АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К СИНТЕЗУ ПСЕВДО-ДИНАМИЧЕСКИХ SBOX

Прудников В. А.[1]

DOI: 10.21681/2311-3456-2024-4-57-64

Целью исследования *является анализ существующих на текущий момент подходов к синтезу псевдо-динамических sbox, для подтверждения актуальности проблемы синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих требований.*

Методы исследования: *анализ и систематизация существующих подходов к синтезу криптографических операций sbox и псевдо-динамических sbox.*

Результатом исследования является вывод о том, что на текущий момент проблема синтеза sbox, как основного нелинейного элемента современных блочных шифров и псевдослучайных функций, удовлетворяющих взаимоисключающим требованиям, является актуальной. Существует ряд способов решения обозначенной проблемы, подразумевающих подбор sbox в соответствии с требованиями, реализация нелинейного элемента псевдослучайной функции или криптоалгоритма в качестве ARX-функции, применение динамических sbox и синтез псевдо-динамических sbox, в основе которых могут быть как фиксированные нелинейные элементы, так и ARX-конструкции. К операциям sbox, вне зависимости от их вида, предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость псевдослучайных функций, перестановок и криптоалгоритмов. Следовательно, проблема синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих параметров является базовой. Синтез псевдо-динамических операций sbox на основе специально подобранных ARX-функций, обладающих разностными и линейными свойствами эквивалентных sbox, аналогичным случайно сформированным фиксированным нелинейным элементам той же размерности, в псевдослучайных функциях семейства pCollapser, потенциально позволяет обеспечить оптимальное использование векторных инструкций процессора и параллелизм обработки информации.

Практическая значимость *заключается в обосновании актуальности применения нового подхода к синтезу перспективного криптографического преобразования – псевдо-динамического sbox, удовлетворяющего широкому спектру взаимоисключающих требований, для задач криптографической защиты информации.*

Ключевые слова: *криптография, криптографические примитивы, sbox, псевдо-динамические sbox, ARX-функции, псевдослучайные функции.*

ANALYSIS OF EXISTING APPROACHES TO THE SYNTHESIS OF PSEUDO-DYNAMIC SBOX

Prudnikov V. A.[2]

The purpose of the research *is to analyze currently existing approaches to the synthesis of pseudo-dynamic substitution operations, to confirm the relevance of the problem of synthesizing substitution operations that satisfy a wide range of mutually exclusive requirements.*

Research methods: *analysis and systematization of existing approaches to the synthesis of cryptographic operations sbox and pseudo-dynamic sbox.*

The result of the research *is the conclusion that at the moment the problem of synthesizing substitution operations as the main nonlinear element of modern block ciphers and pseudo-random functions that satisfy mutually exclusive requirements is relevant. There are a number of ways to solve this problem, implying the selection of substitution operations in accordance with the requirements, the implementation of a nonlinear element of a pseudo-random function or a cryptoalgorithm as an ARX function, the use of dynamic substitutions in ciphers and the synthesis of pseudo-dynamic substitutions, which can be based on either fixed substitution operations, and ARX-constructions. Substitution operations, regardless of their type, are subject to about a dozen requirements that directly affect the cryptographic strength of pseudorandom functions, permutations and cryptoalgorithms. Consequently, the problem of synthesizing replacements that satisfy a wide range of mutually exclusive parameters is basic. Synthesis of pseudo-dynamic substitution operations*

1 Прудников Вадим Александрович, ассистент кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет», Таганрог, Россия. E-mail: prudnikov@sfedu.ru. ORCHID: 0000-0002-5011-727X.

2 Vadim A. Prudnikov, Assistant Professor, Department of Information Security of Telecommunication Systems, Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog, Russia. E-mail: prudnikov@sfedu.ru. ORCHID: 0000-0002-5011-727X.

based on specially selected ARX functions that have differential and linear properties of equivalent substitutions, similar to randomly fixed substitution operations of the same dimension, in pseudo-random functions of the pCollapser family, potentially allows for optimal use of processor vector instructions and parallelism of information processing.

***The practical significance** lies in substantiating the relevance of using a new approach to the synthesis of a promising cryptographic transformation - pseudo-dynamic sbox, satisfying a wide range of mutually exclusive requirements for problems of cryptographic information protection.*

***Keywords:** cryptography, cryptographic primitives, sbox, pseudo-dynamic sbox, ARX functions, pseudo-random functions.*

Введение

Блок криптографической подстановки (sbox) – это нелинейный элемент, осуществляющий отображение n-битного сообщения на входе в m-битное сообщение на выходе. Sbox обладают множеством криптографических свойств: нелинейность; разностные характеристики; сбалансированность; корреляционный иммунитет; глобальный лавинный критерий; алгебраический иммунитет; критерий распространения; порядок прозрачности.

Обозначенные параметры криптографического элемента sbox оказывают ключевое влияние на устойчивость криптоалгоритмов и псевдослучайных функций (PRF) к различным методам криптоанализа.

Криптографические операции sbox являются основным нелинейным элементом множества современных блочных шифров и псевдослучайных функций. Их устойчивость к различным методам криптоанализа напрямую зависит от типа и качества используемых операций sbox.

