $P(\alpha,\beta)$ вычисляется с использованием логико-вероятностного выражения, эквивалентному операции Исключающее ИЛИ-НЕ (XNOR).

Линейные свойства 2-элементной *PD-sbox*. Рассмотрим пример определения таблицы вероятностей линейной аппроксимации $P(\alpha,\beta)$ для 2-элементной *PD-sbox*, представленной на рис. 3.

Зададим параметры *PD-sbox*:

- $N = 3$ – размерность входа, бит;
- $M = 3$ – размерность выхода, бит;
- $K = 2$ – количество фиксированных подстановок;
- $sbox_0(x) = [0,4,3,2,7,1,5,6]$ – первая подстановка;
- $sbox_1(x) = [5,0,4,3,2,1,6,7]$ – вторая подстановка.

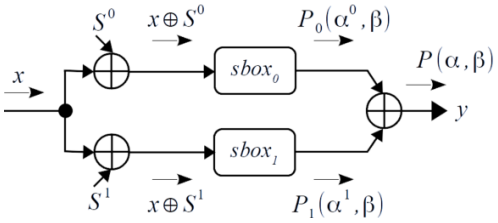

Рис. 3. Пример 2-элементной PD-sbox

Используя (1-2) определим значения $NSbox(\alpha, \beta)$ и $P(\alpha, \beta)$ для каждой фиксированной подстановки (табл. 1, 2).

Таблица 1

Значения $NSbox(\alpha, \beta)$ для $sbox_0$ и $sbox_1$

$NS_0(\alpha_0, \beta)$	β 0	1	2	3	4	5	6	7
α_0 0	8	4	4	4	4	4	4	4
1	4	2	4	6	4	6	4	6
2	4	4	6	6	4	4	6	2
3	4	6	2	4	4	6	6	4
4	4	6	4	6	6	4	2	4
5	4	4	4	4	6	2	6	6
6	4	6	6	4	2	4	4	6
7	4	4	6	2	6	6	4	4

$NS_1(\alpha_1, \beta)$	β 0	1	2	3	4	5	6	7
α_1 0	8	4	4	4	4	4	4	4
1	4	6	4	2	2	4	2	4
2	4	4	6	2	6	6	4	4
3	4	2	2	4	4	6	2	4
4	4	4	6	6	4	4	2	6
5	4	2	6	4	2	4	4	2
6	4	4	4	4	2	6	6	6
7	4	2	4	2	4	2	4	6

Таблица 2

Значения $P(\alpha, \beta)$ для $sbox_0$ и $sbox_1$.

$P_0(\alpha_0, \beta)$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.25	0.5	0.75	0.5	0.75	0.5	0.75
2	0.5	0.5	0.75	0.75	0.5	0.5	0.75	0.25
3	0.5	0.75	0.25	0.5	0.5	0.75	0.75	0.5
4	0.5	0.75	0.5	0.75	0.75	0.5	0.25	0.5
5	0.5	0.5	0.5	0.5	0.75	0.25	0.75	0.75
6	0.5	0.75	0.75	0.5	0.25	0.5	0.5	0.75
7	0.5	0.5	0.75	0.25	0.75	0.75	0.5	0.5

$P_1(\alpha_1, \beta)$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.75	0.5	0.25	0.25	0.5	0.25	0.5
2	0.5	0.5	0.75	0.25	0.75	0.75	0.5	0.5
3	0.5	0.25	0.25	0.5	0.5	0.75	0.25	0.5
4	0.5	0.5	0.75	0.75	0.5	0.5	0.25	0.75
5	0.5	0.25	0.75	0.5	0.25	0.5	0.5	0.25
6	0.5	0.5	0.5	0.5	0.25	0.75	0.75	0.75
7	0.5	0.25	0.5	0.25	0.5	0.25	0.5	0.75

Используя тривиальный метод вычислим *большую* эквивалентную подстановку, соответствующую двум параллельно включенным фиксированным подстановкам. Для этого переберём все возможные входные комбинации $x \oplus S^0 \,||\, x \oplus S^1$ и вычислим соответствующие выходные значения y. Размерность входа составит $N = 3 \cdot 2$ или $N = 6$ бит, а размерность выхода будет $M = 3$ бита.

