УДК 512.542.66

И.А. Мартынова

ХАРАКТЕРИСТИКИ ПОДСТАНОВОК ФАКТОРИАЛЬНЫХ МНОЖЕСТВ И КРИТЕРИИ ВЫБОРА ОДИНОЧНЫХ ПОДСТАНОВОК

Мартынова Инна Александровна, кандидат физико-математических наук, окончила факультет проблем физики и энергетики Московского физико-технического института (государственного университета), аспирантуру МФТИ (ГУ). Старший научный сотрудник Саровского физико-технического института НИЯУ МИФИ (СарФТИ). Работа выполнена на кафедре «Радиофизика и электроника» СарФТИ. Имеет монографии, учебные пособия, изобретения и статьи в области системного анализа элементов информационно-криптографических систем. [e-mail: dim010307@yandex.ru].

Аннотация

Основными функциями криптографических систем, обеспечивающими рассеивание и перемешивание информации, являются функции подстановки и перестановки, которые в работе представлены как элементы ряда факториальных множеств. В процессе анализа подстановок с целью создания новых переменных функций преобразования актуальной стала задача их однозначной нумерации и идентификации. В процессе решения этой задачи предложена новая система счисления – система счисления ряда факториальных множеств, позволившая осуществить сквозную нумерацию элементов ряда факториальных множеств и установить взаимно однозначное соответствие между номером и конкретным видом подстановок. Это позволило приступить к системному изучению их характеристик. В работе приведены основные понятия ряда факториальных множеств. Отмечено, что подстановки ряда факториальных множеств образуют симметрические группы подстановок, а конкретные подстановки, при их возведении в степень – циклические группы. Для них выполняются аксиомы групп, заданы область определения, групповая операция умножения, тождественные и обратные подстановки. Общими характеристиками подстановок ряда факториальных множеств являются количество независимых циклов, декремент, инверсия, четность и знак. В процессе их анализа в работе предложены критерии выбора одиночных подстановок с наилучшими характеристиками.

Ключевые слова: подстановка, ряд факториальных множеств, количество независимых циклов, декремент, инверсия.

doi: 10.35752/1991-2927-2020-4-62-109-117

SUBSTITUTION CHARACTERISTICS OF FACTORIAL SETS AND CRITERIA FOR CHOOSING THE SINGLE SUBSTITUTIONS

Inna Aleksandrovna Martynova, Candidate of Sciences in Engineering; graduated from the Moscow Institute of Physics and Technology at National Research University with the Bachelor's, Master's and Academic degree in physics problems and energetics; Senior Research Associate of the Sarov Institute of Physics and Technology at National Research Nuclear University MEPhI; an author of monographies, manuals, inventions, and articles in the field of system analysis of cryptographic information system elements. The present work was carried out at the Department of Radiophysics and Electronics of the Sarov Institute of Physics and Technology. e-mail: dim010307@yandex.ru.

Abstract

The substitution and permutation function, which are presented in the article as elements of a number of factorial sets, are the key functions of cryptographic systems that provide diffusion and mixing of information. A new scale of notation is proposed while analyzing this problem. This is the notation scale of a number of factorial sets. This scale of notation helps to index the elements of a number of factorial sets and establish a one-to-one correspondence between the number and a specific type of substitution. This allows analyzing substitutions characteristics systematically. This paper presents the basic concepts of a number of the factorial sets. It is noted that the permutations of the factorial sets form symmetric permutation groups, and specific permutations (when raised to a power) form cyclic groups. The group axioms are fulfilled

for the permutations of a number of factorial sets. Also, the definition domain, the group operation of multiplication, and identical and inverse substitutions are given for them. The number of independent cycles, decrement, inverse, parity and sign are common characteristics of the substitutions of a number of factorial sets. The criteria for choosing single substitutions with the best characteristics are proposed.

Keywords: substitution, a number of factorial sets, a number of insensitive cycles, decrement, inverse.

ВВЕДЕНИЕ

Основными функциями информационно-криптографических систем, обеспечивающими рассеивание и перемешивание информации, являются функции подстановки и перестановки. Их свойства и характеристики достаточно подробно описаны в работах [1–3] и других работах по общей алгебре и дискретной математике, в которых они представлены как отдельные структуры и группы преобразований. В работах [4, 5] приведена полная классификация алгебраических структур, к которым они принадлежат.

