УДК 004.056.55 DOI 10.18522/2311-3103-2022-6-148-162

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

ИССЛЕДОВАНИЕ СВОЙСТВ МИНИВЕРСИИ ПСЕВДО-СЛУЧАЙНОЙ ФУНКЦИИ PCOLLAPSER

Целью работы является оценка криптографических свойств семейства псевдо-случайных функций (PRF) pCollapser на основе исследования свойств её миниверсии mini_pCollapser_12x12 при использования фиксированных подстановок с предельно низкими криптографическими свойствами. В качестве элемента сравнения использована миниверсия типовой функции на основе SP-сети, содержащая аналогичное количество фиксированных подстановок и имеющая аналогичную размерность входа/выхода, равную 12 битам. Для достижения поставленной цели решались следующие задачи: – определение структуры исследуемых функций и количества раундов; – определение модели формирования фиксированных подстановок с предельно низкими криптографическими свойствами; – генерация наборов 6-битовых фиксированных подстановок с предельно низкими криптографическими свойствами; – включение в исследуемые функции полученных подстановок и определение основных криптографических свойств функций – максимальное значение преобладания для отдельных значений ключей и максимальное усреднённое по всему множеству ключей значение преобладания, максимальное и максимальное усреднённое по всему множеству ключей значение в таблице распределения разностей, алгебраическая степень и алгебраический иммунитет; – анализ полученных результатов. В работе представлены две модели формирования фиксированных подстановок с предельно низкими криптографическими свойствами – на основе перемешивания значений ячеек в предварительно заполненной таблице и на основе простейшей ARX-функции (состоящей из операций сложения по модулю, циклического сдвига и исключающего ИЛИ). Использование фиксированных подстановок с предельно низкой нелинейностью позволяет оценить, насколько сложной (нелинейной) является исследуемая функция и какой минимальный уровень нелинейности необходим для эффективного разрушения статистических зависимостей между входными/выходными данными. Кроме этого, становится ясным возможность применения в качестве нелинейных элементов ARX-функций, зачастую обладающих спорными и явно низкими криптографическими свойствами, но позволяющих создавать высокоскоростные программные и аппаратные реализации. Определено, что миниверсия PRF pCollapser, в отличии от типовой функции на основе SP-сети, позволяет получить из набора ARX-функций с предельно низкими криптографическими свойствами, качественную нелинейную функцию, учитывая то, что других нелинейных элементов в pCollapser не представлено. Полученные результаты отражают наличие принципиальной разницы между PRF pCollapser и типовой PRF на базе SP-сети, а также подтверждают правильность концепции псевдо-динамических подстановок PD-sbox и состоящей из них функции pCollapser в целом.

Криптографические свойства; псевдо-случайная функция; псевдо-динамические подстановки; pCollapser.

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

STUDY OF THE MINIVERSION PROPERTIES IN THE PSEUDO-RANDOM FUNCTION PCOLLAPSER

The aim of the work is to evaluate the cryptographic properties of the pCollapser family of pseudo-random functions (PRF) based on the study of the properties of its mini_pCollapser_12x12 mini-version using fixed substitutions with extremely low cryptographic properties. As a comparison element, we used a mini-version of a typical function based on an SP-net, containing a similar number of fixed substitutions, and having a similar input/output dimension equal to 12 bits. To achieve this goal, the following tasks were solved: – determination of the structure of the studied functions and the number of rounds; – definition of a model for the formation of fixed substitutions with extremely low cryptographic properties; – generation of sets of 6-bit fixed substitutions with extremely low cryptographic properties;

– inclusion of the substitutions obtained into the functions under study and determination of the main cryptographic properties of functions – the maximum dominance value for individual key values and the maximum dominance value averaged over the entire set of keys, the maximum and averaged over the entire set of keys value in the difference distribution table, algebraic degree and algebraic immunity; – analysis of the obtained results. The paper presents two models for the formation of fixed substitutions with extremely low cryptographic properties – based on the mixing of cell values in a pre-filled table and based on the simplest ARX function (consisting of modulo addition, cyclic shift and XOR). The use of fixed substitutions with extremely low non-linearity makes it possible to estimate how complex (non-linear) the function under study is and what minimum level of non-linearity is necessary to effectively destroy the statistical dependencies between input/output data. In addition, it becomes clear that ARX functions can be used as non-linear elements, which often have controversial and clearly low cryptographic properties, but allow creating high-speed software and hardware implementations. It has been determined that the PRF pCollapser mini-version, in contrast to the typical function based on the SP network, makes it possible to obtain a high-quality non-linear function from the set of ARX-functions with extremely low cryptographic properties, given that no other non-linear elements are presented in pCollapser. The obtained results reflect the existence of a fundamental difference between the pCollapser PRF and a typical SP-network based PRF and confirm the correctness of the concept of PD-sbox pseudo-dynamic substitutions and the pCollapser function consisting of them as a whole.

Cryptographic properties; pseudo-random function; pseudo-dynamic substitutions; pCollapser.

Введение. Псевдо-динамические операции подстановки *PD-sbox*, являются основным нелинейным элементом перспективной псевдо-случайной функции *pCollapser*. Конструкция обладает рядом параметров, которые позволяют эффективно разрушать статистические зависимости между входными и выходными значениями за счёт динамической трансформации их криптографических свойств, а также позволяет обеспечить параллельную работу входящих в её состав фиксированных подстановок *sbox*. В свою очередь, *pCollapser* позволяет продемонстрировать реализацию возможностей псевдо-динамических операций подстановок, что отражается в обеспечении динамической работы *PD-sbox*, путём формирования и распределения управляющих значений, а также в реализации экстремального параллелизма обработки данных за счёт независимого функционирования группы псевдо-динамических операций подстановок в рамках одного раунда [1].

Одним из способов анализа свойств псевдо-случайных функций (PRP) и псевдо-случайных перестановок (PRP) является анализ их миниверсий – алгоритмов, повторяющих концепцию оригинальных функций, однако, имеющих ряд усечённых параметров, в частности: размер блока данных, длину ключа, размер операций подстановки/перестановки, и других, с последующей экстраполяцией результатов на полноразмерную псевдо-случайную функцию. В качестве примера следует привести работы [2–7], посвященные анализу свойств миниверсии криптоалгоритма AES (Advanced Encryption Standard).