В нашем случае *большая* эквивалентная подстановка будет иметь вид:

$$bigSbox(x) = [5, 1, 6, 7, 2, 4, 0, 5, 1, 6, 7, 2, 4, 0, 3, 0, 4, 3, 2, 7,$$
$$1, 5, 6, 4, 0, 7, 6, 3, 5, 1, 2, 3, 7, 0, 1, 4, 2, 6, 5, 2, 6, 1,$$
$$0, 5, 3, 7, 4, 1, 5, 2, 3, 6, 0, 4, 7, 6, 2, 5, 4, 1, 7, 3, 0, 7, 3, 4, 5, 0, 6, 2, 1].$$

Используя (1-2) определим значения $NSbox(\alpha,\beta)$ и $P(\alpha,\beta)$ для *большой* эквивалентной подстановки $bigSbox$. Для экономии места приведём только часть строк таблицы (табл. 3, 4).

Таблица 3

Значения $NSbox(\alpha,\beta)$ для $bigSbox$.

$\alpha\backslash\beta$	0	1	2	3	4	5	6	7
0	64	32	32	32	32	32	32	32
1	32	32	32	32	32	32	32	32
…	…	…	…	…	…	…	…	…
9	32	24	32	24	32	32	32	32
10	32	32	32	24	32	32	24	32
11	32	40	32	32	32	32	24	32
12	32	40	32	24	24	32	40	32
…	…	…	…	…	…	…	…	…
63	32	32	32	40	32	24	32	32

Таблица 4

Значения $P(\alpha,\beta)$ для $bigSbox$.

$\alpha\backslash\beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
…	…	…	…	…	…	…	…	…
9	0.5	0.375	0.5	0.375	0.5	0.5	0.5	0.5
10	0.5	0.5	0.5	0.375	0.5	0.5	0.375	0.5
11	0.5	0.625	0.5	0.5	0.5	0.5	0.375	0.5
12	0.5	0.625	0.5	0.375	0.375	0.5	0.625	0.5
…	…	…	…	…	…	…	…	…
63	0.5	0.5	0.5	0.625	0.5	0.375	0.5	0.5

Обратим внимание на следующие значения $P(\alpha,\beta)$ для $bigSbox$:

1) $\alpha = 9; \beta = 4; P(9,4) = 0.5;$
2) $\alpha = 9; \beta = 1; P(9,1) = 0.375;$
3) $\alpha = 11; \beta = 1; P(11,1) = 0.625.$

Согласно указанному принципу вычисления $bigSbox$ соответствие между значениями масок $bigSbox$, $sbox_0$ и $sbox_1$ будет иметь следующий вид:

$$\alpha = \{\alpha^0 || \alpha^1\} = \alpha^0 \cdot 2^M + \alpha^1, \quad (5)$$

где $||$ – операция конкатенации двух битовых слов.

Таким образом, мы имеем следующее соответствие между масками:

1) $\alpha = 9 = 1 \cdot 8 + 1 \rightarrow \alpha^0 = 1, \alpha^1 = 1;$
2) $\alpha = 9 = 1 \cdot 8 + 1 \rightarrow \alpha^0 = 1, \alpha^1 = 1;$
3) $\alpha = 11 = 1 \cdot 8 + 3 \rightarrow \alpha^0 = 1, \alpha^1 = 3.$

С учётом этого, указанные выше значения $P(\alpha,\beta)$ для $bigSbox$ зависят от следующих значений $P(\alpha,\beta)$ фиксированных подстановок $sbox_0$ и $sbox_1$:

1) $P(9,4) = 0.5 : P_0(\alpha^0 = 1, \beta = 4) = 0.5$ и $P_1(\alpha^1 = 1, \beta = 4) = 0.25$;
2) $P(9,1) = 0.375 : P_0(\alpha^0 = 1, \beta = 1) = 0.25$ и $P_1(\alpha^1 = 1, \beta = 1) = 0.75$;
3) $P(11,1) = 0.625 : P_0(\alpha^0 = 1, \beta = 1) = 0.25$ и $P_1(\alpha^1 = 3, \beta = 1) = 0.25$.