В процессе более углубленного анализа функций подстановки и перестановки возникла задача их однозначной идентификации, классификации, нумерации, анализа принципов распределения свойств и характеристик. К первым работам в этом направлении относится работа [6], связанная с разработкой метода факториального сжатия, обеспечивающего максимально возможное сжатие информации перестановок при реализации на ЭВМ. Настоящим прорывом в данном направлении стала работа [7], в которой впервые предложена новая система счисления – система счисления ряда факториальных множеств. Данная работа позволила осуществить однозначную нумерацию и идентификацию перестановок, описать внутреннюю структуру факториальных множеств и приступить к их комплексному изучению.

1 ОСНОВНЫЕ ПОНЯТИЯ ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

Рассмотрим функцию факториал $f(n) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n = n!$. Множество натуральных чисел $\{1, 2, 3, \dots, n\}$, расположенных в ряд в функции, являются *множеством образующих элементов* факториала. Для каждого набора образующих элементов

n факториал имеет свое значение равное $n!$. При увеличении числа образующих элементов факториал порождает своеобразный ряд значений, расположенных в порядке возрастания их номеров. Если их представить в виде множеств, то получится своеобразный ряд (рис. 1), который в работе [7] назван рядом факториальных множеств.

Для факториальных множеств $(n-1)!$ – число элементов предыдущего множества, а $n!$ – число элементов последующего множества. Если вместо абстрактных элементов факториального множества взять подстановки, то факториальное множество (Φ_n) можно представить как упорядоченное множество в виде матрицы (размерностью $n \times m$), столбцами которой являются n образующих элементов множества (равное номеру множества), а строками – m перестановок образующих элементов множества. Элементом факториального множества становится конкретная перестановка $(S_{n,m})$ образующих элементов, расположенная в одной из строк матрицы (таблицы) факториального множества. Факториальные множества, расположенные в возрастающем порядке их номеров: $\Phi_0, \Phi_1, \Phi_2, \Phi_3, \dots, \Phi_n$, образуют ряд факториальных множеств. Предыдущие множества полностью входят в последующие множества в качестве их первоначального подмножества [8]. Это свойство дает возможность осуществить сквозную нумерацию подстановок для всего ряда факториальных множеств.

2 ОБЩИЕ ХАРАКТЕРИСТИКИ ПОДСТАНОВОК РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

Подстановки ряда факториальных множеств образуют симметрические группы подстановок

Рис. 1. Ряд факториальных множеств

$G_0(S), G_1(S), G_2(S), \dots, G_n(S)$, а конкретные подстановки при их возведении в степень – циклические группы, для них заданы область определения, групповая операция умножения, тождественные и обратные подстановки. Обоснование выбора основных характеристик подстановок приведено в работах [9–12]. В соответствии с этим обоснованием общими характеристиками подстановок ряда факториальных множеств являются количество независимых циклов, декремент, инверсия, четность и знак. Примем этот перечень характеристик за основу для подстановок ряда факториальных множеств.

Количество независимых циклов подстановки. Цикл $(\sigma_1 \sigma_2 \dots \sigma_k)$ длины k – это подстановка, переводящая элемент σ_i в σ_{i+1} при $i = 1, 2, \dots, k-1$ и элемент σ_k в σ_1 . Циклы в подстановках могут быть зависимыми и независимыми. Независимые циклы – это циклы, на которые можно разложить конкретную подстановку S . Например, подстановка

$$S = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 0 & 8 & 7 & 2 & 6 & 5 & 1 & 3 \end{pmatrix}$$

разлагается на три независимых цикла

$$S = \left[\begin{pmatrix} 0 & 3 & 7 & 1 \\ 3 & 7 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 8 & 4 \\ 8 & 4 & 2 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix} \right] = (0371)(284)(56).$$

Количество независимых циклов подстановки n -го факториального множества обозначается $H_n(S_m)$, где H – количество независимых циклов, n – порядок (номер) факториального множества, S – подстановка, m – номер подстановки. Например, $H_4(S_m)$ – количество независимых циклов подстановки S_m факториального множества Φ_4 , $n = 4$, $m = n! = 4! = 24$, $m = \{0, 1, 2, \dots, 23\}$.