В работе [2] представлена мини-версия криптоалгоритма AES – Mini-AES, позволяющая достичь лучшего понимания его криптографических свойств. Криптоалгоритм, по сравнению с оригиналом, обладает значительно упрощёнными свойствами, повторяя структуру. Указанная псевдо-случайная функция рассматривается исключительно как обучающий шифр, не предназначенный для его применения вне рамок исследований. В работе [3] представлен пример SQUARE-атаки на Mini-AES.

В [4] рассматривается линейный криптоанализ второго раунда псевдо-случайной функции Mini-AES. Результаты исследований демонстрируют уязвимость второго раунда миниверсии к линейной атаке. Как следствие, данный факт позволяет лучше понять криптоанализ полноценного AES.

В работе [5] продемонстрированы результаты разностной атаки на криптоалгоритм Mini-AES. Разностные пути построены с использованием всех комбинаций коэффициента распространения без повторения. Чтобы получить практические результаты, авторы реализовали извлечение ключа для разностных свойств, которые имеют наибольшую и наименьшую вероятность появления. Основываясь на общем коэффициенте распространения и полученной сложности, авторы делают вывод о том, что криптоалгоритм Mini-AES уязвим для разностного криптоанализа.

В работе [6] рассматривается алгебраическая атака на функцию Mini-AES. В исследовании представлены результаты применения алгебраической атаки на Mini-AES для получения системы полиномиальных уравнений алгоритма и её решений с использованием XL-алгоритма. Система полиномиальных уравнений миниверсии определяется системой полиномиальных уравнений для *sbox*-ов (операций подстановок или узлов замены), операции формирования ключей (key schedule), операции шифрования. Основываясь на уникальных характеристиках системы полиномиальных уравнений, балансе числа полиномиальных уравнений и числа мономов, следует сделать вывод о потенциальной уязвимости Mini-AES к алгебраическому криптоанализу.

В [7] представлено исследование возможности криптоанализа алгоритма Mini-AES с использованием машинного обучения. Разработана нейросеть, включающая три скрытых слоя и контролируемое число нейронов. Нейросеть, обученная контролируемым количеством случайных пар открытого текста и шифртекста, осуществила успешную атаку на криптоалгоритм.

На примере исследований одного из вариантов миниверсии широко распространённого криптоалгоритма AES следует сделать вывод о том, что проблема анализа упрощённых криптоалгоритмов является актуальной, так как в большинстве случаев подобный подход позволяет лучше понимать принципы криптоанализа полноценных PRF и PRP.

Статистические методы криптоанализа основываются на том, что нелинейные элементы исследуемых криптографических функций (PRP и PRF) не обладают идеальными свойствами (например, идеальной таблицей распределения разностей DDT или идеальной таблицей линейных аппроксимаций LAT). При наборе определённого количества статистики (пар входных-выходных сообщений) эти свойства начинают проявляться и позволяют уверенно различать поведение исследуемой функции от случайной (что соответственно, даёт возможность с определённой вероятностью определять значения ключа). Для практически стойких алгоритмов сложность набора статистики и определения по ней ключа должна превышать стойкость к общим атакам (полный перебор и др.)

Естественным способом противодействия статистическим атакам является применение в качестве нелинейных элементов динамических *sbox*-ов, у которых изменяется правило замены в зависимости от значений на управляющем входе (которые сами зависят как от ключа, так и от промежуточных значений) и, соответственно, изменяются распределение значений в DDT и LAT. Соответственно, при попытке набора статистики происходит усреднение значений в DDT и LAT. Чем больше осуществляется набор статистики, тем сильнее усреднение и можно добиться приближения значений в DDT и LAT к идеальным. Таким образом, динамические подстановки могут предотвращать возможность осуществления статистических атак.

В данной работе рассматривается анализ свойств миниверсии псевдослучайной функции *pCollapser* при использовании различных наборов фиксированных подстановок, а также её сравнение с параметрами миниверсии типовой функции на основе SP-сети (состоящая из слоёв операций подстановок и перестановок). Для оценки свойств использовались наборы фиксированных *sbox*-ов с предельно низкими криптографическими свойствами.

Цель работы – оценить криптографические свойства семейства псевдо-случайных функций *pCollapser* на основе исследования свойств её миниверсии *mini_pCollapser_12x12* при использования фиксированных *sbox*-ов с предельно низкими криптографическими свойствами.

Используемые термины и обозначения:

PRF – псевдо-случайная функция;

PRP – псевдо-случайная перестановка;

sbox (s-box) является сокращением от substitution box – блок подстановки/замены (узел замены, в терминологии ГОСТ 28147-89). В данной работе мы будем для краткости использовать термин «подстановка» или *sbox* для обозначения операции над двоичными словами, которую можно представить в виде табличной замены значений, операция не обязательно должна быть взаимно однозначной (как, например, в криптоалгоритме DES [8]);

fsbox – блок фиксированной подстановки/замены;

PD-sbox – псевдо-динамическая подстановка, функция, состоящая из набора фиксированных подстановок и операций XOR;

max bias – максимальное значение преобладания (полученное на основе таблицы линейных аппроксимаций LAT);

avg max bias – максимальное усреднённое по всему множеству ключей значение преобладания;

max Δs – максимальное значение в таблице распределения разностей (DDT);

max avg Δs – максимальное усреднённое по всему множеству ключей значение в таблице распределения разностей (дифференциалов);

λs – алгебраическая степень;

AI – алгебраический иммунитет.

Описание псевдо-динамических подстановок *PD-sbox.* Структура псевдо-динамической подстановки *PD-sbox* состоит из набора фиксированных *sbox*-ов [9,10]. Аргумент каждой фиксированной операции подстановки параметризован значением состояния S_i, где i – номер фиксированной подстановки (от 0 до $N-1$).

Текущее значение состояния $S = \{S_0, S_1, S_2, \dots, S_{N-1}\}$ задаёт одну операцию подстановки из набора возможных *PD-sbox*.

Подстановку, полученную с помощью конкретного значения S мы будем называть эквивалентной (сгенерированной) операцией подстановки для *PD-sbox*. Соответственно, число эквивалентных подстановок для *PD-sbox* определяется количеством возможных значений состояний S. Это подразумевает то, что значения состояния S не обязательно являются фиксированными и могут динамически изменяться в процессе шифрования, а вероятностные свойства соответствуют равномерному распределению.