Обозначим функцию, которая связывает $P(\alpha,\beta)$ с $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$ как $F()$:

$$P(\alpha,\beta) = F(P_0(\alpha^0,\beta), P_1(\alpha^1,\beta)).$$

Тогда приведённые выше варианты можно записать в следующем виде:

1) $F(0{,}5; 0{,}25) = 0{,}5$;
2) $F(0{,}25; 0{,}75) = 0{,}375$;
3) $F(0{,}25; 0{,}25) = 0{,}625$.

Выражение для первого случая сразу наводит на мысль, что мы имеем зависимость, аналогичную операции XOR (Исключающее ИЛИ). Как известно [20], логико-вероятностное выражение для XOR является «терминатором» – если на любом из входов будет равновероятное значение $(x = 0{,}5)$, то на выходе также будет равновероятное значение: $Pxor(0{,}5; any) = 0{,}5$.

Выражения для второго и третьего случая позволяют уточнить вид зависимости. Найденное авторами выражение, описывающее зависимость между $P(\alpha,\beta)$, $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$, имеет следующий вид:

$$p(\alpha,\beta) = F(p_0,p_1) = 1 - ((1-p_0)\cdot p_1 + p_0\cdot(1-p_1)), \quad (6)$$

где $p_0 = P_0(\alpha^0,\beta)$; $p_1 = P_1(\alpha^1,\beta)$.

Легко проверить, что данное выражение соответствует операции Исключающее ИЛИ-НЕ (XNOR) – путём подстановки значений «0» и «1» в выражение для $F(p_0,p_1)$ в соответствии с таблицей истинности XNOR.

То, что операции XOR на выходе *PD-sbox* соответствует логико-вероятностное выражение само по себе не вызывает вопросы. Теория логико-вероятностных выражений развивается много лет и находит применение, в том числе, для расчёта надёжности сложных систем [20].

Очень интересным фактом выступает то, что здесь логико-вероятностное выражение описывает связь между вероятностями аппроксимации подстановок линейными функциями, причём эта зависимость имеет инверсный характер – на выходе *PD-sbox* расположена операция XOR, а выражение для $P(\alpha,\beta)$ соответствует логико-вероятностной форме операции XNOR (рис. 3).

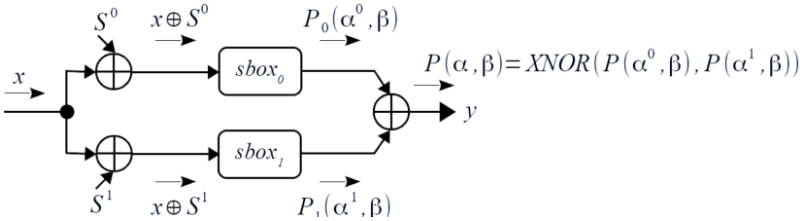

Рис. 4. Пояснения формирования $P(\alpha,\beta)$

Таким образом, мы получили **первый важный вывод**: для вычисления таблицы вероятностей $P(\alpha,\beta)$ для 2-элементной *PD-sbox* достаточно только таблиц вероятностей $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$ соответствующих фиксированных подстановок $sbox_0$ и $sbox_1$ (входящих в состав *PD-sbox*) и вычисления по формуле (6) результирующих значений таблицы вероятностей $P(\alpha,\beta)$.

Однако, с точки зрения вычислительной эффективности данный вывод пока не даёт преимуществ, так как для расчёта результирующей таблицы вероятностей $P(\alpha,\beta)$ потребуется проход 2^{2M} значений $\alpha = \alpha^0||\alpha^1$.

Линейные свойства K-элементной *PD-sbox*. Рассмотрим пример определения таблицы вероятностей линейной аппроксимации $P(\alpha,\beta)$ для 3-элементной *PD-sbox*. В соответствии с правилами булевой алгебры, мы можем представить операцию XOR от 3 переменных в виде двух последовательных операций XOR от 2 переменных. Данный вариант *PD-sbox* представлен на рис. 5.