Количество независимых циклов подстановок максимально для единичных циклов. Оно равно числу образующих элементов подстановки факториального множества Φ_n . Данной характеристике соответствует начальная подстановка S_0 любого факториального множества

$$\begin{cases} H_n(S_0)_{\max} = n, \\ S_0 = (1)(2) \dots (n), \\ S_0 \in \Phi_n, n = \{1, \dots, n\}. \end{cases} \quad (1)$$

Количество независимых циклов минимально для подстановок, имеющих один (единственный) независимый цикл. Число таких подстановок равно числу элементов предыдущего факториального множества $(n-1)!$.

$$\begin{cases} H_n(S_m)_{\min} = 1, \\ N_S = \{S_m | S_m \in \Phi_n, H_n(S_m)_{\min}\} = \\ = N_{\Phi_{n-1}} = (n-1)! \end{cases} \quad (2)$$

Подстановки в зависимости от количества независимых циклов подразделяются на отдельные классы [10]. Подстановки с одним независимым циклом образуют отдельный класс подстановок. Подстановки и их обратные подстановки имеют одну область определения.

Декремент подстановки. Декремент $D_n(S_m)$ – это разность между числом элементов подстановки (n), равным порядку факториального множества, и количеством независимых циклов $H_n(S_m)$, включая циклы единичной длины:

$$D_n(S_m) = n - H_n(S_m). \quad (3)$$

Декремент подстановки обозначается $D_n(S_m)$, где D – декремент подстановки, n – порядок (номер) факториального множества, S – подстановка, m – номер подстановки. Например, $D_4(S_m)$ – декремент подстановки S_m множества Φ_4 , $n = 4$, $m = 4! = 24$, $m = \{0, 1, 2, \dots, 23\}$.

Декремент минимальный для единичных циклов и равен 0. Данной характеристике соответствует начальная подстановка S_0 любых факториальных множеств Φ_n

$$\begin{cases} D_n(S_0)_{\max} = n - H_n(S_0)_{\max} = n - n = 0, \\ S_0 = (1)(2) \dots (n), \\ S_0 \in \Phi_n, n = \{1, \dots, n\}. \end{cases} \quad (4)$$

Декремент максимальный для подстановок, имеющих один независимый цикл. Он равен $n-1$. Число таких подстановок равно числу элементов предыдущего факториального множества $(n-1)!$

$$\begin{cases} D_n(S_m)_{\min} = n - 1, \\ N_S = \{S_m | S_m \in \Phi_n, D_n(S_m)_{\max}\} = \\ = N_{\Phi_{n-1}} = (n-1)! \end{cases} \quad (5)$$

Зависимость между количеством независимых циклов и декрементом можно отразить тремя правилами:

1) при максимальном количестве независимых циклов декремент минимальный и, наоборот, при минимальном декременте количество независимых циклов максимально:

$$\begin{cases} H_n(S_0)_{\max} = n \rightarrow D_n(S_0)_{\max} = 0, \\ D_n(S_0)_{\max} = 0 \rightarrow H_n(S_0)_{\max} = n; \end{cases} \quad (6)$$

2) при минимальном количестве независимых циклов декремент максимальный и, наоборот, при макси-

мальном декременте количество независимых циклов минимально:

$$\begin{cases} H_n(S_m)_{\min} = 1 \rightarrow D_n(S_m)_{\max} = n-1, \\ D_n(S_m)_{\max} = n-1 \rightarrow H_n(S_m)_{\min} = 1; \end{cases} \quad (7)$$

3) в промежутке между крайними значениями чем больше количество независимых циклов, тем меньше декремент и, наоборот, чем меньше количество независимых циклов, тем больше декремент:

$$\begin{cases} H_n(S_m) \uparrow \rightarrow D_n(S_m) \downarrow, \\ H_n(S_m) \downarrow \rightarrow D_n(S_m) \uparrow. \end{cases} \quad (8)$$

Учитывая такую зависимость, на практике при необходимости можно использовать только одну из этих характеристик.