Одной из основных задач рассматриваемого нелинейного элемента является обеспечение устойчивости к статистическим методам криптоанализа, в частности к линейному и разностному. Подбор операций sbox для криптоалгоритмов или псевдослучайных функций не является тривиальной задачей, основная проблема – анализ множества синтезируемых нелинейных элементов для отбора структур, соответствующих взаимоисключающим критериям, которые определяют sbox, максимально приближенный к идеальному. При генерации нелинейного элемента необходимо соблюдать множество жестких требований для обеспечения стойкости к статистическим атакам. Синтез криптоустойчивых sbox необходим как для разрабатываемых алгоритмов, так и для использующихся в настоящее время.

Проблема синтеза операций sbox, удовлетворяющих широкому спектру взаимоисключающих требований по устойчивости к различным методам криптоанализа и потреблению как программных, так и аппаратных ресурсов, является актуальной и ей уделяется значительное внимание.

Существует множество подходов решения проблемы синтеза sbox. Большинство из них заключается в применении различных методик при генерации фиксированных нелинейных элементов, обладающих требуемыми криптографическими свойствами. Иным способом решения задачи является применение конструкций, потенциально способных заменить операции sbox в шифрах и псевдослучайных функциях, к ним относятся ARX-конструкции (структуры, включающие в свой состав операции сложения по модулю слова, циклического сдвига и XOR), динамические sbox, позволяющие потенциально нивелировать возможность применения статистических атак на криптоалгоритм, псевдо-динамические sbox, включающие в свой состав либо фиксированные sbox, либо специально подобранные ARX-функции, и позволяющие объединить преимущества как классических sbox, так и динамических, что даёт ряд преимуществ при их аппаратной и программной реализации в составе псевдослучайных функций.

Анализ существующих подходов к синтезу нелинейного элемента sbox

Проанализируем первый вариант решения проблемы – синтез криптографических операций sbox с использованием различных алгоритмов, позволяющих получить элемент, обладающий криптографическими свойствами, приближенными к идеальным.

В работе[3] описан реверсивный генетический алгоритм, использование которого позволяет быстро генерировать большое число стойких биективных sbox размерностью от 8 бит до 16, которые имеют неоптимальные свойства и более сложную алгебраическую структуру, а также не обладают линейной избыточностью. В статье[4] представлен метод генерации sbox размерностью 8 бит с нелинейностью, достигающей значения 104. Метод комбинирует специальный генетический алгоритм с полным деревом поиска. В исследовании[5] представлен метод генерации нелинейных sbox на основе градиентного спуска. Приведены критерии отбора операций sbox для криптографических симметричных примитивов,

3 Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. – 2016. – Vol. 8. – P. 247–276. – DOI: 10.1007/s12095-015-0170-5. – URL: https://doi.org/10.1007/s12095-015-0170-5

4 Tesař P. A new method for generating high non-linearity s-boxes // Radioengineering. – 2010. – Vol. 19, no. 1. – P. 23–26. – URL: https://www.radioeng.cz/fulltexts/2010/10_01_023_026.pdf

5 Kazymyrov O., Kazymyrova V., Oliynykov R. A method for generation of high-nonlinear s-boxes based on gradient descent // IACR Cryptology ePrint Archive (2013). – 2014. – URL: http://eprint.iacr.org/2013/578

основанных на анализе свойств векторных булевых функций. Предлагается усовершенствованный метод градиентного спуска для увеличения эффективности генерации нелинейных векторных булевых функций с оптимальными криптографическими показателями. Использование предложенного метода для наиболее часто применяемых sbox, размерностью 8 бит, позволяет добиться показателей нелинейности 104. Авторами работы[6] предлагается подход к генерации операций sbox, основанный на применении четвертичных последовательностей де Брейна, позволяющих добиться значительного увеличения числа доступных экономичных sbox по сравнению с использованием двоичных последовательностей де Брейна. Исследования в [1] посвящены разработке новой реализации криптоалгоритма AES, включающего в свой состав HPAC-SBOX (Hybrid Prediction and Adaptive Chaos – гибридное прогнозирование и адаптивный хаос), который объединяет алгоритмы обучения с прогнозированием и адаптивные хаотические логистические операции sbox. В [2] сравнивается эффективность подходов к генерации операций sbox в соответствии с их значениями нелинейности. Рассмотрены преимущества и недостатки представленных подходов. В [3] представлена разработка алгоритма генерации sbox с использованием генетического алгоритма. В алгоритме генерации обработано значение нелинейности, которое является одним из наиболее важных критериев оценки операций sbox. Качество сгенерированных блоков sbox определено с помощью тестов производительности. В [4] предлагается алгоритм генерации операций sbox, основанный на 4D гиперхаотической системе и улучшенной оптимизации роя частиц. Улучшена хаотическая система Лоренца и предложена 4D гиперхаотическая система с более высоким показателем Ляпунова и более сложной динамикой. Идея алгоритма имитационного отжига введена в алгоритм оптимизации роя частиц, что еще больше повышает эффективность алгоритма оптимизации и устраняет проблему, заключающуюся в том, что алгоритм оптимизации роя частиц легко поддается локальному оптимальному решению. Алгоритм использован для оптимизации нелинейности блоков sbox и повышения их производительности. В [5] представлена новая разновидность стохастического алгоритма генерации sbox, суть которого заключается в постепенном построении вектора значений булевой функции. Поиск новых значений выполняется случайным образом, основанном на ограничениях на дифференциальный спектр генерируемого sbox. В [6] представлен новый подход к генерации sbox, устойчивых к атакам по анализу мощности. На предварительном этапе создаётся sbox с базовыми криптографическими свойствами. Затем, на основе полученного sbox осуществляется генерация новых, с использованием генетического алгоритма на определенном подмножестве набора линейных комбинаций координатных функций исходного sbox. Работа [7] посвящена новому генетическому алгоритму, предназначенному для улучшения свойств sbox, созданных структурой Фейстеля. Однородность бумеранга определяет устойчивость блочных шифров к атакам бумеранга и является одним из параметров sbox. Стоит отметить, что операции sbox, созданные структурой Фейстеля, обладают недостаточной однородностью бумеранга. Авторами предложен новый генетический алгоритм для улучшения свойств подобных sbox, позволяющий генерировать несколько биективных sbox размерностью 8 бит с дифференциальной однородностью 6, нелинейностью 108 и однородностью бумеранга 10. В [8] представлен новый метод генерации криптостойких sbox размерностью 8 бит, путём применения матрицы смежности к полю Галуа GF(28).