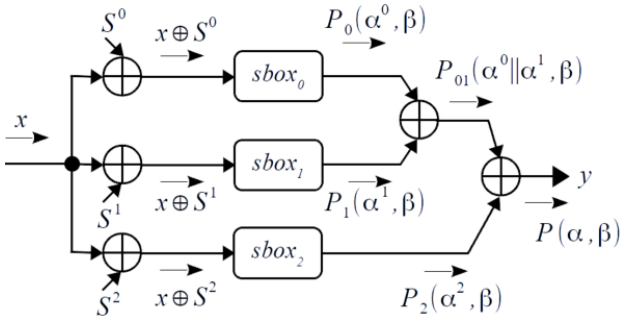

Рис. 5. Пример 3-элементной PD-sbox

Проведённые исследования показали, что для этого случая также походит выражение (6), только в качестве p_0 подставляется результат вычисления $P_{01}(\alpha^0 \parallel \alpha^1,\beta) = F(P_{01}(\alpha^0,\beta), P_1(\alpha^1,\beta))$ для двух фиксированных подстановок:

$$P(\alpha,\beta) = F(p_0,p_1) = 1 - ((1-p_0)\cdot p_1 + p_0\cdot(1-p_1)), \quad (7)$$

где $p_0 = P_{01}(\alpha^0 \parallel \alpha^1,\beta)$; $p_1 = P_2(\alpha^2,\beta)$.

Очевидно, что таким итерационным способом мы можем вычислять таблицы вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox*. Таким образом, мы получили **второй важный вывод**: для вычисления таблицы вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox* достаточно только таблиц вероятностей $P_0(\alpha^0,\beta)...P_{K-1}(\alpha^{K-1},\beta)$ соответствующих фиксированных подстановок $sbox_0...sbox_{K-1}$ (входящих в состав *PD-sbox*) и итерационного попарного вычисления по формуле (7) значений таблицы вероятностей $P(\alpha,\beta)$.

Итоговое итерационное выражение, позволяющее определить результирующее значения вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox* можно записать в следующем виде:

$$P(\alpha^0 \parallel \alpha^i,\beta)|_{imax=K-1} = 1 - \left(1 - P(\alpha^0 \parallel \alpha^{i-1},\beta)\right)\cdot P(\alpha^i,\beta) + \\ + P(\alpha^0 \parallel \alpha^{i-1},\beta)\cdot\left(1 - P(\alpha^i,\beta)\right). \quad (8)$$

Как и в предыдущем случае, с точки зрения вычислительной эффективности данный вывод пока не даёт преимуществ, так как для расчёта результирующей таблицы вероятностей $P(\alpha,\beta)$ потребуется проход 2^{KM} значений маски $\alpha = \alpha^0 \parallel \alpha^1 \parallel \ldots \parallel \alpha^{K-1}$.

Поиск максимальных значений $bias(\alpha,\beta)$. С точки зрения стойкости к линейному криптоанализу в большинстве случаев важно только определение максимальных отклонений значений преобладания $bias(\alpha,\beta)$ от идеального значения $(1/2)$.

В соответствии с выражением (3) значения преобладания $bias(\alpha,\beta)$ показывают отклонение вероятности аппроксимации подстановки линейными функциями $P(\alpha,\beta)$ от равновероятного значения 0,5. Если проанализировать выражение (6),

то мы увидим, что максимальное значение на выходе $F(p_0, p_1)$ будет в случае, если на входах будут значения p_0 и p_1, максимально отличающиеся от значения 0,5. Иными словами, максимальное значение $bias(\alpha, \beta)$ задаётся максимальными значениями исходных фиксированных подстановок $bias(\alpha^0, \beta)$ и $bias(\alpha^1, \beta)$.

Вернёмся к нашему примеру с 2-элементными *PD-sbox*. Так как нам нужны максимальные значения $bias(\alpha, \beta)$ для всех вариантов выходной маски β, то для поиска максимальных значений $bias(\alpha, \beta)$ вместо *полных* таблиц $bias(\alpha^0, \beta)$ и $bias(\alpha^1, \beta)$ нам достаточно только по одной строке с максимальными значениями из этих таблиц. Например:

$row_{maxbias}(\alpha^0, \beta) =$
$\{bias_{max}(\alpha^0, 0); bias_{max}(\alpha^0, 1); bias_{max}(\alpha^0, 2); \ldots; bias_{max}(\alpha^0, 2^{M-1})\},$
$row_{maxbias}(\alpha^1, \beta) =$
$\{bias_{max}(\alpha, 0); bias_{max}(\alpha^1, 1); bias_{max}(\alpha^1, 2); \ldots; bias_{max}(\alpha^1, 2^{M-1})\}.$

Для нашей 2-элементной *PD-sbox* строки будут иметь следующий вид:

