Таблица 2

Число подстановок со свойствами 1, 2 и характеристикой $p_s \in \{8/256, 10/256\}$, $n = 4$

p_s	Узлы замены, использованные в МАГ							
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
8/256	0	2	0	0	0	0	0	2
10/256	18615	19968	20309	19921	20107	18898	18506	19807

близки по порядку к характеристике 6/256 наилучших на сегодняшний день s-боксов [5]. Заметим, что величина $p_s = 10/256$ соответствует большому количеству случайных подстановок степени 256 и не превышает их среднего значения [5, табл. 1].

Таблица 3

Сравнение характеристик p_s для s-боксов известных алгоритмов

Алгоритм	«Skipjack»	«Кузнечик»	s-боксы работы [5]	s-боксы табл. 1 и 2
p_s	12/256	8/256	6/256	8/256, 10/256

Выводы

Алгоритмический подход позволяет построить с использованием МАГ и s-боксов 4×4 большое количество s-боксов 8×8 с рядом позитивных криптографических свойств. Представляется перспективным совершенствование характеристик s-боксов 8×8 за счёт изменения параметров схемы построения и исследование вопросов синтеза s-боксов больших размеров (16×16, 32×32 и др.).

ЛИТЕРАТУРА

1. *Коренева А. М., Фомичев В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 2. С. 47–67.
2. Рекомендации по стандартизации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89. М., 2013.
3. *Anderson R., Biham E., and Knudsen L. R.* Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal, 1998.
4. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 1. С. 97–119.
5. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-boxes // CTCrypt Preproceedings. Yaroslavl, 2016. P. 232–252.

УДК 519.1 DOI 10.17223/2226308X/10/42

О ПОСТРОЕНИИ S-БОКСОВ РАЗМЕРА 4×4[1]

В. М. Фомичев, П. В. Овчинников

Предложен и реализован метод построения всех s-боксов размера $4{\times}4$, для которых выполнены следующие криптографические свойства: 1) биективность; 2) отсутствие неподвижных точек; 3) нелинейность всех нетривиальных линейных комбинаций вида координатных функций; 4) значение разностной характеристики p_s

[1]Работа первого автора выполнена в соответствии с грантом РФФИ № 16-01-00226.

подстановки s не более 4/16. Получен список всех s-боксов размера 4×4 (всего 383 084 314), обладающих данными свойствами. Созданное программное обеспечение использовано для определения указанных характеристик s-боксов алгоритмов DES и ГОСТ 28147-89.

Ключевые слова: *s-бокс, разностная характеристика.*

Введение

Нелинейные преобразования векторных пространств, получившие название s-боксов, являются важнейшим элементом раундовых преобразований симметричных блочных шифров. Размер s-бокса, реализующего преобразование множества n-мерных векторов, равен $n \times n$. Отечественные и зарубежные учёные активно проводят исследование свойств s-боксов и методов их построения [1, см. библиографию].

В работе представлен алгоритм построения всех s-боксов размера 4×4, обладающих рядом позитивных криптографических свойств. К таким свойствам относятся: подстановочность, нелинейность, совершенность, небольшая величина разностной характеристики. Изложены результаты выполненного на персональном компьютере экспериментального исследования множества s-боксов размера 4×4, в том числе используемых в некоторых известных блочных шифрах.

Алгоритм построения всех s-боксов размера 4×4. Обозначим s_1, s_2, s_3, s_4 систему булевых координатных функций s-бокса s, $V_n = \{0,1\}^n$. Алгоритм состоит из следующих шагов:

1. Построение множества F_4 всех булевых функций от четырёх переменных со свойствами: функция зависит существенно от всех переменных; функция сбалансирована (равновероятна); степень нелинейности равна 2 или 3.