Указанные подходы не удовлетворяют всем взаимоисключающим требованиям. В частности, размерность сгенерированной sbox может не позволить эффективно применять её в программной или аппаратной реализации в силу потребления большого объёма ресурсов.

Иной способ решения заключается в применении в качестве фиксированных sbox ARX-функций. В работе[7] представлено семейство поточных шифров Salsa20, основанное на ARX-операциях. Классическая версия криптоалгоритма включает 20 раундов преобразований и три вида операций над 32-битными словами: сложение по модулю 2^{32}, операция XOR, циклический сдвиг. Salsa20 расширяет 256-битный ключ и 64-битный nonce (уникальный номер сообщения) в 270-байтовый поток. Он шифрует b-байтовый открытый текст, объединяя открытый текст с первыми b байтами потока и отбрасывая остальную часть потока. Операция дешифрования осуществляется выполнением операции XOR над зашифрованным текстом с первыми b байтами потока. В алгоритме отсутствует обратная связь от открытого или зашифрованного текста к потоку. Salsa20 генерирует поток блоками по 64 байта (512 бит). Каждый блок включает независимый хэш ключа, nonce и 64-битный номер блока, отсутствует сцепление предыдущего блока с последующим. Поток на выходе криптоалгоритма может быть доступен случайным образом, и любое количество блоков может быть вычислено

6 Соколов А. В., Мазурков М. И. Методы синтеза четверичных последовательностей де Брейна для задач криптографии // Решетневские чтения. 2012. №16. URL: https://cyberleninka.ru/article/n/metody-sinteza-chetverichnyh-posledovatelnostey-de-breyna-dlya-zadach-kriptografii

7 Bernstein, D. J. (2008). The Salsa20 Family of Stream Ciphers. In: Robshaw, M., Billet, O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol 4986. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-68351-3_8.

параллельно. В Salsa20 нет предварительной обработки. В исследовании[8] представлены результаты криптоанализа над семейством поточных шифров Salsa20. Авторам удалось достичь сложности поиска ключа в $2^{247,2}$ при осуществлении анализа 8-раундовой реализации, что значительно превосходит результаты прошлых лет в 2^{251} и 2^{250}. Работа [9] посвящена новому методу поиска линейных аппроксимаций криптоалгоритмов на основе ARX-конструкций, в частности шифра ChaCha. Авторами демонстрируется получение линейных аппроксимаций для 3 и 4 раундов ChaCha. В [10] представлены улучшения в системе дифференциально-линейных атак, предназначенных для шифров на базе ARX-операций. Для демонстрации результатов работы применены к криптоалгоритмам Chaskey и ChaCha. В работе[9] представлены шифры Simon и Speck – легковесные блочные криптоалгоритмы, предназначенные для интернета вещей. Максимальный размер блока составляет 128 бит, максимальный размер ключа – 256 бит. Блок состоит из двух слов, при этом слово может иметь размер 16, 24, 32, 48 или 64 бит. Ключ обладает размерностью в 2, 3 или 4 слова. Раундовая функция включает в себя операции: циклического сдвига первого слова вправо на 8 бит, сложение второго слова с первым по модулю 2 в степени длины слова, операция XOR ключа и результата сложения, циклический сдвиг второго слова влево на 3 бита, операция XOR второго слова и результата предыдущего XOR. Количество раундов зависит от выбранных размеров слова и ключа, для максимальных размеров блока и ключа количество раундов равно 34, при минимальных значениях – 22. В статье[10] продемонстрированы результаты разностного криптоанализа над описанными шифрами. В [11] представлен новый блочный шифр на базе ARX-конструкций и MDS-матрицы на основе концепции белого ящика – WARX. В [12] представлена 64-битная операция sbox Alzette, основой которой являются ARX-функции. Особенностью преобразования является то, что оно вычисляется на современных процессорах за фиксированное время и использует всего 12 инструкций. Параллельная реализация Alzette может использовать векторные (SIMD) инструкции. Одна итерация обладает разностными и линейными характеристиками, сравнимыми со свойствами операции sbox алгоритма AES, две последующие итерации обеспечивают тот же уровень устойчивости, что и супер-sbox AES. Alzette используется для построения малоресурсного 64-битного блочного криптоалгоритма Crax, превосходящего SPECK-64/128 на коротких сообщениях на микроконтроллерах, а также 256-битного блочного шифра Trax.