$P_{max}(\alpha^0, \beta)$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
max	0.5	0.25	0.75	0.75	0.75	0.75	0.75	0.75

$P_{max}(\alpha^1, \beta)$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
max	0.5	0.75	0.75	0.25	0.75	0.75	0.25	0.75

$bias(\alpha^0, \beta) = |P_0(\alpha^0, \beta) - 0{,}5|$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
max	0	0.25	0.25	0.25	0.25	0.25	0.25	0.25

$bias(\alpha^1, \beta) = |P_1(\alpha^1, \beta) - 0{,}5|$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
max	0	0.25	0.25	0.25	0.25	0.25	0.25	0.25

При попарной подстановке значений $P_{max}(\alpha^0, \beta)$ и $P_{max}(\alpha^1, \beta)$ в выражение XNOR (6) мы получим строку с максимальными значениями $P_{max}(\alpha^0 \parallel \alpha^1, \beta)$:

$\alpha^0 \parallel \alpha^1 \backslash \boldsymbol{\beta}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
max	0,5	0,375	0,625	0,375	0,625	0,625	0,375	0,625

Или, если перевести в значения $bias_{max}(\alpha^0 \parallel \alpha^1, \beta)$:

$\alpha^0_{max} \parallel \alpha^1_{max} \backslash \boldsymbol{\beta}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
max	0	0,125	0,125	0,125	0,125	0,125	0,125	0,125

Полученные максимальные значения *совпадают* с максимальными значениями при расчёте *полных* таблиц $P(\alpha, \beta)$, $P_0(\alpha^0, \beta)$ и $P_1(\alpha^1, \beta)$.

Используя выражение (8) приведённый пример можно расширить на вычисление максимальных значений $P_{max}(\alpha, \beta)$ и $bias_{max}(\alpha, \beta)$ для K-элементных подстановок *PD-sbox*:

$$P_{max}(\alpha^0 \parallel \alpha^i, \beta)|_{imax=K-1} = 1 - ((1 - P_{max}(\alpha^0 \parallel \alpha^{i-1}, \beta)) \cdot P_{max}(\alpha^i, \beta) + \\ + P_{max}(\alpha^0 \parallel \alpha^{i-1}, \beta) \cdot (1 - P_{max}(\alpha^i, \beta))). \quad (9)$$

Сравнение вычислительной эффективности. Для предложенного метода вычислительные затраты будут складываться из следующих составляющих:

1. Расчёт таблиц $P_0(\alpha^0, \beta) \ldots P_{K-1}(\alpha^{K-1}, \beta)$ и преобладания $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ для фиксированных подстановок, входящих в состав *PD-sbox*. Для одной фиксированной подстановки потребуется:

$$N_{Sbox} = N_{rows} \cdot N_{columns} \cdot N_{count} = 2^M \cdot 2^M \cdot 2^M = 2^{3 \cdot M}$$

проходов в соответствии с формулой (1).

2. Поиск максимальных значений по столбцам в таблице $bias(\alpha, \beta)$ и составление строки максимальных значений. Для одной фиксированной подстановки всего требуется $N_{find\_max} = N_{rows} \cdot N_{columns} = 2^M \cdot 2^M = 2^{2 \cdot M}$ операций просмотра и определения максимальных значений.

3. Итоговый расчёт вероятности $P(\alpha, \beta)$ и преобладания $bias(\alpha, \beta)$ используя итерационное выражение (9). Для K-элементной *PD-sbox* всего потребуется $N_{iter} = K - 1$ итераций вычисления функции Исключающее ИЛИ-НЕ $F(\alpha, \beta)$.

Например, для *PD-sbox* с $K = 8$ и $M = 4$ мы получим $K \cdot N_{Sbox} = K \cdot 2^{3 \cdot M} = 8 \cdot 2^{12}$ проходов в соответствии с формулой (1) для вычисления таблиц $NSbox(\alpha, \beta)$ всех фиксированных подстановок. Такое же количество уйдёт на вычисление значений вероятностей и преобладания по формулам (2) и (3).

Кроме этого, потребуется $K \cdot N_{find\_max} = K \cdot 2^{2 \cdot M} = 8 \cdot 2^8$ операций просмотра и определения максимальных значений для всех фиксированных подстановок и $N_{iter} = 7$ итераций вычисления функции Исключающее ИЛИ-НЕ $F(\alpha, \beta)$.