Минимальный декремент любой подстановки любого факториального множества равен нулю

$$D_n(S_m)_{\min} = 0. \quad (9)$$

Максимальный декремент подстановок любого факториального множества равен

$$D_n(S_m)_{\max} = n-1, \quad (10)$$

где n – порядок (номер) факториального множества.

Инверсия подстановки. Инверсия – это пара чисел $1 \leq i < j \leq n$, таких, что $a(i) > a(j)$. Число всех инверсий обозначается I . Можно привести другое определение инверсии. Инверсия (или беспорядок) – это пара элементов i_p, i_q подстановки

$$\sigma = \begin{pmatrix} 1 & \dots & p & \dots & q & \dots & n \\ i_1 & \dots & i_p & \dots & i_q & \dots & i_n \end{pmatrix},$$

такая, что $p < q$, но $i_p > i_q$ [2, 3].

Инверсия подстановки факториального множества (Φ_n) обозначается $I_n(S_m)$, где I – инверсия подстановки, n – порядок (номер) факториального множества, S – подстановка, m – номер подстановки. Например, $I_4(S_m)$ – инверсия подстановки S_m факториального множества Φ_4 , $n = 4$, $m = 4! = 24$, $m = \{0, 1, 2, \dots, 23\}$.

Инверсия минимальная и равна нулю для единичных циклов, когда никакие подстановки не производятся, это начальная подстановка S_0 для любых факториальных множеств

$$\begin{cases} I_n(S_0)_{\min} = 0, \\ S_0 = (1)(2)\dots(n). \end{cases} \quad (11)$$

Инверсия максимальная для конечной подстановки S_{m-1} любого факториального множества

$$\begin{cases} I_n(S_{m-1})_{\max}, \\ S_{m-1} = (n)\dots(2)(1). \end{cases} \quad (12)$$

Для выбора среднего значения инверсии предложены три варианта:

1) выбираются все одиночные подстановки с учетом всех значений инверсии, кроме крайних значений $I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}$. Число таких подстановок будет равно общему числу подстановок факториального множества – 2.

$$N_s = \{S_m | S_m \in \Phi_n, \text{ кроме } I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}\} = n! - 2; \quad (13)$$

2) среднее значение инверсии выбирается по формуле

$$\begin{aligned} I_n = I_{cp} &= \frac{I_{\max} + I_{\min}}{2} = \\ &= \frac{I_n(S_0)_{\min} + I_n(S_{m-1})_{\max}}{2}; \end{aligned} \quad (14)$$

3) среднее значение инверсии выбирается в промежутке между минимальным и максимальным значениями по некоторому выбранному критерию.

Выбор вариантов среднего значения инверсии осуществляет разработчик.

Четность подстановки. Четность подстановки определяется четностью числа транспозиций, на которые можно разложить подстановку, или иначе, четностью подстановки является четность ее декремента. Можно отметить также следующее, если число инверсий подстановки нечетно, то подстановка нечетная. Для любых подстановок σ и τ выполняется [2, 3] соотношение

$$|\sigma \tau| \equiv |\sigma| + |\tau| \pmod{2}. \quad (15)$$

Знак подстановки. Знак $sgn(a)$ подстановки a – это $(-1)^{d(a)}$, т. е.

$$sgn(a) = (-1)^{d(a)}. \quad (16)$$

Таким образом, если декремент четный, то знак подстановки плюс (+), если декремент нечетный, то знак подстановки минус (-).

3 КРИТЕРИИ ВЫБОРА ОДИНОЧНЫХ ПОДСТАНОВОК

Подстановки можно рассматривать во взаимодействии с другими подстановками или перестановками при выполнении определенных операций или каждую в отдельности. При рассмотрении одиночных подстановок встает задача выбора одиночной подстановки с наилучшими характеристиками. Предварительный анализ показывает, что для решения этой задачи можно ограничиться рассмотрением количества независимых циклов, декремента и инверсией подстановки, так как знак и четность подстановки полностью зависят от декремента. Характеристики подстановок факториального множества Φ_4 в объеме, необходимом для понимания процесса анализа, приведены в таблице 1, в ней m – номер подстановки в десятичной системе счисления, СС РФМ – образ номера в системе счисления ряда

факториальных множеств, S – прямая подстановка, Φ_4 – значение подстановки в табличном виде (верхняя часть табличного вида записана один раз вверху столбца жирными цифрами), S^{-1} – обратная подстановка, соответствующая прямой. Объединенный график количества независимых циклов, декремента и инверсии для подстановок множества Φ_4 приведен на рисунке 2.