Общий вид выражения, описывающего структуру псевдо-динамической подстановки *PD-sbox*:

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

где *sbox* – фиксированная операция подстановки; N – количество фиксированных подстановок; X – биты на входе; Y – биты на выходе; S – биты состояния псевдо-динамической подстановки; $\oplus$ – операция сложения по модулю 2.

PD-sbox может работать в двух режимах – статическом (ключезависимом) и динамическом (зависимом от значений ключа и промежуточных состояний).

В случае динамического равновероятного изменения состояний S, как дифференциальные усреднённые свойства, так и линейные, близки к идеальным (при усреднении характеристик по всем эквивалентным операциям подстановки). Это позволяет нейтрализовать существующие методы дифференциального и линейного криптоанализа. [9, 10]

Псевдо-случайная функция mini_pCollapser_12x12. На CTCrypt'2015 была впервые представлена структура *"Collapser"* [11], в виде цепочек последовательно включенных *PD-sbox*. Данная структура была демонстратором возможного применения *PD-sbox*. В *pCollapser* была предложена PRF *"pCollapser"* (parallel Collapser), в которой были устранены ряд недостатков *"Collapser"*. В *"pCollapser"* в рамках одного раунда все *PD-sbox* работают параллельно и независимо друг от друга. Это даёт много возможностей по оптимальной аппаратной реализации: итеративная реализация обеспечивает максимальную пропускную способность и минимальный критический путь, реализация на базе *PD-sbox* позволяет достичь сбалансированной пропускной способности и занимаемой площади, последовательная реализация обеспечивает минимальную площадь на кристалле.

Для исследования будем использовать упрощённую мини-версию PRF *"pCollapser"* с размерностями входа/выхода 12 бит – *mini_pCollapser_12x12*, представленный на рис. 1.

mini_pCollapser_12x12 в каждом раунде содержит 2 параллельно включенные псевдо-динамические подстановки *PD-sbox0* и *PD-sbox*1, каждая из которых состоит из 4 фиксированных подстановок *fsbox1 – fsbox4*.

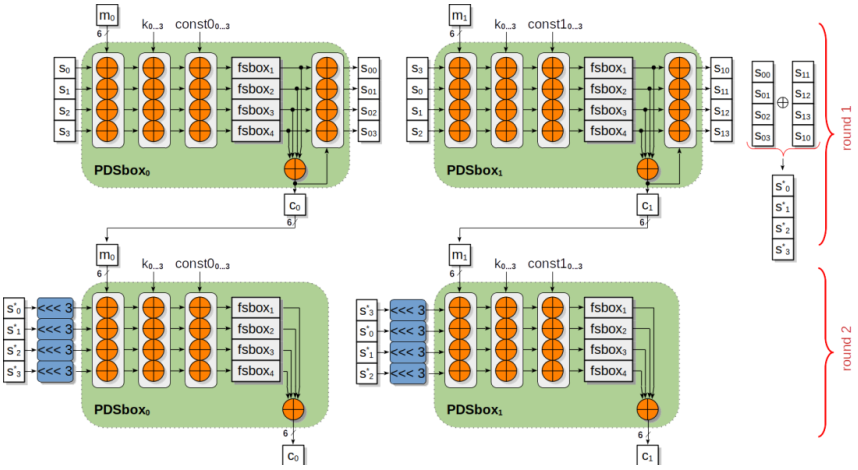

Рис. 1. Миниверсия PRF pCollapser (mini_pCollapser_12x12)

Выражение, описывающее выходы псевдо-динамические подстановки:

$$c_i = \bigoplus_{j=0}^{3} fsbox_j\left(m_i \oplus s_j^i \oplus k_j^i \oplus const_j^i\right),$$

где: i – индекс 6-битного слова входного/выходного вектора, соответственно, индекс *PD-sbox*; j – индекс элементов *PD-sbox*; m_i – 6-битное слово входного вектора; c_i – 6-битное слово выходного вектора; $fsbox_j$ – фиксированные операции подстановки (элементы *PD-sbox*); s_j^i – 6-битные слова значения состояния входного вектора (для каждого *PD-sbox*); k_j^i – 6-битное слово раундового ключа (для каждого *PD-sbox*); $const_j^i$ – 6-битное слово константы (для каждого *PD-sbox*).

Выражение для функции выработки индивидуального (на выходе отдельной PD-sbox) значения состояния:

$$s_n^i = c_i \oplus fsbox_j\left(m_i \oplus s_j^i \oplus k_j^i \oplus const_j^i\right) =$$

$$= \bigoplus_{n=0,\, n\neq i}^{3} fsbox_j\left(m_i \oplus s_j^i \oplus k_j^i \oplus const_j^i\right).$$

Выражение для функции, вырабатывающей индивидуальный (для каждого *PD-sbox*) вектор управляющего состояния:

$$s_j = s_j <<< 2,$$

где операция: $a >>> b$ – циклический побитовый сдвиг в векторе a на b элементов в право.

Выражение для функции, вырабатывающей новый вектор управляющего состояния:

$$s^* = (s_0^*, s_1^*, \dots, s_3^*) =$$

$$= \bigoplus_{i=0}^{1} \left(s^i <<< ((i \cdot 6) \bmod 24)\right),$$

где $s^i = \left(s_0^i, s_1^i, \dots, s_3^i\right)$, а >>> b – циклический побитовый сдвиг в векторе a на b элементов влево.

Всего, *mini_pCollapser_12x12* содержит 2 раунда (итерации) преобразования. В первом раунде *PD-sbox* работают в статическом режиме (значения вектора входного управляющего состояния зависят только от ключа), значение входного управляющего состояния фиксировано и равно нулю. Первый раунд служит для запуска динамического режима работы *PD-sbox* во втором раунде (значения вектора входного управляющего состояния зависят от ключа и входных значений).

