УДК 512.542.66

И.А. Мартынова

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОПЕРАЦИЙ ДЕЛЕНИЯ ПОДСТАНОВОК РЯДА ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

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 информационно-криптографических систем, обеспечивающими рассеивание и перемешивание информации, являются функции подстановки и перестановки. При синтезе новых алгоритмов преобразования данных с использованием таких функций необходимо осуществлять анализ данных криптографических примитивов. Для проведения такого анализа была 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. Использование такой системы позволяет осуществить изучение свойств и характеристик подстановок. Так как подстановки ряда факториального множества образуют циклическую группу, в данной группе можно определить операцию над элементами группы. В общем случае, в качестве данной операции выступает операция умножения (композиции) подстановок, однако в данной работе предложена иная операция для определения группы. В работе показана возможность выполнения операции деления подстановок ряда факториальных множеств. Для реализации операций деления подстановок предложены два метода: метод последовательного перемещения и метод группового перемещения, реализуемые через некоммутативные операции умножения на обратные подстановки.

Ключевые слова: подстановка, ряд факториальных множеств, умножение, деление.

doi: 10.35752/1991-2927-2021-1-63-91-97

METHODOLOGICAL SUPPORT FOR THE DIVIDING OF FACTORIAL SETS SUBSTITUTIONS

Inna Aleksandrovna Martynova, Candidate of Sciences in Physics and Mathematics; graduated from the Department of Problems of Physics and Energetics of the Moscow Institute of Physics and Technology, National Research University (MIPT); completed her postgraduate studies at MIPT; Senior Research Associate of the Sarov Institute of Physics and Technology at MIPT of National Research Nuclear University; an author of monographs, 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 functions are the main functions of information cryptographic systems that provide diffusion and mixing of information. It is required to analyze these cryptographic primitives while creating new algorithms for data transformation using such functions. A new scale of notation has been proposed for performing such analysis. This is the factorial sets statistical series notation scale. This scale of notation helps to index the factorial sets statistical series elements and establish a one-to-one correspondence between the number and a specific type of substitution. The use of this system provides a way to find new characteristics and properties of substitutions. Since substitutions of the factorial sets form a cyclic group, the operation on elements of this group can be determined. In the general case, the operation used is a multiplication of substitutions, but this paper suggests another operation for group determination. The article presents a capability for dividing the factorial sets substitutions. Two methods for implementing the substitution division operations

are proposed such as a method of successive transition and a method of group transition, which are implemented through non commutative operation of multiplying on inverted substitutions.

Keywords: substitutions, factorial sets, multiplying, dividing.

ВВЕДЕНИЕ

Основными функциями информационно-криптографических систем, обеспечивающими рассеивание и перемешивание информации, являются функции подстановки и перестановки [1–4]. При синтезе новых алгоритмов преобразования данных с использованием таких функций [5, 6] необходимо осуществлять анализ данных криптографических примитивов [7–10]. Известно, что подстановки конечного множества элементов образуют симметрические группы. В работах [11–13] отмечено, что для симметрических групп подстановок из доказательства того, что каждый левый обратный элемент является и правым обратным элементом, а каждая левая единица является правой единицей, следует возможность и однозначность двустороннего деления.

В работах [14, 15] предложены и рассмотрены ряд факториальных множеств и система счисления ряда факториальных множеств. Элементами ряда факториальных множеств являются подстановки, которые однозначно идентифицированы и пронумерованы, то есть для них установлено взаимно однозначное соответствие между номером подстановки в позиционной системе счисления с постоянным основанием (десятичной, двоичной, восьмеричной и т. д.) и конкретным видом подстановки, определяемым системой счисления ряда факториальных множеств (СС РФМ) с переменным основанием. Подстановки ряда факториальных множеств также образуют симметрические группы подстановок [15], для которых выполняются операции умножения (последовательного выполнения). Покажем для них возможность выполнения операции двустороннего деления на примере факториальных множеств Φ_3 и Φ_4 .