Минусом подхода, подразумевающего использование ARX-операций являются, как правило, неудовлетворительные криптографические свойства создаваемых конструкций, однако, они позволяют добиться высокого быстродействия и малого потребления ресурсов при программной и аппаратной реализации.

Для противодействия статистическим методам криптоанализа неоднократно осуществлялись попытки применять вместо фиксированных sbox динамически изменяемые.

Наиболее успешной попыткой применения динамически изменяемой sbox можно назвать криптоалгоритм RC4, который считается устаревшим и ненадёжным. Основная проблема стойкости RC4 – применение всего одной динамически изменяемой sbox и медленное обновление содержимого (за одну итерацию обновляется 2 ячейки из 256)[11]. Проблема предопределена тем, что динамические операции sbox (в сравнении с фиксированными sbox) требуют на порядки больше вычислительных ресурсов.

Применение псевдо-динамических sbox (PD-sbox) на базе фиксированных нелинейных элементов потенциально позволяет решить ряд описанных выше проблем, в частности, обеспечить устойчивость к статистическим методам криптоанализа.

Описание структуры псевдо-динамической операции PD-sbox

Псевдо-динамический sbox – нелинейный элемент (функция), объединяющий свойства фиксированных (высокая скорость преобразования, эффективное использование вычислительных ресурсов) и динамических (нейтрализация статистических методов криптоанализа) операций sbox[12].

Структура псевдо-динамической операции PD-sbox включает в свой состав фиксированные sbox. Аргумент каждой фиксированной операции sbox параметризован значением состояния S_i, где i – номер фиксированной sbox (от 0 до N–1).

Текущее значение состояния $S = \{S_0, S_1, S_2, \ldots, S_{N-1}\}$ задаёт эквивалентный sbox из множества возможных, порождаемых PD-sbox. Число формируемых

8 Maitra, Subhamoy et al. «Salsa20 Cryptanalysis: New Moves and Revisiting Old Styles.» IACR Cryptol. ePrint Arch. 2015 (2015): 217. – URL: https://www.semanticscholar.org/paper/Salsa20-Cryptanalysis%3A-New-Moves-and-Revisiting-Old-Maitra-Paul/8deb80ff7f9cc16a7dd05388927b4a29f1706f62

9 Beaulieu, Ray et al. “SIMON and SPECK: Block Ciphers for the Internet of Things.” IACR Cryptol. ePrint Arch. 2015 (2015): 585. – URL: https://www.semanticscholar.org/paper/SIMON-and-SPECK%3A-Block-Ciphers-for-the-Internet-of-Beaulieu-Shors/06f11891201b321294ffff9d91e3682acb160be6

10 Abed F., List E., Lucks S., Wenzel J. Cryptanalysis of the Speck Family of Block Ciphers. Cryptology ePrint Archive, Paper 2013/568. – 2013. – URL: https://eprint.iacr.org/2013/568

11 Klein A. Attacks on the RC4 stream cipher // Designs, codes and cryptography. – 2008. – Vol. 48, no. 3. – P. 269–286. – DOI: 10.1007/s10623-008-9206-6.

12 Поликарпов С. В., Кожевников А. А. Псевдо-динамические sbox: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – Т. 169, № 8. – С. 19–31. – URL: http://old.izv- tn.tti.sfedu.ru/wp-content/uploads/2015/8/2.pdf.

эквивалентных sbox определено набором возможных значений состояния S, которые могут динамически изменяться в процессе обработки блоков информации, что приведет равномерному распределению вероятностных свойств между порождаемыми sbox.

Структура псевдо-динамической sbox представлена на (рис.1).

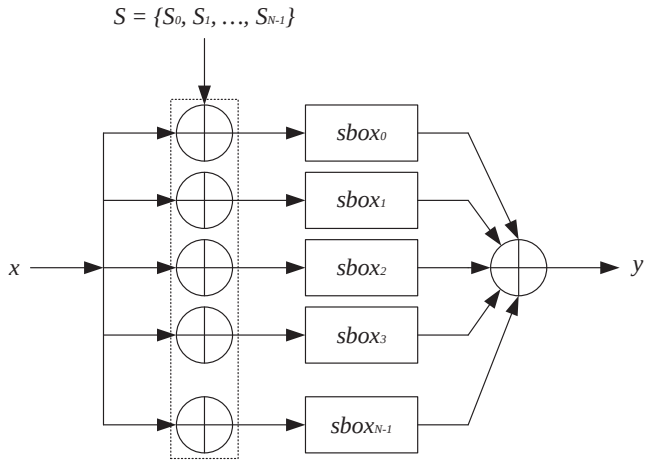

Рис. 1. Структура PD-sbox

Ниже представлено выражение, описывающее структуру псевдо-динамической операции PD-sbox:

$$Y = \oplus_{i=0}^{N-1} \text{sbox}_i (X \oplus S_i), \quad (1)$$

где sbox – фиксированная операция sbox; N – количество фиксированных подстановок; X – биты входного сообщения; Y – биты выходного сообщения; S – биты значения состояния псевдо-динамической sbox; $\oplus$ – операция сложения по модулю 2.