В табл. 4 приведено сравнение тривиального и предложенного методов по двум наиболее ресурсоёмким показателям.

Таблица 4

Эффективность предложенного метода поиска $bias_{max}(\alpha, \beta)$

	Тривиальный метод		**Предложенный метод**	
***PD-sbox*:**	$N_{bigSbox}$	$sizeNsbox(\alpha, \beta)$	$K \cdot N_{Sbox}$	$sizeNsbox(\alpha, \beta)$
$K = 2$ и $M = 4$	2^{20}	$2^8 \times 2^4$	2^{13}	$2 \times 2^4 \times 2^4$
$K = 4$ и $M = 4$	2^{36}	$2^{16} \times 2^4$	2^{14}	$4 \times 2^4 \times 2^4$
$K = 8$ и $M = 4$	2^{68}	$2^{32} \times 2^4$	2^{15}	$8 \times 2^4 \times 2^4$
$K = 16$ и $M = 4$	2^{132}	$2^{64} \times 2^4$	2^{16}	$16 \times 2^4 \times 2^4$
$K = 2$ и $M = 8$	2^{40}	$2^{16} \times 2^8$	2^{25}	$2 \times 2^8 \times 2^8$
$K = 4$ и $M = 8$	2^{72}	$2^{32} \times 2^8$	2^{26}	$4 \times 2^8 \times 2^8$
$K = 8$ и $M = 8$	2^{136}	$2^{64} \times 2^8$	2^{27}	$8 \times 2^8 \times 2^8$
$K = 16$ и $M = 8$	2^{264}	$2^{128} \times 2^8$	2^{28}	$16 \times 2^8 \times 2^8$

Как видно, данная задача является решаемой при использовании типовых персональных компьютеров.

Заключение. Таким образом, представлен вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок, заключающийся в поиске максимальных значений преобладания (смещения) вероятности линейной аппроксимации $bias(\alpha, \beta)$ для K-элементных *PD-sbox*, который состоит из следующих этапов:

1. Расчёт таблиц значений вероятности $P_0(\alpha^0, \beta) \ldots P_{K-1}(\alpha^{K-1}, \beta)$ и преобладания $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ для фиксированных подстановок, входящих в состав *PD-sbox*.

2. Для каждой из полученных таблиц $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ формируется строка максимальных значений $bias_{maxi}(\alpha^i, \beta)$, содержащая максимальные значения преобладания для всех комбинаций маски b.

3. Для каждой из полученных таблиц $P_0(\alpha^0,\beta)\ldots P_{K-1}(\alpha^{K-1},\beta)$ формируется аналогичная строка значений $P_{maxi}(\alpha^i,\beta)$, с соответствующими п.2 значениями вероятностей.

4. Расчёт промежуточных и итоговых максимальных значений $P_{max}(\alpha,\beta)$ и $bias_{max}(\alpha,\beta)$ используя итерационное выражение (9).