1 ФАКТОРИАЛЬНОЕ МНОЖЕСТВО И РЯД ФАКТОРИАЛЬНЫХ МНОЖЕСТВ

Факториальное множество (Φ_n) – это упорядоченное множество, представляющее собой матрицу (размерностью $n \times m$), столбцами которой являются n образующих элементов множества (равное номеру множества), а строками – m перестановок образующих элементов множества. Элементами факториального множества являются конкретные перестановки ($S_{n,m}$) образующих элементов, расположенные в одной из строк матрицы. 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 последующее множе-

ства в качестве их первоначального подмножества [15]. Это свойство позволило осуществить сквозную нумерацию подстановок для всего ряда факториальных множеств.

Подстановки факториального множества Φ_4 приведены в таблице 1, которая содержит символьный S , табличный и циклический виды подстановок (в полном и сокращенном виде), а также их обратные подстановки S^{-1} .

Подстановки S_0, S_1 входят в состав множества Φ_2 ($n = 2$), подстановки $S_0, \dots, S_6$ входят в состав множества Φ_3 ($n = 3$), подстановки $S_0, \dots, S_{23}$ входят в состав множества Φ_4 ($n = 4$). Подстановки факториальных множеств в общем случае обозначаются как $S_{n,m}$, где n – номер факториального множества, а m – номер подстановки этого факториального множества, например, для факториального множества Φ_4 :

$S_1 \rightarrow S_{4,1}, S_4 \rightarrow S_{4,4}, S_8 \rightarrow S_{4,8}$. Для краткости номер факториального множества можно не указывать.

Верхняя часть таблицы конкретной подстановки записана один раз для всех подстановок жирным шрифтом вверху таблицы, нижняя часть – в строке с соответ-

ствующим номером, например, $S_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

2 ВАРИАНТЫ ОПЕРАЦИЙ ДЕЛЕНИЯ И МЕТОД ПОСЛЕДОВАТЕЛЬНОГО ПЕРЕМЕЩЕНИЯ

Рассмотрим случай, когда элементами уравнения $a \cdot b = c$ являются числа. Для уравнения $a \cdot b = c$ справедливы операции деления, которые могут быть выражены через умножение:

$$\begin{cases} a \cdot b = c, \\ a = \frac{c}{b} = c \frac{1}{b} = \frac{1}{b} c = cb^{-1} = b^{-1}c, \\ b = \frac{c}{a} = c \frac{1}{a} = \frac{1}{a} c = ca^{-1} = a^{-1}c. \end{cases} \quad (1)$$

Операция деления для чисел возможна при условии, что $a \neq 0, b \neq 0$. Операция коммутативна. Порядок следования сомножителей не имеет значения.

Но природа цифр и подстановок принципиально отличается. Подстановки – это не числа, а операции. Для симметрических групп подстановок ряда факториальных множеств справедливы аксиомы группы: замкну-

Таблица

Подстановки факториального множества Φ_4

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

тости, ассоциативности, наличие обратного элемента и единицы (тождественной подстановки) [15]. Для подстановок умножение – это их последовательное выполнение, и операции деления из-за особенностей построения напрямую невозможны. Кроме того, элементы группы подстановок некоммутативны, значит выражение для подстановки a и выражение для подстановки b будут отличаться в зависимости от того, справа или слева в уравнении они расположены. Рассмотрим варианты умножения подстановок a, b, c, d , обратные подстановки представим в виде $a^{-1}, b^{-1}, c^{-1}, d^{-1}$,

e – единичный элемент (тождественная подстановка), $a \cdot a^{-1} = e, a \cdot e = e \cdot a = a$.