В процессе анализа характеристик подстановок факториальных множеств Φ_2 – Φ_5 сформулированы три ус-

ловия выбора одиночной подстановки с наилучшими характеристиками:

1) количество независимых циклов подстановки должно быть минимальным, а декремент одновременно с этим должен быть максимальным;

2) значение инверсии должно иметь некоторое среднее значение;

3) для выбора одиночной подстановки с наилучшими характеристиками необходимо одновременное выполнение первого и второго условий.

Таблица 1

Характеристики подстановок факториального множества Φ_4

m	СС РФМ				S	Φ_4				S^{-1}	Циклы подстановок		Характеристики				
						1	2	3	4		полный	сокр.	N_4	D_4	чет.	I_4	sgn
0	0	0	0	0	S_0	1	2	3	4	S_0	(1)(2)(3)(4)	e	4	0	ч	0	+
1	1	0	0	0	S_1	2	1	3	4	S_1	(12)(3)(4)	(12)	3	1		1	-
2	0	1	0	0	S_2	3	1	2	4	S_4	(132)(4)	(132)	2	2	ч	2	+
3	1	1	0	0	S_3	1	3	2	4	S_3	(1)(23)(4)	(23)	3	1	ч	1	-
4	0	2	0	0	S_4	2	3	1	4	S_2	(123)(4)	(123)	2	2	ч	2	+
5	1	2	0	0	S_5	3	2	1	4	S_5	(13)(2)(4)	(13)	3	1		2	-
6	0	0	1	0	S_6	4	1	2	3	S_{18}	(1432)	(1432)	1	3		3	-
7	1	0	1	0	S_7	1	4	2	3	S_{14}	(1)(243)	(243)	2	2	ч	3	+
8	0	1	1	0	S_8	2	4	1	3	S_{15}	(1243)	(1243)	1	3		3	-
9	1	1	1	0	S_9	4	2	1	3	S_{19}	(143)(2)	(143)	2	2	ч	4	+
10	0	2	1	0	S_{10}	1	2	4	3	S_{10}	(1)(2)(34)	(34)	3	1		1	-
11	1	2	1	0	S_{11}	2	1	4	3	S_{11}	(12)(34)	(12)(34)	2	2	ч	2	+
12	0	0	2	0	S_{12}	3	4	1	2	S_{12}	(13)(24)	(13)(24)	2	2	ч	4	+
13	1	0	2	0	S_{13}	4	3	1	2	S_{22}	(1423)	(1423)	1	3		5	-
14	0	1	2	0	S_{14}	1	3	4	2	S_7	(1)(234)	(234)	2	2	ч	2	+
15	1	1	2	0	S_{15}	3	1	4	2	S_8	(1342)	(1342)	1	3		3	-
16	0	2	2	0	S_{16}	4	1	3	2	S_{21}	(142)(3)	(142)	2	2	ч	4	+
17	1	2	2	0	S_{17}	1	4	3	2	S_{17}	(1)(24)(3)	(24)	3	1		3	-
18	0	0	3	0	S_{18}	2	3	4	1	S_6	(1234)	(1234)	1	3		3	-
19	1	0	3	0	S_{19}	3	2	4	1	S_9	(134)(2)	(134)	2	2	ч	4	+
20	0	1	3	0	S_{20}	4	2	3	1	S_{20}	(14)(2)(3)	(14)	3	1		5	-
21	1	1	3	0	S_{21}	2	4	3	1	S_{16}	(124)(3)	(124)	2	2	ч	4	+
22	0	2	3	0	S_{22}	3	4	2	1	S_{13}	(1324)	(1324)	1	3		5	-
23	1	2	3	0	S_{23}	4	3	2	1	S_{23}	(14)(23)	(14)(23)	2	2	ч	6	+

Рис. 2. Количество независимых циклов, декремент и инверсия множества Φ_4

Условие 1 подтверждается для всех рассмотренных факториальных множеств. Анализ показывает, что оно может быть принято в качестве основного критерия при выборе одиночных подстановок факториальных множеств с наилучшими характеристиками (критерий 1).

