Ключові слова: інформація, інформатизація, персональні комп'ютери, інформаційно-комунікаційні системи, автоматизовані робочі місця, ідентифікація, аутентифікація, несанкціонований доступ, паролі.

Ключевые слова: информация, информатизация, персональные компьютеры, информационно-коммуникационные системы, автоматизированные рабочие места, идентификация, аутентификация, несанкционированный доступ, пароли.

Key words: information, informatization, personal computers, information and communication systems, automated workstations, identification, authentication, unauthorized access, passwords.

БАКУНИНА ЕЛЕНА ВАЛЕРЬЕВНА

Национальный университет «Одесская юридическая академия»,
доцент кафедры кибербезопасности,
кандидат физико-математических наук, доцент

О СУЩЕСТВОВАНИИ КЛАССА S-БЛОКОВ, УДОВЛЕТВОРЯЮЩИХ КОРРЕЛЯЦИОННОМУ ИММУНИТЕТУ КОМПОНЕНТНЫХ БУЛЕВЫХ ФУНКЦИЙ И 4-ФУНКЦИЙ

Одно из важнейших мест в любой комплексной системе защиты информации занимает криптографическая подсистема. При этом, со времен открытия К. Шенноном математически строго обоснованной теории секретной связи, теория криптографической стойкости получила свое существенное развитие во многом благодаря введению и описанию критериев криптографического качества компонентных булевых функций, с помощью которых могут быть представлены конструкции криптографического алгоритма [1; 2].

Тем не менее, дальнейшее развитие методов криптографии и криптоанализа, а также разработка новых методов криптоаналитических атак, основанных на функциях многозначной логики, актуализирует переход к последующему этапу развития криптографии, основанному на использовании преимуществ функций многозначной логики.

Переход к новому этапу означает разработку криптографических примитивов, в первую очередь S-блоков, для которых выполняются не только критерии криптографического качества компонентных булевых функции, но и новые критерии криптографического качества функций многозначной логики, с помощью которых могут быть описаны конструкции практически всех современных криптографических алгоритмов [3].

При этом важнейшим критерием, характеризующим способность S-блока, а значит, и всего криптопреобразования в котором он используется, противостоять атакам корреляционного криптоанализа, является критерий корреляционного иммунитета его компонентных функций.

Одной из практически применимых длин S-блоков является длина $N = 16$, используемая во многих современных криптоалгоритмах, например, в криптоалгоритме Магма [4]. Известно [3], что данные S-блоки могут быть представлены как с помощью математического аппарата булевых функций, так и с помощью математического аппарата 4-функций.

Тем не менее, классы S-блоков практически ценных длин, в частности, длины $N = 16$, соответствующие как критерию корреляционного иммунитета компонентных булевых функций, так и критерию корреляционного иммунитета компонентных 4-функций, остаются неисследованными. В настоящий момент в открытых источниках отсутствуют как методы синтеза данных подстановочных конструкций, так и точные оценки количества их возможных структур.

Для определения соответствия компонентных 4-функций S-блоков критерию корреляционного иммунитета обозначим следующее. Концепция критерия корреляционного иммунитета была введена в работе [5], в то время как определения корреляционной независимости выхода 3-функции от заданной её входной переменной, а также определение корреляционного иммунитета 3-функций, основанные на определении разбаланса функций многозначной логики были введены в работе [6].

Далее мы вводим необходимое нам для дальнейших исследований определение корреляционного иммунитета 4-функций, основываясь на обобщенном определении разбаланса функций многозначной логики.

Определение 1. Разбалансом последовательности f назовем значение модуля суммы поэлементных произведений элементов вектора K на соответствующие им элементы экспоненциального алфавита $\{z_0, z_1, \ldots, z_{q-1}\}$

$$\Delta(f) = \left| K_0 z_0 + K_1 z_1 + \ldots + K_{q-1} z_{q-1} \right|. \qquad (1)$$

На основе Определения 1 разбаланса функции многозначной логики введем определение независимости выхода 4-функции от её входных переменных, а также определение корреляционного иммунитета 4-функции.

Определение 2 [6]. Подфункцией q-функции $f(x)$, называется функция f', полученная подстановкой в f значений из множества $\{0, 1, \ldots q-1\}$ вместо некоторых переменных. Если подставим в функцию f константы $\sigma_{i_1}, \cdots, \sigma_{i_s}$ вместо переменных $x_{i_1}, \cdots, x_{i_s}$ соответственно, то полученная подфункция обозначается $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$.