1. Рассмотрим уравнение $a \cdot b = c$:

1) вычислим a , умножив справа обе части уравнения на обратную подстановку b^{-1} ,
 $abb^{-1} = cb^{-1} \rightarrow b^{-1} \rightarrow a = cb^{-1}$;

2) вычислим b , умножив слева обе части уравнения на обратную подстановку a^{-1} ,
 $a^{-1}ab = a^{-1}c \rightarrow a^{-1}a = e \rightarrow b = a^{-1}c$.

Отметим, что операция деления в уравнении $a \cdot b = c$ реализуется через некоммутативные операции умножения на обратные подстановки, что позволяет нам говорить об операции деления подстановок, т. е. фактически об операции деления операций, реализуемой через умножение операций:

$$\begin{cases} a \cdot b = c, \\ a = cb^{-1}, \\ b = a^{-1}c. \end{cases} \quad (2)$$

Поясним это на примере подстановок ряда факториальных множеств Φ_4 .

Выберем подстановки:

$$a = S_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (123),$$

$$a^{-1} = S_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123) = S_4,$$

$$b = S_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1243),$$

$$b^{-1} = S_8^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1342) = S_{14}.$$

Уравнение $a \cdot b = c$ представим в виде:

$$S_2 \cdot S_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = S_1,$$

$$c = S_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

Уравнение $a = cb^{-1}$ представим в виде:

$$a = S_2 \cdot S_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = S_2.$$

Уравнение $b = a^{-1}c$ представим в виде:

$$b = S_4 \cdot S_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = S_8.$$

В результате все уравнения выполняются, более того, они выполняются для всех подстановок ряда факториальных множеств.

2. Рассмотрим уравнение $a \cdot b \cdot c = d$:

1) вычислим a :

$$abcc^{-1} = dc^{-1}, \quad cc^{-1} = e, \quad ab = dc^{-1}, \\ abb^{-1} = dc^{-1}b^{-1}, \quad bb^{-1} = e, \quad a = dc^{-1}b^{-1};$$

2) вычислим b :

$$abcc^{-1} = dc^{-1}, \quad cc^{-1} = e, \quad ab = dc^{-1}, \\ a^{-1}ab = a^{-1}dc^{-1}, \quad a^{-1}a = e, \quad b = a^{-1}dc^{-1};$$

3) вычислим c :

$$a^{-1}abc = a^{-1}d, \quad a^{-1}a = e, \quad bc = a^{-1}d, \\ b^{-1}bc = b^{-1}a^{-1}d, \quad b^{-1}b = e, \quad c = b^{-1}a^{-1}d.$$

Операция деления в уравнении $a \cdot b \cdot c = d$ реализуется через некоммутативные операции умножения на обратные подстановки:

$$\begin{cases} a \cdot b \cdot c = d, \\ a = dc^{-1}b^{-1}, \\ b = a^{-1}dc^{-1}, \\ c = b^{-1}a^{-1}d. \end{cases} \quad (3)$$

3. Рассмотрим уравнение $a \cdot b \cdot c \cdot d = f$:

1) вычислим a :

$$abcdd^{-1} = fd^{-1}, \quad dd^{-1} = e, \quad abc = fd^{-1}, \\ abcc^{-1} = fd^{-1}c^{-1}, \quad cc^{-1} = e, \quad ab = fd^{-1}c^{-1}, \\ abb^{-1} = fd^{-1}c^{-1}b^{-1}, \quad bb^{-1} = e, \quad a = fd^{-1}c^{-1}b^{-1};$$

2) вычислим b :

$$a^{-1}abcd = a^{-1}f, \quad a^{-1}a = e, \quad bcd = a^{-1}f, \\ bcdd^{-1} = a^{-1}fd^{-1}, \quad dd^{-1} = e, \quad bc = a^{-1}fd^{-1}, \\ bcc^{-1} = a^{-1}fd^{-1}c^{-1}, \quad cc^{-1} = e, \quad b = a^{-1}fd^{-1}c^{-1};$$