Предложенный метод, в противовес известным подходам, позволяет определять максимальные значения $bias_{max}(\alpha,\beta)$ используя приемлемые вычислительные ресурсы.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Preneel B.* 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 M.* The first experimental cryptanalysis of the data encryption standard / Y. Desmedt (ed.), CRYPTO // Lecture Notes in Computer Science. – Vol. 839. – Springer, 1994. – P. 1-11.
3. *Harpes C., Kramer G.G., Massey J.L.* A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma / L.C. Guillou, J.-J. Quisquater (eds.), EUROCRYPT // Lecture Notes in Computer Science. – Vol. 921. – Springer, 1995. – P. 24-38.
4. *Selçuk A.A.* On probability of success in linear and differential cryptanalysis // J. Cryptology. – 2008. – Vol. 21 (1). – P. 131-147.
5. *Bogdanov A., Rijmen V.* Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography. – Springer, US, 2012. – P. 1-15.
6. *Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen.* Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard // Information Processing Letters. – 2014. – Vol. 114, Issue 6. – P. 322-330. – https://doi.org/10.1016/j.ipl.2014.01.007.
7. *Andrey Bogdanov, Elif Bilge Kavun, Elmar Tischhauser, Tolga Yalçın.* Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis // Journal of Computational and Applied Mathematics. – 2014. – Vol. 259, Part B. – P. 592-598. – https://doi.org/10.1016/j.cam.2013.10.020.
8. *Eichlseder M., Leander G., & Rasoolzadeh S.* (Accepted/In press). Computing Expected Differential Probability of (Truncated) Differentials and Expected Linear Potential of (Multidimensional) Linear Hulls in SPN Block Ciphers. In Progress in Cryptology - IndoCrypt 2020.
9. *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.
10. 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.
11. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Псевдо-динамические таблицы подстановки: основа современных симметричных криптоалгоритмов // Научное обозрение. – 2014. – № 12. – С. 162-166. – URL: http://www.sced.ru/ru/files/7_12_1_2014/7_12_1_2014.pdf.
12. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Исследование линейных характеристик псевдо-динамических подстановок // Известия ЮФУ. Технические науки. – 2015. –№ 5 (166). – С. 111-123.
13. *Поликарпов С.В., Кожевников А.А.* Псевдо-динамические подстановоки: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – № 8 (169). – С. 19-31.
14. *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. – Электрон. текстовые дан. – Россия. – г. Москва. – 2014 г. – Киров: МЦНИП, 2015. – С. 77-89.
15. *Sergey Polikarpov, Konstantin Rumyantsev and Dmitry Petrov.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions // AIP Conference Proceedings 1952, 020091. 2018.

16. *Polikarpov S., Petrov D., Kozhevnikov A.* On A Class Pseudo-Dynamic Substitutions PD-Sbox, With A Perfect Averaged Distribution of Differentials in Static Mode of Work // Proceedings of the 2017 International Conference on Cryptography, Security and Privacy. – Wuhan, China: ACM, 2017. – P. 17-21. – (ICCSP 17). – ISBN 978-1-4503-4867-6. – DOI: 10.1145/3058060.3058087. – URL: http://doi.acm.org/10.1145/3058060.3058087.
17. *Kozhevnikov A.A., Polikarpov S.V., Rumyantsev K.E*. On differential properties of a symmetric cryptoalgorithm based on pseudo-dynamic substitutions // Математические вопросы криптографии. – 2016. – Т. 7:2. – С. 91-102. – URL: https://doi.org/10.4213/mvk186.
18. *Поликарпов С.В., Кожевников А.А., Румянцев К.Е., Прудников В.А.* Псевдослучайная функция PCOLLAPSER, обеспечивающая экстремальный параллелизм обработки информации // Известия ЮФУ. Технические науки. – 2019. – № 5 (207). – С. 88-100.
19. *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.
20. *Рябинин И.А.* Логико-вероятностный анализ проблем и надежности, живучести и безопасности: очерки разных лет. ЮРГТУ, 2009. – 599 с. – https://books.google.ru/books?id=7ACRkgAACAAJ.

REFERENCES

1. *Preneel B.* 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 M.* The first experimental cryptanalysis of the data encryption standard, Y. Desmedt (ed.), CRYPTO, *Lecture Notes in Computer Science*, Vol. 839. Springer, 1994, pp. 1-11.
3. *Harpes C., Kramer G.G., Massey J.L*. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma, L.C. Guillou, J.-J. Quisquater (eds.), EUROCRYPT, *Lecture Notes in Computer Science*, Vol. 921. Springer, 1995, pp. 24-38.
4. *Selçuk A.A.* On probability of success in linear and differential cryptanalysis, *J. Cryptology*, 2008, Vol. 21 (1), pp. 131-147.
5. *Bogdanov A., Rijmen V*. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography. Springer, US, 2012, pp. 1-15.
6. *Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen.* Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard, *Information Processing Letters*, 2014, Vol. 114, Issue 6, pp. 322-330. Available at: https://doi.org/10.1016/j.ipl.2014.01.007.
7. *Andrey Bogdanov, Elif Bilge Kavun, Elmar Tischhauser, Tolga Yalçın.* Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis, *Journal of Computational and Applied Mathematics*, 2014, Vol. 259, Part B, pp. 592-598. Available at: https://doi.org/10.1016/j.cam.2013.10.020.
8. *Eichlseder M., Leander G., & Rasoolzadeh S.* (Accepted/In press). Computing Expected Differential Probability of (Truncated) Differentials and Expected Linear Potential of (Multidimensional) Linear Hulls in SPN Block Ciphers. In Progress in Cryptology - IndoCrypt 2020.
9. *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.
10. 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.
11. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Psevdo-dinamicheskie tablitsy podstanovki: osnova sovremennykh simmetrichnykh kriptoalgoritmov [Pseudo-dynamic substitutions: the basis of modern symmetric cryptoalgorithms], *Nauchnoe obozrenie* [Scientific Review], 2014, No. 12, pp. 162-166. Available at: http://www.sced.ru/ru/files/7_12_1_2014/7_12_1_2014.pdf.

12. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Issledovanie lineynykh kharakteristik psevdo-dinamicheskikh podstanovok [Investigation of linear characteristics of pseudo-dynamic substitutions], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 111-123.
13. *Polikarpov S.V., Kozhevnikov A.A.* Psevdo-dinamicheskie podstanovoki: issledovanie lineynykh svoystv [Pseudo-dynamic substitutions: investigation of linear propertie], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 8 (169), pp. 19-31.
14. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Psevdo-dinamicheskie tablitsy podstanovki: issledovanie differentsial'nykh kharakteristik [Pseudo-dynamic substitutions: research of differential characteristics], *Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma* [Physical and mathematical methods and information technologies in natural science, engineering and humanities: collection of materials of the international scientific e-symposium]. Electron. text data. Russia. Moscow, 2014. Kirov: MTSNIP, 2015, pp. 77-89.
15. *Sergey Polikarpov, Konstantin Rumyantsev and Dmitry Petrov.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions, *AIP Conference Proceedings* 1952, 020091. 2018.
16. *Polikarpov S., Petrov D., Kozhevnikov A.* On A Class Pseudo-Dynamic Substitutions PD-Sbox, With A Perfect Averaged Distribution of Differentials in Static Mode of Work, *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*. Wuhan, China: ACM, 2017, pp. 17-21. (ICCSP 17). ISBN 978-1-4503-4867-6. DOI: 10.1145/3058060.3058087. Available at: http://doi.acm.org/10.1145/3058060.3058087.
17. Kozhevnikov A.A., Polikarpov S.V., Rumyantsev K.E. On differential properties of a symmetric cryptoalgorithm based on pseudo-dynamic substitutions, *Matematicheskie voprosy kriptografii* [Mathematical questions of Cryptography], 2016, Vol. 7:2, pp. 91-102. Available at: https://doi.org/10.4213/mvk186.
18. *Polikarpov S.V., Kozhevnikov A.A., Rumyantsev K.E., Prudnikov V.A.* Psevdosluchaynaya funktsiya PCOLLAPSER, obespechivayushchaya ekstremal'nyy parallelizm obrabotki informatsii [Pseudo-random function PCOLLAPSER providing extreme parallelism of information processing], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2019, No. 5 (207), pp. 88-100.
19. *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.
20. *Ryabinin I.A.* Logiko-veroyatnostnyy analiz problem i nadezhnosti, zhivuchesti i bezopasnosti: ocherki raznykh let [Logical-probabilistic analysis of problems and reliability, survivability and safety: essays from different years]. YURGTU, 2009. 599 p. Available at: https://books.google.ru/books?id=7ACRkgAACAAJ.

Статью рекомендовала к опубликованию к.т.н. К.Б. Дахкильгова.

Поликарпов Сергей Витальевич – Южный федеральный университет; e-mail: polikarpovsv@sfedu.ru; 347900, г. Таганрог, ул. Чехова, 2, корпус «И»; тел.: 89085159762; к.т.н.

Прудников Вадим Александрович – e-mail: pruvad@yandex.ru; тел.: 89198961427.

Румянцев Константин Евгеньевич – e-mail: rke2004@mail.ru, тел.: 89281827209; д.т.н.; профессор.

Polikarpov Sergey Vitalievich – Southern Federal University; e-mail: polikarpovsv@sfedu.ru; 347900, Taganrog, 2, Chekhov street; phone: +79085159762; cand. of eng. sc.

Prudnikov Vadim Aleksandrovich – e-mail: pruvad@yandex.ru; phone: +79198961427.

Rumyantsev Konstantin Evgenyevich – e-mail: rke2004@mail.ru; phone: +79281827209; dr. of eng. sc.; professor.