Псевдо-случайная функция *mini_conventional_SPN_12x12.* Рассмотрим свойства псевдо-случайной функции на базе типовой и SP-сети [12, 13] на примере её миниверсии – *mini_conventional_SPN_12x12*, структура которой приведена на рис. 2. Она содержит 4 основных блока операций: сложение входных значений с ключом (XOR); сложение с константами; блок подстановок (основная нелинейная операция) и блок линейного перемешивания на основе циклического сдвига влево на 3 бита.

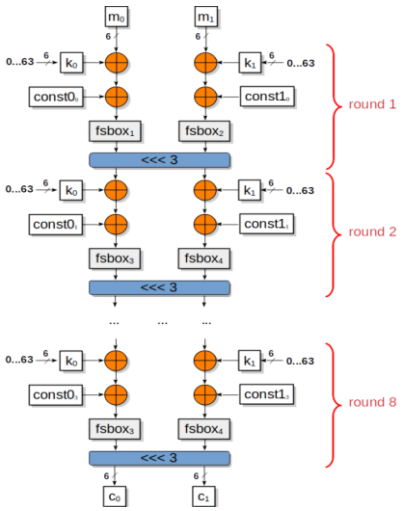

Рис. 2. Миниверсия типовой функции на основе SP-сети (mini_conventional_SPN_12x12)

Используемая *mini_conventional_SPN_12x12* содержит 8 раундов преобразования для обеспечения паритета по количеству нелинейных элементов *mini_pCollapser_12x12*. В табл. 1 приведены основные характеристики исследуемых функций.

Таблица 1

Параметры исследуемых функций

Параметр	*mini_conventional_SPN_12x12*	*mini_pCollapser_12x12*
1. Размерность входа/выхода	12 бит	
2. Количество раундов (итераций)	8	2
3. Критический путь, *sbox*-ов	8	2
4. Количество *sbox*-ов	16	
6. Количество XOR 6x6	32	32 + 32
7. Количество ROTL	8	8

Формирование фиксированных *sbox* с предельно низкими криптографическими свойствами. Для оценки свойств миниверсий использовались фиксированные *sbox*-ы с предельно низкими криптографическими свойствами, так как при использовании качественных *sbox*-ов исследуемые функции не будут отличимы от случайных PRF и PRP такой же размерности (для случаев 8 и более раундов преобразования информации). Использование фиксированных *sbox*-ов с предельно низкой нелинейностью позволяет оценить, насколько сложной (нелинейной) является исследуемая функция и какой минимальный уровень нелинейности необходим для эффективного разрушения статистических зависимостей между входными/выходными данными. Кроме этого, станет ясным возможность применения в качестве нелинейных элементов ARX-функций (состоящих из операций сложения по модулю, циклического сдвига и исключающего ИЛИ), зачастую обладающих спорными и явно низкими криптографическими свойствами, но позволяющих создавать высокоскоростные программные и аппаратные реализации (как пример, ARX операции используются в популярном поточном шифре ChaCha20 [14]).

Модель фиксированных *sbox*-ов №1. Для формирования тестовых *sbox*-ов с предельно низкими криптографическими свойствами применялся следующий алгоритм:

1. Ячейки в *sbox* заполнялись значениями $(i+1) mod N$, где i – индекс ячейки, N – количество ячеек;

2. Случайным образом выбирались две ячейки, после чего производился обмен значениями этих ячеек;

3. Пункт 2 повторялся Nmix раз (Nmix – количество перемешиваний ячеек).

Предложенный алгоритм позволяет обеспечить обратимость (биективность) получаемых *sbox*-ов.

Для исследования использовались значения $Nmix = 9, 11, \dots, 19$. Соответственно, для каждого значения Nmix формировался набор из 4 отличающихся *sbox*-ов. Одни и те же наборы *sbox*-ов применялись как в *mini_pCollapser_12x12*, так и в *mini_conventional_SPN_12x12*.

Модель фиксированных *sbox*-ов №2. Для формирования тестовых *sbox*-ов с предельно низкими криптографическими свойствами применялась ARX-функция следующего вида:

$$y = ROTL\big((x \oplus ROTL(x,t) \oplus const), t_2\big),$$

где x – входное 6 битное слово; $const$ – 6-битная константа; ROTL – операция циклического сдвига влево на t бит, $t_2 = 0,2,3,4$.

Оцениваемые криптографические свойства. В рамках исследования будем оценивать основные статистические криптографические свойства:

♦ разностные – определяя максимальные значения в таблице распределения разностей *max Δs* и максимальные усреднённое по всему пространству ключей значения в таблице распределения разностей *avg max Δs* [15, 17, 18];

♦ линейные – определяя максимальные значения преобладания *max bias* и максимальные усреднённые усреднённое по всему пространству ключей значения преобладания *avg max bias* [16–18];

♦ Алгебраические свойства: алгебраическая степень λs и алгебраический иммунитет *AI* [19, 20].

Криптографические свойства тестовых фиксированных *sbox*-ов. Пример полученных *sbox*-ов при $Nmix = 1$ (размерность входа/выхода 6x6 бит) при использовании модели №1:

fsbox1: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 27, 22, 23, 24, 25, 26, 21, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 0];

fsbox2: [2, 40, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 4, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 0];

fsbox3: [4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 0, 54, 58, 62, 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63, 50];

fsbox4: [8, 16, 24, 32, 40, 48, 56, 1, 9, 17, 25, 33, 41, 49, 57, 2, 10, 18, 26, 34, 42, 50, 58, 3, 11, 19, 27, 35, 43, 51, 59, 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, 21, 29, 37, 45, 53, 61, 6, 14, 22, 30, 38, 46, 54, 62, 55, 15, 23, 31, 39, 47, 7, 63, 0].

На рис. 3 приведены гистограммы (в виде цветовых градиентов) распределения максимальные значения в таблице распределения разностей *max Δs* для фиксированных подстановок *fsbox1-fsbox4* в зависимости от значений *Nmix*. Для сравнения, под значением $Nmix = 21$ приведены типовые значения для случайно сформированных *sbox*-ов.

Для построения гистограмм использовались результаты 20 попыток генерации фиксированных подстановок.