2. Перебор всех возможных систем четырёх булевых функций из множества функций F_4 и проверка преобразований, соответствующих построенным системам, на наличие таких криптографических свойств, как:

1) биективность;
2) отсутствие неподвижных точек, то есть $s(\alpha) \neq \alpha$ для любого $\alpha \in V_4$;
3) нелинейность всех нетривиальных линейных комбинаций вида

$$a_1 s_1 \oplus a_2 s_2 \oplus a_3 s_3 \oplus a_4 s_4, \ a_i \in \{0,1\}, \ i = 1, \ldots, 4;$$

4) значение разностной характеристики p_s подстановки s не более 4/16, где

$$p_s = 2^{-n} \max_{\alpha,\beta \in V_n^*} |\{x \in V_n : s(x \oplus \alpha) \oplus s(x) = \beta\}|.$$

Для распознавания биективности использован критерий [2, с. 116]: s — подстановка тогда и только тогда, когда равновероятна любая нетривиальная линейная комбинация её координатных функций. Заметим, что при построении раундовой подстановки предпочтение отдается биективным s-боксам как функциям, усложняющим применение криптоаналитических атак типа метода статаналогов и др.

Полученные результаты. Из всех булевых функций от четырёх переменных (65 536 функций) в множество F_4 отобраны 12 618 (п. 1 алгоритма).

Составлен список s-боксов (систем четырёх функций) со свойствами 1–4, размер списка 383 084 314 s-боксов.

Определение характеристик s-боксов DES и ГОСТ 28147-89. Созданное программное обеспечение использовано для определения характеристик s-боксов алгоритмов DES и ГОСТ 28147-89.

Каждый из восьми s-боксов размера 6×4 алгоритма DES можно представить как 32 s-бокса размера 4×4 с помощью фиксаций битов a_1 и a_6, управляющих выбором одной из четырёх подстановок степени 16 s-бокса, где $a_1, a_2, \ldots, a_6$ — биты входного набора s-бокса. При фиксации других битов биективность s-бокса не обеспечена. Установлено, что 6 s-боксов не обладают свойством 2 (наличие неподвижных точек). Ряд s-боксов не обладают свойством 4: у 16 s-боксов $p_s = 8/16$, у 14 — $p_s = 6/16$, и имеется по одному s-боксу, у которых $p_s = 4/16$ и $10/16$.

В алгоритме ГОСТ 28147-89 используется 8 s-боксов размера 4×4, имеются рекомендации по их выбору [3]. Установлено, что из восьми s-боксов три не обладают свойством 2 (наличие неподвижных точек); у всех s-боксов $p_s = 4/16$.

Выводы

1. Построенное множество s-боксов размера 4×4, обладающее рядом позитивных свойств, может быть использовано при решении задач синтеза перспективных криптографических алгоритмов.

2. Созданное программное обеспечение может быть использовано для исследования s-боксов размера 4×4, используемых в различных действующих и перспективных криптографических системах.

ЛИТЕРАТУРА

1. *Menyachikhin A.* Spectral-Linear and Spectral-Difference Methods for Generating Cryptographically Strong S-Boxes. CTCrypt Preproc., 2016.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. Рекомендации по стандартизации ТК 26 «Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89». 2013.

УДК 519.7 DOI 10.17223/2226308X/10/43

CRYPTAUTOMATA: DEFINITION, CRYPTANALYSIS, EXAMPLE

G. P. Agibalov

This conference paper is an extended abstract of a recent article in Prikladnaya Diskretnaya Matematika (2017, No. 36), where we presented the definition of the cryptautomata and described some cryptanalysis techniques for them. In cryptosystems, the cryptautomata are widely used as its primitives including cryptographic generators, s-boxes, filters, combiners, key hash functions as well as symmetric and public-key ciphers, and digital signature schemes. A cryptautomaton is defined as a class C of automata networks of a fixed structure N constructed by means of the series, parallel, and feedback connection operations over initial finite automata (finite state machines) with transition and output functions taken from some predetermined functional classes. A cryptautomaton key can include initial states, transition and output functions of some components in N. Choosing a certain key k produces a certain network N_k from C to be a new cryptographic algorithm. In case of invertibility of N_k, this algorithm can be used for encryption. The operation (functioning) of any network N_k in the discrete time is described by the canonical system of equations of its automaton. The structure of N_k is described by the union of canonical systems of equations of its components. The cryptanalysis problems for a cryptautomaton are considered as the problems of solving the operational or structural system of equations of N_k with the corresponding unknowns that are key k variables and (or) plaintexts (input sequences). For solving such a system E, the method DSS is used. It is the