3) вычислим c :

$$a^{-1}abcd = a^{-1}f, \quad a^{-1}a = e, \quad bcd = a^{-1}f, \\ b^{-1}bcd = b^{-1}a^{-1}f, \quad b^{-1}b = e, \quad cd = b^{-1}a^{-1}f, \\ cdd^{-1} = b^{-1}a^{-1}fd^{-1}, \quad dd^{-1} = e, \quad c = b^{-1}a^{-1}fd^{-1};$$

4) вычислим d :

$$a^{-1}abcd = a^{-1}f, \quad a^{-1}a = e, \quad bcd = a^{-1}f, \\ b^{-1}bcd = b^{-1}a^{-1}f, \quad b^{-1}b = e, \quad cd = b^{-1}a^{-1}f, \\ c^{-1}cd = c^{-1}b^{-1}a^{-1}f, \quad c^{-1}c = e, \quad d = c^{-1}b^{-1}a^{-1}f.$$

Операция деления в уравнении $a \cdot b \cdot c \cdot d = f$ реализуется через некоммутативные операции умножения на обратные подстановки:

$$\begin{cases} a \cdot b \cdot c \cdot d = f, \\ a = fd^{-1}c^{-1}b^{-1}, \\ b = a^{-1}fd^{-1}c^{-1}, \\ c = b^{-1}a^{-1}fd^{-1}, \\ d = c^{-1}b^{-1}a^{-1}f. \end{cases} \quad (4)$$

Во всех рассмотренных случаях для вычисления использован один и тот же метод, который назван **методом последовательного перемещения**, когда последовательно левая и правая части равенства умножаются на подстановку, обратную выбранной подстановке. Формирование обратной подстановки является ключевым элементом метода последовательного перемещения и подробно рассмотрено в [15]. Затем в левой части равенства выбранная подстановка исключается на основании аксиомы $a^{-1}a = aa^{-1} = e$. Это продолжается до тех пор, пока в левой части не останется одна искомая подстановка.

3 Метод группового перемещения

Метод последовательного перемещения удобен и нагляден для уравнений с небольшим числом сомножителей. При увеличении числа сомножителей в уравнении более удобным является предложенный автором **метод группового перемещения**, в основу которого положена еще одна известная аксиома

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Для большого числа сомножителей ее можно представить в следующем виде:

$$\begin{aligned} (a_1a_2a_3...a_{n-1}a_n)^{-1} = \\ = (a_n)^{-1}(a_{n-1})^{-1}...(a_3)^{-1}(a_2)^{-1}(a_1)^{-1}. \end{aligned} \quad (5)$$

Приведем пример вычисления методом группового перемещения ряда подстановок уравнения $a \cdot b \cdot c \cdot d = f$:

1) вычислим a :

$$\begin{aligned} abcd(bcd)^{-1} &= f(bcd)^{-1}, \quad bcd(bcd)^{-1} = e, \\ (bcd)^{-1} &= d^{-1}c^{-1}b^{-1}, \quad a = fd^{-1}c^{-1}b^{-1}; \end{aligned}$$

2) вычислим d :

$$\begin{aligned} (abc)^{-1}abcd &= (abc)^{-1}f, \quad (abc)^{-1}abc = e, \\ (abc)^{-1} &= c^{-1}b^{-1}a^{-1}, \quad d = c^{-1}b^{-1}a^{-1}f. \end{aligned}$$

Полученные результаты совпадают с результатами, полученными методом последовательного перемещения, но преимущество по объему вычислений методом группового перемещения очевидно для возрастающего числа сомножителей.

Проиллюстрируем справедливость полученных результатов на подстановках факториальных множеств Φ_3 и Φ_4 , образующих группы подстановок $G_3(S)$ и $G_4(S)$ в циклическом виде, который является более компактным по сравнению с табличным. Отметим, что факториальное множество Φ_3 является начальным подмножеством множества Φ_4 и содержит подстановки $(S_0, S_1, S_2, S_3, S_4, S_5)$.

Рассмотрим уравнение $a \cdot b = c$ (пример 1).