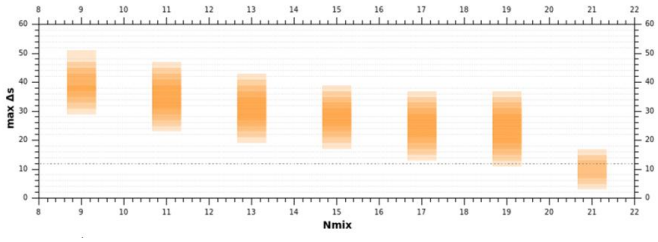

Рис. 3. Максимальные значения в таблице распределения дифференциалов (DDT) max Δs для тестовых фиксированных sbox-ов

На рис. 4 приведены гистограммы (в виде цветовых градиентов) распределения максимальных значений преобладания в таблице линейных аппроксимаций (LAT) *max bias* для тестовых фиксированных подстановок *fsbox1-fsbox4* в зависимости от значений *Nmix*.

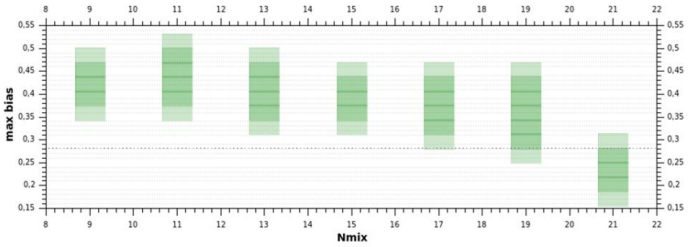

Рис. 4. Максимальные значения преобладания в таблице линейных аппроксимаций (LAT) max bias для тестовых фиксированных sbox-ов

Алгебраическая степень для тестовых фиксированных *sbox*-ов λs: от 4 до 5. Алгебраический иммунитет *AI* для тестовых фиксированных *sbox*-ов принимал значение 2.

Приведённые значения подтверждают, что мы получили *sbox*-ы с предельно низкими (плохими) криптографическими свойствами. Так, для *sbox* размерностью 6x6 бит диапазон значений Δs составляет $0 \dots 64$. Для случайно сформированного *sbox* размерностью 6x6 бит значение Δs обычно не превышает 12. Для полученных *sbox*-ов значения Δs составляют от 46 (при $Nmix = 9$) до 16 (при $Nmix = 19$).

Криптографические свойства исследуемых функций. Рассмотрим результаты анализа криптографических свойств миниверсий псевдо-случайных функций *mini_pCollapser_12x12* – на базе псевдо-динамических подстановок *PD-sbox*, включающих набор фиксированных подстановок *sbox*, обладающие крайне низкими заведомо неудовлетворительными криптографическими свойствами, а также *mini_conventional_SPN_12x12* – на базе типовой SP-сети, включающей фиксированные операции *sbox*, аналогичные тем, из которых состоят *PD-sbox*.

Разностные свойства. На рис. 5 представлены гистограммы (в виде цветовых градиентов) распределения максимальных усреднённых значений в таблице распределения разностей *avg max* Δs. На рис. 6 представлены максимальные значения в таблице распределения разностей *max* Δs в зависимости от значений *Nmix*.

Для построения гистограмм использовались результаты 20 попыток генерации фиксированных подстановок, применяемых в исследуемых функциях. Для каждой попытки при вычислении усреднённых значений набиралась статистика на основе 64 значений ключа $(k_1 = 0 \dots 63, k_2 = 0 \dots 63)$.

Синим градиентом показаны свойства для *mini_conventional_SPN_12x12*, пурпурным цветом – *для mini_pCollapser_12x12*.

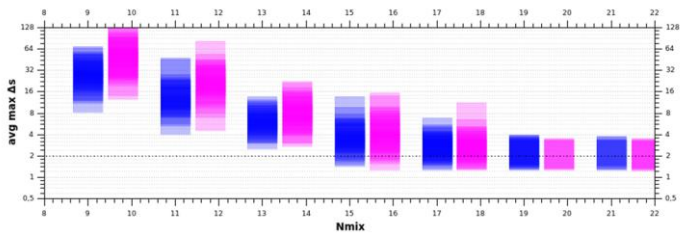

Рис. 5. Максимальные усреднённые значения в таблице распределения разностей (DDT) avg max Δs для исследуемых миниверсий

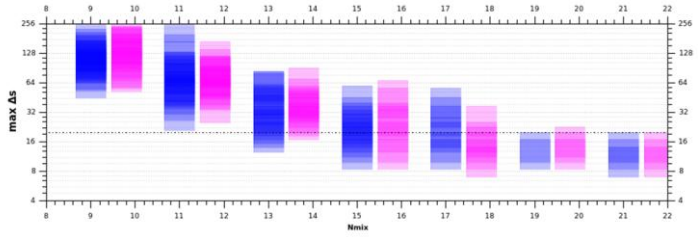

Рис. 6. Максимальные значения в таблице распределения разностей (DDT) max Δs для исследуемых миниверсий

Для функций размерностью 12x12 бит диапазон значений Δs может составлять $0 \ldots 4096$. Идеальное значение Δs равно 1,0. Граница устойчивости к статистической разностной атаке соответствует $\Delta s < 2$ [11, 13, 15].

Для случайных PRP и PRF размерностью 12x12 бит максимальное значение Δs обычно не превышает 20.

Таким образом, разностные свойства исследуемых функций достаточно близки и при $Nmix = 15$ могут приближаться к разностным свойствам случайных функций.

Линейные свойства. На рис. 7 представлены гистограммы (в виде цветовых градиентов) распределения максимальных усреднённых значений преобладания *avg max bias*. На рис. 8 представлены максимальные значения преобладания *max bias* в зависимости от значений *Nmix*.

Для построения гистограмм использовались результаты 20 попыток генерации фиксированных подстановок, применяемых в исследуемых функциях. Для каждой попытки при вычислении усреднённых значений набиралась статистика на основе 64 значений ключа ($k_1 = 0 \ldots 63, k_2 = 0 \ldots 63$).

Синим градиентом показаны свойства для *mini_conventional_SPN_12x12*, пурпурным цветом – для *mini_pCollapser_12x12*.