Условие 2 может быть реализовано в трех вариантах:

Вариант 1. Выбираются все подстановки с учетом всех значений инверсии, кроме крайних значений $I_n(S_0)_{\min}$, $I_n(S_{m-1})_{\max}$. Число таких подстановок будет равно общему числу подстановок факториального множества – 2.

$$N_s = \{S_m | S_m \in \Phi_n, \text{ кроме } I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}\} = n! - 2.$$

При выборе этого варианта мощность множества подстановок, соответствующих инверсии, значительно превосходит мощность множества подстановок с минимальным значением количеством независимых циклов и максимальной дисперсией.

Вариант 1 соответствует критерию 2.1.

Вариант 2. Выбираются все подстановки, соответствующие среднему значению инверсии

$$I_m = I_{cp} = \frac{I_{\max} + I_{\min}}{2}.$$

При выборе этого варианта мощность множества подстановок, соответствующих инверсии, значительно

меньше мощности множества подстановок с минимальным значением количества независимых циклов и максимальной дисперсией.

Вариант 2 соответствует критерию 2.2.

Вариант 3. Выбираются все подстановки, соответствующие среднему значению инверсии, которые находятся в промежутке между минимальным и максимальным значениями по некоторому выбранному критерию.

При выборе этого варианта мощность множества подстановок, соответствующих данному выбору инверсии, может быть меньше, больше или равно мощности множества подстановок с минимальным значением количества независимых циклов и максимальной дисперсией.

Вариант 3 соответствует критерию 2.3.

В соответствии с условием 3 для выбора одиночной подстановки с наилучшими характеристиками необходимо одновременное выполнение первого и второго условий, т. е. количество независимых циклов должно быть минимальным, декремент – максимальным, а инверсия должна иметь некоторое среднее значение. Критерий для реализации условия 1 определен, это Критерий 1. Условие 2 для выбора среднего значения инверсии может быть реализовано в трех вариантах. Условию 2 соответствуют Критерии 2.1, 2.2 и 2.3.

Пересечению критерия 1 с критериями 2.1, 2.2 и 2.3 соответствуют критерии 3.1, 3.2 и 3.3.

Критерий 3.1.

$$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp}1, \\ N_s = \{S_m | S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)!, \\ N_s = \{S_m | S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)!, \\ N_s = \{S_m | S_m \in \Phi_n, \text{ кроме } I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}\} = n! - 2. \end{cases} \quad (17)$$

Критерий 3.2.

$$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp2}, \\ N_S = \{S_m | S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)!, \\ N_S = \{S_m | S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)!, \\ I_{cp2} = \frac{I_{\max} + I_{\min}}{2} = \frac{I_n(S_0)_{\min} + I_n(S_{m-1})_{\max}}{2}. \end{cases} \quad (18)$$

Критерий 3.3.

$$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp3}, \\ N_S = \{S_m | S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)!, \\ N_S = \{S_m | S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)!, \\ I_{cp1} \geq I_{cp3} > 0. \end{cases} \quad (19)$$

Сводная информация по критериям выбора одиночных подстановок с наилучшими характеристиками приведена в таблице 2.

Критерий 3.1 предназначен для выбора одиночных подстановок с наилучшими характеристиками. Количество таких подстановок для выбранного факториально-множества Φ_n максимально возможно и равно мощности предыдущего факториального множества Φ_{n-1} .

Критерии 3.2 и 3.3 могут быть использованы для проведения исследований подстановок. Критерий 3.3 может быть использован для выбора взаимодействующих друг с другом подстановок при выполнении над ними определенных операций (например, умножения или возведения в степень). Особенно его роль может возрасти, если в процессе анализа ослабить критерий 1. Причина ослабления критерия 1 может быть связана с процессом возведения подстановки с одиночным циклом в степень, в результате которого, если длина цикла не является простым числом, он может разлагаться на отдельные циклы. Это направление требует проведения дополнительного анализа.