Входное значение каждой фиксированной sbox задаётся индивидуальным значением состояния S_i, где i – номер фиксированной sbox (от 0 до N–1). Текущее значение состояния $S = \{S_0, S_1, S_2, \ldots, S_{N-1}\}$ задаёт одну эквивалентную операцию sbox из всего множества возможных замен псевдо-динамической sbox. На (рис.2) представлена псевдо-динамическая операция sbox в виде набора эквивалентных замен[12].

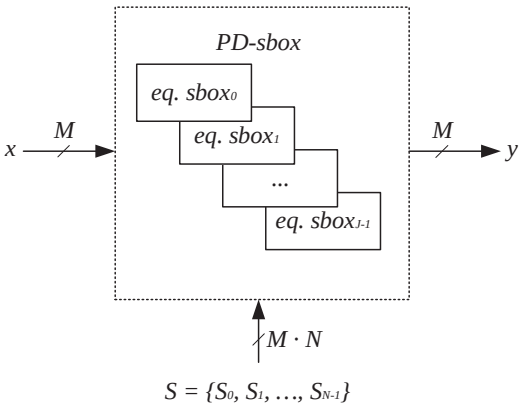

Рис.2. Псевдо-динамическая операция sbox в виде набора эквивалентных нелинейных элементов

Псевдо-динамическая операция sbox способна функционировать в двух режимах: статическом (ключезависимом) и динамическом (выходное значение зависит не только от ключа, но и от промежуточных состояний).

Статический режим работы подразумевает, что значение внутреннего состояния равно нулю или константе. При динамическом режиме работы наблюдается равновероятное изменение значений внутреннего состояния S и в таком случае дифференциальные усреднённые свойства, а также линейные, близки к идеальным (при усреднении характеристик по всем эквивалентным операциям sbox). Данная особенность потенциально позволяет нейтрализовать существующие методы дифференциального и линейного криптоанализа [13].

Анализ свойств псевдо-динамических подстановок

Исследование свойств PD-sbox представлено в следующих трудах.[13]

В работе предложена концепция применения перспективного криптографического примитива – PD-sbox, объединяющих в себе свойства фиксированных sbox (высокая скорость преобразования блока информации и эффективность использования вычислительных ресурсов) и динамических sbox (нейтрализация статистических методов криптоанализа). В работе представлены результаты предварительного криптографического анализа линейных и дифференциальных свойств PD-sbox, которые демонстрируют неэффективность аппроксимации нелинейного элемента набором линейных статистических аналогов, и существенное улучшение разностных свойств криптографического примитива при последовательном увеличении количества фиксированных sbox.

Цель исследования[14] заключалась в разработке методики определения линейных характеристик псевдо-динамических sbox для оценки возможности их применения в блочных криптоалгоритмах. В рамках исследования получены выражения, позволяющие определить линейные свойства PD-sbox. Первичный анализ выражения позволил сделать вывод, что сама структура псевдо-динамической sbox существенно усложняет определение её линейных свойств и препятствует линейному криптоанализу.

Целью в работе[15] являлся анализ линейных характеристик псевдо-динамических операций sbox

13 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Псевдо-динамические таблицы sbox: 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.

14 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Исследование линейных характеристик псевдо-динамических подстановок // Известия ЮФУ. Технические науки. – 2015. – Т. 166, № 5. – С. 111–123. – URL:http ://old.izv-tn.tti.sfedu.ru/wp-content/uploads/2015/5/11.pdf.

15 Поликарпов С. В., Кожевников А. А. Псевдо-динамические sbox: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – Т. 169, № 8. – С. 19–31. – URL: http://old.izv- tn.tti.sfedu.ru/wp-content/uploads/2015/8/2.pdf.

на основе экстраполяции линейных свойств, случайно сформированных малоразмерных PD-sbox. Определение усреднённых значений максимумов смещения позволило упростить анализ полученных результатов и найти закономерность между параметрами псевдо-динамических sbox и вероятностью достижения максимальных значений смещения случайно сформированных PD-sbox. Выявленная закономерность позволила приблизительно экстраполировать линейные свойства малоразмерных псевдо-динамических sbox на линейные свойства полноразмерных PD-sbox.

Исследованию разностных характеристик PD-sbox посвящена работа[16]. Анализ полученных данных показывает, что поочерёдное добавление в состав PD-sbox фиксированных sbox уменьшает вдвое максимальное значение центрированного коэффициента распространения разностных свойств. В свою очередь, распределение отклонений центрированного коэффициента распространения дифференциалов приближается к гауссовому распределению.

В исследовании[17] представлены результаты первоначального анализа псевдо-динамических sbox, имеющих идеальное распределение разностных свойств, при усреднении всех возможных генерируемых sbox в статическом режиме работы (при фиксированных значениях состояния). Доказано существование класса PD-sbox, имеющих идеально усредненное распределение разностных свойств в статическом режиме работы. В [14] представлены первые результаты по исследованию нелинейных свойств эквивалентных sbox, формируемых PD-sbox, состоящими из фиксированных операций sbox размерностью 4 бит. Распределение значений нелинейности для эквивалентных sbox существенно отличается от распределения значений нелинейности фиксированных sbox. Примерно 30 полученных PD-sbox формируют эквивалентные с нелинейностью больше нуля. Путём подбора составляющих PD-sbox можно добиться того, что эквивалентные sbox всегда будут нелинейными.