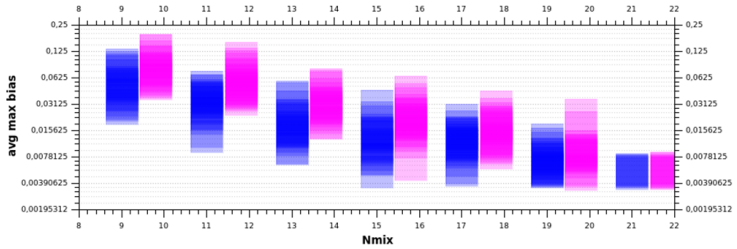

Рис. 7. Максимальные усреднённые значений преобладаний avg max bias для исследуемых миниверсий

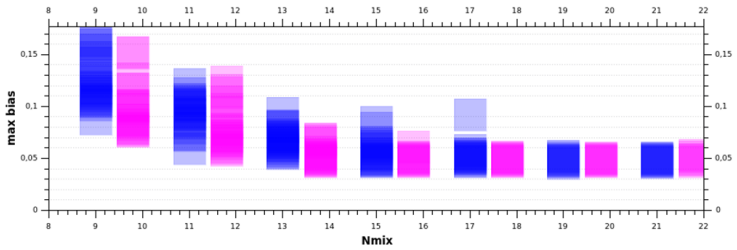

Рис. 8. Максимальные значений преобладания max bias для исследуемых миниверсий

Для функций размерностью 12x12 бит диапазон усреднённых значений *avg max bias* может составлять $-0{,}5 \ldots 0{,}5$. Идеальное значение *avg max bias* равно 0. Граница устойчивости к статистической атаке на основе линейных аппроксимаций соответствует $max\ bias < 2^{-6}$ [9, 16]. Для случайных PRP и PRF размерностью 12x12 бит максимальное значение *max bias* обычно не превышает 0,0478516 или $2^{-4.385}$.

Таким образом, при $Nmix < 15$ усреднённые значений преобладаний для *mini_pCollapser_12x12* заметно уступают усреднённым значений преобладаний для *mini_conventional_SPN_12x12.* А при $Nmix = 15$ и более приближаются к линейным свойствам случайных функций.

При анализе максимальных значений преобладания *mini_pCollapser_12x12* напротив, имеет небольшое преимущество перед *mini_conventional_SPN_12x12* при $Nmix < 15$. А при $Nmix = 15$ и более приближаются к свойствам случайных функций.

Алгебраические свойства: обе функции имеют значения алгебраической степени λs равное 11 и алгебраического иммунитета *AI* равный 4 при $Nmix = 9$ и более, что говорит об отсутствии слабых алгебраических свойств.

Модель фиксированных подстановок №2. Таблицы замены для ARX-функций, полученные при помощи модели №2:

fsbox1: [57, 62, 51, 56, 45, 50, 39, 44, 33, 38, 27, 32, 21, 26, 15, 20, 8, 13, 2, 7, 60, 1, 54, 59, 48, 53, 42, 47, 36, 41, 30, 35, 27, 32, 21, 26, 15, 20, 9, 14, 3, 8, 61, 2, 55, 60, 49, 54, 42, 47, 36, 41, 30, 35, 24, 29, 18, 23, 12, 17, 6, 11, 0, 5];

fsbox2: [51, 23, 58, 30, 2, 37, 9, 44, 20, 59, 31, 3, 38, 10, 45, 17, 56, 28, 0, 39, 11, 46, 18, 53, 29, 1, 36, 8, 47, 19, 54, 26, 33, 5, 40, 12, 51, 23, 58, 30, 6, 41, 13, 48, 20, 59, 31, 3, 42, 14, 49, 21, 56, 28, 0, 39, 15, 50, 22, 57, 29, 1, 36, 8];

fsbox3: [60, 52, 44, 36, 30, 22, 14, 6, 63, 55, 47, 39, 25, 17, 9, 1, 58, 50, 42, 34, 28, 20, 12, 4, 61, 53, 45, 37, 31, 23, 15, 7, 48, 40, 32, 24, 18, 10, 2, 57, 51, 43, 35, 27, 21, 13, 5, 60, 54, 46, 38, 30, 16, 8, 0, 63, 49, 41, 33, 25, 19, 11, 3, 58];

fsbox4: [52, 7, 17, 35, 61, 0, 26, 44, 38, 56, 3, 21, 47, 49, 12, 30, 24, 42, 52, 7, 17, 35, 61, 0, 10, 28, 38, 56, 3, 21, 47, 49, 61, 0, 26, 44, 54, 9, 19, 37, 47, 49, 12, 30, 40, 58, 5, 23, 17, 35, 61, 0, 26, 44, 54, 9, 3, 21, 47, 49, 12, 30, 40, 58].

В табл. 2 приведены криптографические свойства ARX-функций, выступающих в роли фиксированных подстановок, а в таблице 3 приведены криптографические свойства исследуемых миниверсий при использовании в качестве фиксированных подстановок ARX-функций.

Таблица 2

Криптографические свойства ARX-функций

Свойства	***fsbox1_6x6***	***fsbox2_6x6***	***fsbox3_6x6***	***fsbox4_6x6***	***rnd_sbox_6x6***
max Δs	32	32	56	32	8
max bias	-0,5	0,5	-0,5	-0,5	0,21875
λs	**1** [1, 2, 3, 4, 5, 5]	**1** [4, 4, 1, 2, 3, 4]	**1** [4, 5, 6, 1, 2, 3]	**1** [3, 4, 4, 4, 1, 2]	5
AI	1	1	1	1	2

Таблица 3

Криптографические свойства исследуемых миниверсий

Свойства	*mini_conventional_SPN_12x12*	*mini_pCollapser_12x12*
avg max Δs	2055,25	2,0625
max Δs	2080	12
avg max bias	0,2537	0,0053
max bias	0,3284	0,0486
λs	11	11
AI	2	4

В соответствии с табл. 2 полученные *fsbox1-fsbox4* по факту являются линейными функциями (преобладание равно 0,5), что, в частности, отражается в крайне низком значении алгебраической степени, равной 1.

Полученные результаты вскрывают наличие принципиальной разницы между PRF *pCollapser* и типовой функции на базе SP-сети.

В частности, SP-сеть при использовании данных ARX-функций не способна за 8 раундов набрать достаточную сложность преобразования, что выражается в неприемлемо больших значениях max Δs, avg max Δs, max bias и avg max bias.

PRF *pCollapser* в данном случае наоборот, имеет хорошие значения max Δs, avg max Δs, max bias и avg max bias, соответствующие свойствам случайных функций аналогичной размерности.