ЗАКЛЮЧЕНИЕ

Решение задачи однозначной идентификации, нумерации функций подстановки, являющихся элементами ряда факториальных множеств и образующих взаимосвязанные симметрические группы подстановок, результаты анализа их характеристик и предложенные критерии выбора одиночных подстановок позволяют выбирать одиночные подстановки с наилучшими характеристиками в процессе системного автоматизированного анализа существующих функций преобразования.

Оно открывает новое направление, связанное с созданием новых переменных функций преобразования информационно-криптографических систем и операций их взаимодействия.

СПИСОК ЛИТЕРАТУРЫ

1. Shannon C. Communication theory of secret system // Bell System Techn. J. 28/1949. № 4. pp. 656–715.
2. Основы криптографии : учеб. пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М. : Гелиос АРН, 2001. 480 с.
3. Мартынов А.П., Фомченко В.Н. Криптография и электроника / под ред. А.И. Астайкина. Саров : ФГУП «РФЯЦ-ВНИИЭФ», 2006. 452 с.
4. Ван дер Варден Б.Л. Алгебра. М. : «Наука», 1976. 648 с.
5. Винберг Э.Б. Курс алгебры. М. : Изд-во «Факториал», 1999. 528 с.
6. Мартынова И.А., Мартынов А.П., Николаев Д.Б. Криптографические системы и метод факториального сжатия информации // Известия института инженерной физики. 2016. № 42. С. 54–58.
7. Мартынова И.А., Мартынов А.П. Функции перестановки в системе счисления ряда факториальных множеств // Вестник Воронежского государственного университета. Сер. Системный анализ и информационные технологии. 2016. № 3. С. 42–49.
8. Акимов О.Е. Дискретная математика: логика, группы, графы. 2-е изд., доп. М. : Лаборатория базовых знаний, 2003.
9. Мартынова И.А., Сплюхин Д.В. Исследование критериев факторов разложения рядов факториальных множеств // Наука. Мысль. 2017. № 5. С. 13–16.

Критерии выбора одиночных подстановок с наилучшими характеристиками

Таблица 2

		Критерий 1 для количества независимых циклов и инверсии	
		$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, \\ N_S = \{S_m S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)! \\ N_S = \{S_m S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)! \end{cases}$	
Критерий 2.1 для инверсии →	I_{cp1} $N_S = \{S_m S_m \in \Phi_n, \text{ кроме } I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}\} = n! - 2$	$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp1}, \\ N_S = \{S_m S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)! \\ N_S = \{S_m S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)! \\ N_S = \{S_m S_m \in \Phi_n, \text{ кроме } I_n(S_0)_{\min}, I_n(S_{m-1})_{\max}\} = n! - 2 \end{cases}$	Критерий 3.1 ←
Критерий 2.2 для инверсии →	I_{cp2} $I_{cp2} = \frac{I_{\max} + I_{\min}}{2} = \frac{I_n(S_0)_{\min} + I_n(S_{m-1})_{\max}}{2}$	$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp2}, \\ N_S = \{S_m S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)! \\ N_S = \{S_m S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)! \\ I_{cp2} = \frac{I_{\max} + I_{\min}}{2} = \frac{I_n(S_0)_{\min} + I_n(S_{m-1})_{\max}}{2} \end{cases}$	Критерий 3.1 ←
Критерий 2.3 для инверсии →	I_{cp3} $I_{cp1} \geq I_{cp3} > 0$	$\begin{cases} H_n(S_m)_{\min} = 1, D_n(S_m)_{\min} = n-1, I_{cp3}, \\ N_S = \{S_m S_m \in \Phi_n, H_n(S_m)_{\min}\} = N_{\Phi_{n-1}} = (n-1)! \\ N_S = \{S_m S_m \in \Phi_n, D_n(S_m)_{\max}\} = N_{\Phi_{n-1}} = (n-1)! \\ I_{cp1} \geq I_{cp3} > 0 \end{cases}$	Критерий 3.3 ←

10. Современные методы обеспечения безопасности в атомной энергетике : Монография / В.Г. Грибунин, В.Е. Костюков, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко ; под ред. А.И. Астайкина. Саров : ФГУП «РФЯЦ-ВНИИЭФ», 2014. 636 с.