Развитием структуры псевдо-динамической операции sbox является применение ARX-функций в их составе [15]. Идея заключалась в том, что объединение слабых, с криптографической точки зрения, конструкций, включающих операции сложения по модулю, циклического сдвига и XOR, позволит получить эквивалентные операции sbox, обладающие характеристиками, не уступающим случайно сгенерированным операциям sbox аналогичной размерности. При этом, полученная структура обладает возможностью параллелизма при её использовании в семействе псевдослучайных функций pCollapser. Одним из основных преимуществ этого подхода является сохранение криптографической устойчивости, при значительном сокращении затрачиваемых ресурсов при программной реализации, а также потенциальное увеличение скорости работы функции, в силу использования более простых операций, в отличие от sbox. В свою очередь, применение подобранных ARX-функций для использования в структуре PD-sbox псевдослучайной функции pCollapser позволяет получить вес разностных и линейных характеристик, превосходящий аналоги, при тех же затратах ресурсов при программной реализации.

Описание структуры псевдо-динамической операции PD-sbox на основе ARX-конструкций (PD-sbox-ARX)

Развитием PD-sbox является применение в их составе специально подобранных ARX-функций вместо фиксированных sbox, несмотря на неудовлетворительные криптографические характеристики ARX-конструкций. Использование ARX-функций, в качестве основного нелинейного элемента псевдо-динамической sbox, позволяет существенно уменьшить затраты ресурсов при программной реализации и получить криптографические свойства PD-sbox, аналогичные, использующим фиксированные sbox той же размерности.

В [15] предложен вариант применения специально подобранных ARX-функций в составе псевдо-динамических операций sbox, для последующего их использования в псевдослучайной функции pCollapser, что позволяет обеспечить как параллелизм обработки информации, так и стойкость к статистическим методам криптоанализа и возможность эффективной программной реализации. Основное назначение синтезированной псевдослучайной функции – применение в качестве высокопроизводительной PRF, в режимах, не требующих наличия возможности обратного преобразования, например: AEAD, CTR, Sponge-конструкции.

Структура используемых ARX-функций приведена на (рис.3). Выбор подобной архитектуры функции обусловлен обеспечением криптографических свойств и оптимальным использованием возможностей современных процессоров и аппаратных платформ.

PD-sbox-ARX состоит из четырёх параллельно включённых в её структуру ARX-функций. Размерность входа-выхода PD-sbox соответствует размерности используемых ARX-конструкций.

16 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Псевдо-динамические таблицы sbox: исследование дифференциальных характеристик // Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках. – М., 2014. – С. 77–89.

17 Polikarpov S., Petrov D., Kozhevnikov A. On a class pseudo-dynamic substitutions PD-sbox, with a perfect distribution of averaged differentials in static mode of work // 2017 International Conference on Cryptography, Security and Privacy. – Wuhan, 2017. – P. 17–21. – (ICCSP 2017).

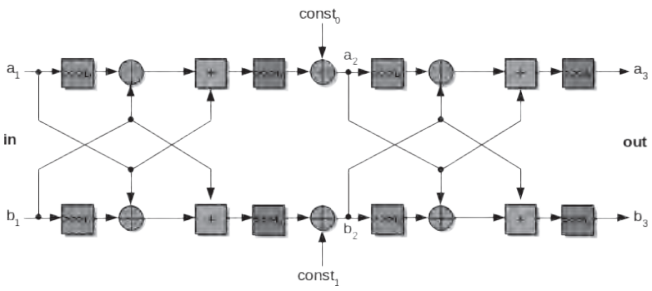

Рис. 3. Структура используемых ARX-функций

На (рис.4) представлена псевдо-динамическая sbox, включающая в свой состав четыре параллельно интегрированных ARX-функции. Размерность входа-выхода PD-sbox соответствует размерности используемых ARX-конструкций.

Выражение, описывающее значение на выходе:

$$c_i = \bigoplus_{j=0}^{3} funcARX_j\,(m_i \oplus s_j^i), \qquad (2)$$

где: i – индекс n-битного слова из входного/выходного вектора и далее индекс PD-sbox; j – индекс компонента PD-sbox ; m_i – n-битные слова из входного вектора; c_i – n-битные слова из выходного вектора; $funcARX$ – ARX-функция (компоненты PD-sbox); s_j^i – n-битные слова из входного вектора управляющего состояния (индивидуальные для каждого PD-sbox) [15].

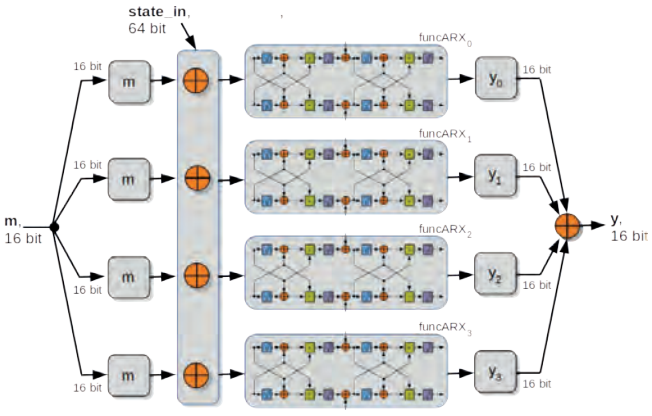

Рис. 4. Псевдо-динамическая операция sbox на основе ARX-конструкций

Выражение, описывающее индивидуальные управляющие состояния на выходе PD-sbox:

$$g_n^i = c_i \oplus funcARX_j\,(m_i \oplus s_j^i) = \bigoplus_{n=0,n\neq i}^{3} funcARX_j\,(m_i \oplus s_j^i). \qquad (3)$$