Заключение. При использовании фиксированных подстановок, полученных на основе модели №1, криптографические свойства двухраундовой миниверсии PRF *pCollapser* близки к свойствам восьмираундовой миниверсии типовой функции на основе SP-сети.

Применение в качестве фиксированных подстановок линейных ARX-функции (на основе модели №2) показало, что миниверсия типовой функции на основе SP-сети не способна обеспечить хоть какой-то уровень нелинейности.

В противовес этому, миниверсия PRF *pCollapser* позволяет получить из набора 4 ARX-функций с предельно низкими криптографическими свойствами, качественную нелинейную функцию, учитывая то, что кроме *fsbox1-fsbox4* другие нелинейные элементы в ней не представлены. Это является неординарным проявлением свойств PRF *pCollapser*, подтверждает правильность концепции псевдодинамических подстановок *PD-sbox* и PRF *pCollapser* в целом, а также требует дополнительных исследований.

Кроме этого, PRF *mini_pCollapser_12x12* обладает рядом существенных преимуществ – в 4 раза меньше количество раундов преобразования и в 4 раза меньше критический путь, что позволяет при том же количестве затрачиваемых ресурсов осуществить программные/аппаратные реализации с кратным увеличением скорости преобразования или с кратным уменьшением задержки преобразования.

Применение ARX-функций с предельно низкими криптографическими свойствами в полновесной PRF *pCollapser* позволит существенно снизить количество затрачиваемых ресурсов как её программной реализации, так и аппаратной.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *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. 88-99. – DOI: 10.23683/2311-3103-2019-5-8.
2. *Raphael Chung-Wei Phan.* Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students // Cryptologia. – XXVI (4). – Swinburne Sarawak Institute of Technology, 2002. – P. 283-306. – URL: https://doi.org/10.1080/0161-110291890948.
3. *Bara Hitapuru, Santi Indarjani.* Square attack on Mini-AES and Simplified AES using all variants of active nibble position // AIP Conference Proceedings, 1729, 020007. – 2016. – URL: https://doi.org/10.1063/1.4946910.
4. *Bizaki H.K., Mansoori S.D. and Falahati A.* Linear Cryptanalysis on Second Round Mini-AES // 2006 2nd International Conference on Information & Communication Technologies. – 2006. – P. 1958-1962. – DOI: 10.1109/ICTTA.2006.1684690.
5. *Asadini Dwi Ajeng Gemellia, Santi Indarjani.* Differential attack on mini-AES // AIP Conference Proceedings. 1450, 222. – 2012. – URL: https://doi.org/10.1063/1.4724144.
6. *Sundari Tianingrum, Santi Indarjani*. Algebraic attack on Mini-AES algorithm // AIP Conference Proceedings. 1729, 020003. – 2016. – URL: https://doi.org/10.1063/1.4946906.
7. *Liu X.* When Mini-AES Meets Machine Learning: Practice and Experience // 2020 IEEE International Symposium on Systems Engineering (ISSE). – 2020. – P. 1-5. – DOI: 10.1109/ISSE49799.2020.9272227.
8. Data Encryption Standard (DES). National Institute of Standards and Technology. – FIPS Publication, 46-3, 1999.
9. *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. – URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2015/5/11.pdf.
10. *Polikarpov S., Rumyantsev K., Petrov D.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions // International Conference on Electrical, Electronics, Materials and Applied Science, AIP Conf. Proc., 1952, eds. V. Rao, A. Ben, S. Bhukya, Amer. Inst. Phys., 2018, UNSP 020091. – DOI: 10.1063/1.5032053.
11. *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. – 7:2. – P. 91-102. – DOI: https://doi.org/10.4213/mvk186.
12. *Biryukov Alex and Léo Perrin.* State of the Art in Lightweight Symmetric Cryptography // IACR Cryptol. ePrint Arch. 2017. – (2017): 511.
13. *Howard M. Heys.* Key Dependency of Differentials: Experiments in the Differential Cryptanalysis of Block Ciphers Using Small S-boxes // Cryptology ePrint Archive, Paper 2020/1349. 2020. – https://eprint.iacr.org/2020/1349.
14. *Nir Y., Langley A.* ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. 2018. – ISSN: 2070-1721.
15. *Biham Eli, Shamir Adi.* Differential Cryptanalysis of DES-like Cryptosystems // J. Cryptology. – 1991. – Vol. 4, No. 1. – P. 3-72. – DOI: http://dx.doi.org/10.1007/BF00630563.
16. *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. – DOI: http://dx.doi.org/10.1007/3-540-48285-7_33.
17. *Zhenzhen Bao and Jian Guo and San Ling and Yu Sasaki*. SoK: Peigen – a Platform for Evaluation, Implementation, and Generation of S-boxes // Cryptology ePrint Archive, Paper 2019/209, 2019.
18. *Adrián Ranea and Vincent Rijmen*. Characteristic Automated Search of Cryptographic Algorithms for Distinguishing Attacks (CASCADA) // Cryptology ePrint Archive, Paper 2022/513, 2022. – DOI: 10.1049/ise2.12077. https://eprint.iacr.org/2022/513
19. *Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, and Olivier Ruatta.* Efficient computation of algebraic immunity for algebraic and fast algebraic attacks // In Proceedings of the 24th annual international conference on The Theory and Applications of Cryptographic Techniques (EUROCRYPT'06). – Springer-Verlag, Berlin, Heidelberg. – P. 147-164. – https://doi.org/10.1007/11761679_10

20. *Eichlseder M. et al.* An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC. In: Moriai, S., Wang, H. (eds) // Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020: Lecture Notes in Computer Science. – Vol. 12491. – Springer, Cham, 2020. – https://doi.org/10.1007/978-3-030-64837-4_16.