Φ_3 : Исходные данные: $a = S_2 = (132)$,

$b = S_3 = (23)$, $c = S_1 = (12)$,

$$a^{-1} = (S_2)^{-1} = (123), \quad b^{-1} = (S_3)^{-1} = (23).$$

Решение 1: $a = c \cdot b^{-1}$.

$$S_2 = S_1 \cdot (S_3)^{-1}, \quad (132) = (12) \cdot (23).$$

Решение 2: $b = a^{-1}c$.

$$S_3 = (S_2)^{-1} \cdot S_1, \quad (23) = (123) \cdot (12).$$

Φ_4 : Исходные данные: $a = S_6 = (1432)$,

$b = S_2 = (132)$, $c = S_{13} = (1423)$,

$$a^{-1} = (S_6)^{-1} = (1234), \quad b^{-1} = (S_2)^{-1} = (123).$$

Решение 1: $a = c \cdot b^{-1}$.

$$S_6 = S_{13} \cdot (S_2)^{-1}, \quad (1432) = (1423)(123).$$

Решение 2: $b = a^{-1}c$.

$$S_2 = (S_6)^{-1} \cdot S_{13}, \quad (132) = (1234)(1423).$$

Рассмотрим уравнение $a \cdot b \cdot c = d$ (пример 2).

Φ_3 : Исходные данные:

$a = S_2 = (132)$, $b = S_3 = (23)$, $c = S_1 = (12)$,

$d = S_4 = (123)$, $a^{-1} = (S_2)^{-1} = (123)$,

$b^{-1} = (S_3)^{-1} = (23)$, $c^{-1} = (S_1)^{-1} = (12)$.

Решение 1: $a = dc^{-1}b^{-1}$.

$$S_2 = S_4(S_1)^{-1}(S_3)^{-1}, \quad (132) = (123)(12)(23).$$

Решение 2: $b = a^{-1} \cdot d \cdot c^{-1}$.

$$S_3 = (S_2)^{-1}S_4(S_1)^{-1}, \quad (23) = (123)(123)(12).$$

Решение 3: $c = b^{-1} \cdot a^{-1} \cdot d$.

$$S_1 = (S_3)^{-1}(S_2)^{-1}S_4, \quad (12) = (23)(123)(123).$$

Факториальное множество Φ_3 и группа $G_3(S)$ подстановок содержат всего 6 подстановок. Каждая прямая подстановка равна некоторой обратной подстановке и наоборот, поэтому их значения часто совпадают, что видно из примеров 1 и 2. Факториальное множество Φ_3 и группа $G_4(S)$ содержат 24 подстановки, для них таких совпадений меньше.

Φ_4 : Исходные данные:

$$a = S_6 = (1432), b = S_2 = (132),$$

$$c = S_{13} = (1423), d = S_4 = (123),$$

$$a^{-1} = (S_6)^{-1} = (1234), b^{-1} = (S_2)^{-1} = (123),$$

$$(c)^{-1} = (S_1)^{-1} = (12).$$

$$\text{Решение 1: } a = dc^{-1}b^{-1}.$$

$$S_6 = S_4(S_1)^{-1}(S_2)^{-1}, (1432) = (123)(12)(123).$$

$$\text{Решение 2: } b = a^{-1} \cdot d \cdot c^{-1}.$$

$$S_2 = (S_6)^{-1} S_4 (S_1)^{-1}, (132) = (1234)(123)(12).$$

$$\text{Решение 3: } c = b^{-1} \cdot a^{-1} \cdot d.$$

$$S_{13} = (S_2)^{-1} (S_6)^{-1} S_4, (1423) = (123)(1234)(123).$$

Рассмотрим уравнение умножения подстановок $S_1 \dots S_{i-1} S_i S_{i+1} \dots S_n$ в общем виде:

$$S_1 \dots S_{i-1} S_i S_{i+1} \dots S_n = S_x, \quad (6)$$

$$i \in \{1, \dots, i-1, i, i+1, \dots, n\},$$

тогда значение S_i подстановки можно вычислять по формуле

$$S_i = (S_{i-1})^{-1} \dots (S_1)^{-1} S_x (S_n)^{-1} \dots (S_{i+1})^{-1}. \quad (7)$$