Определение 3. Говорят, что выход 4-функции $f(x)$ является независимым от группы своих входных переменных $\{x_i\}$, $i = 1, \ldots, m$, если при подстановке вместо этих переменных любых констант

$\sigma_{i_1}, \cdots, \sigma_{i_s} \in \{0,1,2,3\}$, разбаланс полученных таким образом подфункций составляет $\Delta_{f'} = \frac{\Delta_f}{4^m}$.

Определение 4. Говорят, что 4-функция $f(x)$ является корреляционно иммунной порядка $m \le k$, если её выход является независимым относительно любой группы из m своих входных переменных, т. е. разбаланс всех её подфункций $k-m$ переменных составляет $\Delta_{f'} = \frac{\Delta_f}{4^m}$.

В настоящей работе предлагается следующий метод синтеза S-блоков, удовлетворяющих как критерию корреляционного иммунитета компонентных булевых функций, так и критерию корреляционного иммунитета компонентных 4-функций, который запишем в виде конкретных шагов:

Шаг 1. Путем рассмотрения всех возможных вариантов булевых функций длины $N = 16$, количество которых составляет $J = 2^{16} = 65536$, с помощью определения корреляционного иммунитета булевых функций [2] выделяем корреляционно-иммунные булевы функции первого порядка.

Шаг 2. На основе найденного множества корреляционно-иммунных первого порядка булевых функций в соответствии с теоремой о построении S-блоков [7] конструируем полное множество S-блоков, компонентные функции которых являются корреляционно-иммунными первого порядка.

Шаг 3. Представляем каждый из полученных S-блоков, входящих в состав полного множества построенных на *Шаге 2* S-блоков в виде двух компонентных 4-функций.

Шаг 4. На основе Определения 4 исследуем компонентные 4-функции построенных S-блоков на соответствие критерию корреляционного иммунитета первого порядка компонентных 4-функций. Отбрасываем все S-блоки, у которых хотя-бы одна компонентная 4-функция не является корреляционно иммунной.

Выполнение представленного метода позволяет получить следующие результаты.

Исследование полного множества из $J = 65536$ булевых функций позволило установить, что общее количество корреляционно-иммунных первого порядка булевых функций составляет 222.

На основе данного множества булевых функций удается построить множество из 6 728 064 биективных S-блоков.

Среди данных S-блоков существует точно 18 304 S-блока, удовлетворяющих как критерию корреляционного иммунитета компонентных булевых функций, так и критерию корреляционного иммунитета компонентных 4-функций.

Отметим основные результаты проведенных исследований:

1. На основе определения разбаланса функции многозначной логики введено определение независимости выхода 4-функции от её входа, а также определение корреляционного иммунитета 4-функции.

2. Разработан метод синтеза S-блоков длины $N=16$, удовлетворяющих критерию корреляционного иммунитета первого порядка как в смысле компонентных булевых функций, так и в смысле компонентных 4-функций. Используя разработанный метод удалось синтезировать полное множество из 18 304 S-блоков, удовлетворяющих как критерию корреляционного иммунитета компонентных булевых функций, так и критерию корреляционного иммунитета компонентных 4-функций.

3. Указанные S-блоки являются сильнейшими с точки зрения противостояния корреляционному криптоанализу и могут применяться в составе практических конструкций современных криптоалгоритмов.

Список использованной литературы:

1. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М. : ИНФРА-М, 2013. 90 с.
2. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany, 2015. 100 с.
3. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики : монография. М. : Научная мысль, 2020. 192 с.
4. ГОСТ 34.12-2018. Информационная технология. криптографическая защита информации. Блочные шифры. М. : Стандартинформ. 17 с.
5. Gopalakrishnan K. Stinson D. R. Three characterizations of non-binary correlation-immune and resilient functions. Designs, Codes and Cryptography. 1995. P. 241–251.
6. Sokolov A. V., Zhdanov O. N. Correlation immunity of three-valued logic functions. Journal of Discrete Mathematical Sciences and Cryptography, 2020. P. 1–17.
7. Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. Proc. of Asiacrypt'91, Springer Verlag, 1991. P. 59–72.

Ключові слова: криптографія, блоковий симетричний шифр, S-блок, кореляційний імунітет, булева функція, функція багатозначної логіки.

Ключевые слова: криптография, блочный симметричный шифр, S-блок, корреляционный иммунитет, булева функция, функция многозначной логики.

Key words: cryptography, block symmetric cipher, S-box, correlation immunity, Boolean function, many-valued logic function.