PD-sbox-ARX – перспективное направление развития концепции псевдо-динамических sbox, позволяющее наглядно продемонстрировать возможность достижения криптографических характеристик эквивалентных sbox, не уступающих случайно сформированным нелинейным элементам той же размерности, а также возможность нейтрализации статистических атак при динамическом режиме работы как на сам криптографический примитив, так и на PRF или криптоалгоритм, в которых он может быть применён. Особенностью этой концепции является возможность эффективной программной реализации, которая заключается в оптимальном использовании вычислительных возможностей современных процессоров (AVX-инструкции (Advanced Vector Extensions) и параллельная обработка).

Выводы

В ходе исследования проанализированы существующие подходы к синтезу PD-sbox, а также классических sbox и их вариаций. Стоит отметить, что на текущий момент проблема синтеза sbox как основного нелинейного элемента современных блочных шифров и псевдослучайных функций, удовлетворяющих взаимоисключающим требованиям, является актуальной. Существует ряд способов решения этой проблемы, подразумевающих подбор операций sbox в соответствии с требованиями, реализация нелинейного элемента псевдослучайной функции или криптоалгоритма в качестве ARX-функции, применение динамических sbox в шифрах и синтез PD-sbox, в основе которых могут быть как фиксированные операции sbox, так и ARX-конструкции. К операциям sbox, вне зависимости от их вида, предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость псевдослучайных функций, перестановок и криптоалгоритмов. Следовательно, проблема синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих параметров является базовой.

Представлено описание структуры PD-sbox, а также принцип её работы. Конструкция позволяет обеспечить параллелизм обработки информации при её использовании в составе псевдослучайных функций, псевдослучайных перестановок и криптоалгоритмов, а также потенциально способна нейтрализовать существующие методы разностного и линейного криптоанализа.

Применение псевдо-динамических sbox на базе подобранных ARX-функций, обладающих разностными и линейными свойствами эквивалентных sbox, аналогичным случайно фиксированным нелинейным элементам той же размерности, в псевдослучайных функциях семейства pCollapser потенциально позволяет обеспечить оптимальное использование векторных инструкций процессора и параллелизм обработки информации. Из этого следует сделать вывод о том, что данный подход к синтезу PD-sbox является перспективным и требует проведения дополнительных исследований, посвящённых криптографическому анализу свойств нелинейного элемента, а также исследований их программной и аппаратной реализации, как в формате криптографического примитива, так и в составе псевдослучайных функций семейства pCollapser.

Литература

1. *Sankaralingam, A., Vivek, U. HPAC-sbox a novel implementation of predictive learning classifier and adaptive chaotic s-box for counterfeiting sidechannel attacks in an IOT networks // Microprocessors and Microsystems. 81. 103737. – 2021. DOI: 10.1016/j.micpro.2020.103737.*
2. *Artuğer, F., Karakuş, S., Özkaynak, F. Comparison of Nonlinearity Value of Substitution Box Generation Approaches // International Conference on Recent Academic Studies. – 2023. – Vol.1. – P. 46–49. DOI: 10.59287/icras.670.*
3. *Kökçam, A., Çavuşoğlu, Ü. A new approach to design S-box generation algorithm based on genetic algorithm // International Journal of Bio-Inspired Computation. 2021.– 2021. – Vol.17, No.1. – P. 52–62. DOI: 10.1504/IJBIC.2021.10035835.*
4. *Yang, S., Tong, X.,Wang, Z. S-box generation algorithm based on hyperchaotic system and its application in image encryption // Multimedia Tools and Applications. – 2023. – Vol.82.– P. 25559–25583. DOI: 10.1007/s11042-023-14394-1.*
5. *Marochok, S., Zajac, P. Algorithm for Generating S-Boxes with Prescribed Differential Properties // Algorithms. – 2023. – Vol.16. Issue 3. DOI: 10.3390/a16030157.*
6. *Khadem, B., Rajavzadeh, S. Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions // Journal of Electrical and Computer Engineering Innovations (JECEI). – 2022. – Vol.10, No.1. – P. 143–152. DOI: 10.22061/jecei.2021.7801.436.*
7. *Kang, M., Wang, M. New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity // IEEE Access. – 2022. – Vol.10. – P. 10898–10906. DOI: 10.1109/ACCESS.2022.3144458.*
8. *Siddiqui, N., Yousaf, F., Murtaza, F. et al. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field // PLoS ONE. – 2020. – Vol.15(11). DOI: 10.1371/journal.pone.0241890.*
9. *Coutinho, M., Neto, T. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha // Advances in Cryptology – EUROCRYPT 2021. – 2021. – Vol.12696 – P. 711–740. DOI: 10.1007/978-3-030-77870-5_25.*
10. *Beierle, C., Leander, G., Todo, Y. Improved Differential-Linear Attacks with Applications to ARX Ciphers // Journal of Cryptology. – 2022. – Vol.35. DOI: 10.1007/s00145-022-09437-z.*
11. *Liu, J., Rijmen, V., Hu, Y. et al. WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix // Science China Information Sciences. – 2022. – Vol.65. DOI: 10.1007/s11432-020-3105-1.*
12. *Beierle, C., Biryukov, A., Cardoso, D. S. et al. Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX) // Advances in Cryptology – CRYPTO 2020. 40th Annual International Cryptology Conference, CRYPTO 2020. – 2020. – P. 419–448. DOI: 10.1007/978-3-030-56877-1_15.*
13. *Поликарпов С. В., Прудников В. А., Румянцев К. Е. Исследование свойств миниверсии псевдо-случайной функции pCollapser // Известия ЮФУ. Технические науки. – 2023. – Февраль. – Т. 230, No 6. – С. 148–162.*
14. *Прудников В. А. Исследование нелинейных свойств псевдодинамической sbox PD-SBOX 6x4x4 // Сборник статей V Всероссийской научно-технической конференции молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности». – Таганрог, 2019. – С. 96–99.*
15. *Поликарпов С. В., Румянцев К. Е., Прудников В. А. Высокопроизводительная псевдослучайная функция pCollapserARX256-32x2 // РусКрипто'2022. – 2022. – URL: https:// www.ruscrypto.ru/ resource/archive/rc2022/ files /02_polikarpov_ rumyantsev_ prudnikov.pdf.*