REFERENCES

1. *Polikarpov S.V., Kozhevnikov A.A., Rumyantsev K.E., Prudnikov V.A.* Psevdosluchaynaya funktsiya PCOLLAPSER, obespechivayushchaya ekstremal'nyy parallelizm obrabotki informatsii [A pseudo-random PCOLLAPSER function that provides extreme parallelism of information processing], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2019, No. 5 (207), pp. 88-99. DOI: 10.23683/2311-3103-2019-5-8.
2. *Raphael Chung-Wei Phan.* Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students, *Cryptologia,* XXVI (4). Swinburne Sarawak Institute of Technology, 2002, pp. 283-306. Available at: https://doi.org/10.1080/0161-110291890948.
3. *Bara Hitapuru, Santi Indarjani.* Square attack on Mini-AES and Simplified AES using all variants of active nibble position, *AIP Conference Proceedings,* 1729, 020007, 2016. Available at: https://doi.org/10.1063/1.4946910.
4. *Bizaki H.K., Mansoori S.D. and Falahati A.* Linear Cryptanalysis on Second Round Mini-AES, *2006 2nd International Conference on Information & Communication Technologies,* 2006, pp. 1958-1962. DOI: 10.1109/ICTTA.2006.1684690.
5. *Asadini Dwi Ajeng Gemellia, Santi Indarjani.* Differential attack on mini-AES, AIP Conference Proceedings. 1450, 222, 2012. Available at: https://doi.org/10.1063/1.4724144.
6. *Sundari Tianingrum, Santi Indarjani*. Algebraic attack on Mini-AES algorithm, *AIP Conference Proceedings.* 1729, 020003, 2016. Available at: https://doi.org/10.1063/1.4946906.
7. *Liu X.* When Mini-AES Meets Machine Learning: Practice and Experience, *2020 IEEE International Symposium on Systems Engineering (ISSE),* 2020, pp. 1-5. DOI: 10.1109/ISSE49799.2020.9272227.
8. Data Encryption Standard (DES). National Institute of Standards and Technology. FIPS Publication, 46-3, 1999.
9. *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. Available at: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2015/5/11.pdf.
10. *Polikarpov S., Rumyantsev K., Petrov D.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions, *International Conference on Electrical, Electronics, Materials and Applied Science, AIP Conf. Proc., 1952*, eds. V. Rao, A. Ben, S. Bhukya, Amer. Inst. Phys., 2018, UNSP 020091. DOI: 10.1063/1.5032053.
11. *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 Issues of Cryptography], 2016, 7:2, pp. 91-102. DOI: https://doi.org/10.4213/mvk186.
12. *Biryukov Alex and Léo Perrin.* State of the Art in Lightweight Symmetric Cryptography, *IACR Cryptol. ePrint Arch*., 2017. (2017): 511.
13. *Howard M. Heys.* Key Dependency of Differentials: Experiments in the Differential Cryptanalysis of Block Ciphers Using Small S-boxes, *Cryptology ePrint Archive, Paper 2020/1349*. 2020. Available at: https://eprint.iacr.org/2020/1349.
14. *Nir Y., Langley A.* ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. 2018. ISSN: 2070-1721.
15. *Biham Eli, Shamir Adi.* Differential Cryptanalysis of DES-like Cryptosystems, *J. Cryptology,* 1991, Vol. 4, No. 1, pp. 3-72. DOI: http://dx.doi.org/10.1007/BF00630563.
16. *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. DOI: http://dx.doi.org/10.1007/3-540-48285-7_33.

17. *Zhenzhen Bao and Jian Guo and San Ling and Yu Sasaki*. SoK: Peigen – a Platform for Evaluation, Implementation, and Generation of S-boxes, *Cryptology ePrint Archive, Paper 2019/209*, 2019.
18. *Adrián Ranea and Vincent Rijmen*. Characteristic Automated Search of Cryptographic Algorithms for Distinguishing Attacks (CASCADA), *Cryptology ePrint Archive, Paper 2022/513,* 2022. DOI: 10.1049/ise2.12077. https://eprint.iacr.org/2022/513
19. *Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, and Olivier Ruatta.* Efficient computation of algebraic immunity for algebraic and fast algebraic attacks, *In Proceedings of the 24th annual international conference on The Theory and Applications of Cryptographic Techniques (EUROCRYPT'06)*. Springer-Verlag, Berlin, Heidelberg, pp. 147-164. Available at: https://doi.org/10.1007/11761679_10
20. *Eichlseder M. et al.* An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC. In: Moriai, S., Wang, H. (eds), *Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020: Lecture Notes in Computer Science*, Vol. 12491. Springer, Cham, 2020. Available at: https://doi.org/10.1007/978-3-030-64837-4_16.

Статью рекомендовал к опубликованию д.т.н., профессор А.В. Боженюк.

Поликарпов Сергей Витальевич – Южный федеральный университет; e-mail: polikarpovsv@sfedu.ru; г. Таганрог, Россия; 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 Vital'evich – Southern Federal University; e-mail: polikarpovsv@sfedu.ru; Taganrog, Russia; phone: +79085159762; cand. of eng. sc.

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

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

УДК 681.3:519.2 DOI 10.18522/2311-3103-2022-6-162-171

В.П. Федосов, А.И. Приходченко

РАНГОВАЯ ОБРАБОТКА СИГНАЛОВ ДАТЧИКА ВИБРАЦИЙ ДЛЯ СИГНАЛИЗАЦИИ ПРИВОДНЕНИЯ САМОЛЕТА-АМФИБИИ В УСЛОВИЯХ АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ

*Цель работы – использование ранговой модели обработки сигналов для сигнализации приводнения самолета-амфибии**.** Ранговая обработка относится к непараметрическим методам обнаружения сигнала на фоне помех. Непараметрические методы используются, если неизвестен функциональный вид распределения входных данных и указаны только самые общие различия между наличием и отсутствием сигнала. Практически все непараметрические обнаружители содержат в качестве составного элемента устройства, осуществляющие некоторое инвариантное преобразование S массива выборочных значений X. В результате этого преобразования образуется новый массив $Z = SX$, распределение элементов которого при отсутствии сигнала точно известно. Преобразование S, которое выбирается эвристически, позволяет свести задачу обнаружения сигнала на фоне помех с неизвестным распределением к задаче проверки простой гипотезы относительно распределения массива Z. Задачи исследования: 1) предварительная цифровая фильтрация записей полетов самолета-амфибии для применения ранговой обработки; 2) проведение эксперимента для получения характеристик рангового обнаружителя, используемого для сигнализации приводнения самолета-амфибии; 3) анализ полученных результатов. Предложена модель обработки сигналов датчика вибраций для сигнализации приводнения самолета-*