11. Методы и средства комплексной защиты информации в технических системах : учеб. пособие / Э.В. Запонов [и др.]. Саров : ФГУП «РФЯЦ-ВНИИЭФ», 2019. 224 с.

12. Св-во о гос. регистрации программы для ЭВМ № 2020613795. Программный комплекс анализа подстановок ряда факториальных множеств / Мартынова И.А., Николаев Д.Б., Сплюхин Д.В. [и др.]. № 2020612500 ; заявл 06.03.2020 ; опубл. 23.03.2020.

REFERENCES

1. Shannon C. Communication Theory of Secret System. *Bell System Techn. J.*, 28/1949, no. 4, pp. 656–715.
2. Alferov A.P., Zubov A.Iu., Kuzmin A.S., Cheremushkin A.V. *Osnovy kriptografii*. Ucheb. posobie [Cryptography Fundamentals. Textbook]. Moscow, Gelios ARN Publ., 2001. 480 p.
3. Martynov A.P., Fomchenko V.N. *Kriptografiia i elektronika*. Pod red. A.I. Astaikina [Cryptography and Electronics. A.I. Astaikin (ed.)]. Sarov, FGUP RFYaTs-VNIIIEF Publ., 2006. 452 p.
4. Van der Varden B.L. *Algebra* [Algebra]. Moscow, Nauka Publ., 1976. 648 p.
5. Vinberg E.B. *Kurs algebrы* [Algebra Curriculum]. Moscow, Faktorial Publ., 1999. 528 p.
6. Martynova I.A., Martynov A.P., Nikolaev D.B. Kriptograficheskie sistemy i metod faktorialnogo szhatiia informatsii [Cryptographic Systems and Factorial Data Compression Method]. *Izvestiia instituta inzhenernoi fiziki* [Proc. of Institute of Engineering Physics], 2016, no. 42, pp. 54–58.
7. Martynova I.A., Martynov A.P. Funktsii perestanki v sisteme schisleniia riada faktorialnykh mnozhestv [Functions of Rearrangement in the Notation of Some Factorial Sets]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Ser. Sistemnyi analiz i informatsionnye tekhnologii* [Proc. of Voronezh State University. Series: Systems Analysis and Information Technologies], 2016, no. 3, pp. 42–49.
8. Akimov O.E. *Diskretnaia matematika: logika, gruppy, grafy*. 2-e izd., dop. [Discrete Mathematics. Logic, Groups, Graphs. 2nd Ed. enlarged]. Moscow, Laboratoriia bazovykh znaniy Publ., 2003.
9. Martynova I.A., Spliukhin D.V. Issledovanie kriterialnykh faktorov razlozheniia riadov faktorialnykh mnozhestv [Research of Criterion Factors for the Factorization of Factorial Sets]. *Nauka. Mysl.* [Science. Views]. 2017, no. 5, pp. 13–16.
10. Gribunin V.G., Kostiukov V.E., Martynov A.P., Nikolaev D.B., Fomchenko V.N. *Sovremennye metody obespecheniia bezopasnosti v atomnoi energetike*. Monografiia pod red. A.I. Astaikina [State-of-the-Art Techniques for Providing the Safety Measures in Nuclear Power Industry. Monograph. A.I. Astaikin (ed.)]. Sarov, FGUP RFYaTs-VNIIIEF Publ., 2014. 636 p.
11. Zaponov E.V. et al. *Metody i sredstva kompleksnoi zashchity informatsii v tekhnicheskikh sistemakh*. Ucheb. posobie [Complex Information Protection Techniques and Facilities of Engineering Systems. Handbook]. Sarov, FGUP RFYaTs-VNIIIEF Publ., 2019. 224 p.
12. Martynova I.A., Nikolaev D.B., Spliukhin D.V. et al. *Programmnyi kompleks analiza podstanovok riada faktorialnykh mnozhestv*. Svidetelstvo o gos. registratsii programmy dlia EVM no. 2020613795 [Software Package for Analyzing the Factorial Sets Substitution. Certificate of State Registration RF for Computer Program no. 2020613795]. No. 2020612500. Date of filling: March 06, 2020. Date of publications: March 23, 2020.