References

1. *Sankaralingam, A., Vivek, U. HPAC-sbox a novel implementation of predictive learning classifier and adaptive chaotic s-box for counterfeiting sidechannel attacks in an IOT networks // Microprocessors and Microsystems. 81. 103737. – 2021. DOI: 10.1016/j.micpro.2020.103737.*
2. *Artuğer, F., Karakuş, S., Özkaynak, F. Comparison of Nonlinearity Value of Substitution Box Generation Approaches // International Conference on Recent Academic Studies. – 2023. – Vol.1. – P. 46–49. DOI: 10.59287/icras.670.*
3. *Kökçam, A., Çavuşoğlu, Ü. A new approach to design S-box generation algorithm based on genetic algorithm // International Journal of Bio-Inspired Computation. 2021.– 2021. – Vol.17, No.1. – P. 52–62. DOI: 10.1504/IJBIC.2021.10035835.*
4. *Yang, S., Tong, X.,Wang, Z. S-box generation algorithm based on hyperchaotic system and its application in image encryption // Multimedia Tools and Applications. – 2023. – Vol.82.– P. 25559-25583. DOI: 10.1007/s11042-023-14394-1.*
5. *Marochok, S., Zajac, P. Algorithm for Generating S-Boxes with Prescribed Differential Properties // Algorithms. – 2023. – Vol.16. Issue 3. DOI: 10.3390/a16030157.*
6. *Khadem, B., Rajavzadeh, S. Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions // Journal of Electrical and Computer Engineering Innovations (JECEI). – 2022. – Vol.10, No.1. – P. 143–152. DOI: 10.22061/jecei.2021.7801.436.*
7. *Kang, M., Wang, M. New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity // IEEE Access. – 2022. – Vol.10. – P. 10898–10906. DOI: 10.1109/ACCESS.2022.3144458.*
8. *Siddiqui, N., Yousaf, F., Murtaza, F. et al. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field // PLoS ONE. – 2020. – Vol.15(11). DOI: 10.1371/journal.pone.0241890.*
9. *Coutinho, M., Neto, T. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha // Advances in Cryptology – EUROCRYPT 2021. – 2021. – Vol.12696 – P. 711–740. DOI: 10.1007/978-3-030-77870-5_25.*
10. *Beierle, C., Leander, G., Todo, Y. Improved Differential-Linear Attacks with Applications to ARX Ciphers // Journal of Cryptology. – 2022. – Vol.35. DOI: 10.1007/s00145-022-09437-z.*
11. *Liu, J., Rijmen, V., Hu, Y. et al. WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix // Science China Information Sciences. – 2022. – Vol.65. DOI: 10.1007/s11432-020-3105-1.*
12. *Beierle, C., Biryukov, A., Cardoso, D. S. et al. Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX) // Advances in Cryptology – CRYPTO 2020. 40th Annual International Cryptology Conference, CRYPTO 2020. – 2020. – P. 419–448. DOI: 10.1007/978-3-030-56877-1_15.*
13. *Polikarpov S. V., Prudnikov V. A., Rumjancev K. E. Issledovanie svojstv miniversii psevdo-sluchajnoj funkcii pCollapser // Izvestija JuFU. Tehnicheskie nauki. – 2023. – Fevral'. – T. 230, No 6. – S. 148–162.*
14. *Prudnikov V. A. Issledovanie nelinejnyh svojstv psevdodinamicheskoj sbox PD-SBOX 6x4x4 // Sbornik statej V Vserossijskoj nauchno-tehnicheskoj konferencii molodyh uchenyh, aspirantov, magistrantov i studentov «Fundamental'nye i prikladnye aspekty komp'juternyh tehnologij i informacionnoj bezopasnosti». – Taganrog, 2019. – S. 96–99.*
15. *Polikarpov S. V., Rumjancev K. E., Prudnikov V. A. Vysokoproizvoditel'naja psevdosluchajnaja funkcija pCollapserARX256-32x2 // RusKripto'2022. – 2022. – URL: https:// www.ruscrypto.ru/ resource/archive/rc2022/ files /02_polikarpov_ rumyantsev_ prudnikov.pdf.*