ЗАКЛЮЧЕНИЕ

Приведенные результаты подтверждают возможность выполнения операции двустороннего деления подстановок. Для реализации операций деления подстановок ряда факториальных множеств в работе предложены метод последовательного перемещения и метод группового перемещения, реализуемые через некоммутативные операции умножения на обратные подстановки. Они являются основой методического обеспечения операций деления подстановок ряда факториальных множеств [16, 17].

СПИСОК ЛИТЕРАТУРЫ

1. Немченко И.А., Николаев Д.Б. Обеспечение безопасности качественной составляющей информации с использованием стохастических алгоритмов // Вестник Рязанского государственного радиотехнического университета. 2011. № 35. С. 126–128.
2. Васильев Р.А., Николаев Д.Б. Анализ возможностей применения голосовой идентификации в системах разграничения доступа к информации // Научный результат. Информационные технологии. 2016. Т. 1, № 1. С. 48–57.
3. Виртуальная интерактивная система формирования и отработки управляющей информации / Н.Ю. Бабанов, А.П. Мартынов, Д.Б. Николаев, А.В. Новиков, В.Н. Фомченко // Вестник НГИЭИ. 2016. № 4 (59). С. 15–29.
4. Одинцов М.В., Сплюхин Д.В., Николаев Д.Б. Исследование вопросов оптимизации параметров защищен-

ности информации // Сб. матер. IX-й Всерос. молодеж. науч.-инновац. школы «Математика и математическое моделирование». Саров, 2015. С. 75.

5. Пат. 2546238. Способ транслитерационного преобразования информации и передачи ее по каналам связи / Грибунин В.Г., Мартынов А.П., Николаев Д.Б., Фомченко В.Н.; заявл. 07.10.2013; опубл. 10.04.2015. Бюл. № 10.

6. Пат. 2554525. Способ преобразования информации с синхронной сменой инициализирующих последовательностей в блоках, соединенных каналом связи с неопределенным периодом смены / Фомченко В.Н., Мартынов А.П., Николаев Д.Б., Масягин А.М., Мартынов А.А.; заявл. 07.10.2013; опубл. 20.04.2015. Бюл. № 18.

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

8. Акимов О.Е. Дискретная математика: логика, группы, графы. 2-е изд., доп. М.: Лаборатория базовых знаний, 2003.

9. Основы криптографии: учеб. пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРН, 2001. 480 с.

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. Ван дер Варден Б.Л. Алгебра. М.: «Наука», 1976. 648 с.

12. Винберг Э.Б. Курс алгебры. М.: Изд-во «Факториал», 1999. 528 с.

13. Мартынова И.А., Машин И.Г., Фомченко В.Н. Теория поля и защита информации: Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2017. 209 с.

14. 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.

15. Мартынова И.А., Мартынов А.П., Фомченко В.Н. Аксиоматические основы функций подстановки в системе счисления ряда факториальных множеств и их характеристики: Монография. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2019. 210 с.

16. 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.

17. Мартынова И.А., Сплюхин Д.В. Методические аспекты использования системы счисления ряда факториальных множеств для обеспечения информационной безопасности / XXIII Нижегородская сессия молодых ученых (технические, естественные и математические науки): матер. докл. Нижегородский Государственный инженерно-экономический институт (Княгинино), 2018. С. 208–209.

REFERENCES

1. Nemchenko I.A., Nikolaev D.B. Obespechenie bezopasnosti kachestvennoi sostavliaiushchei informatsii s ispolzovaniem stokhasticheskikh algoritmov [Qualitative Information Component Protection with the Use of Stochastic Algorithms]. *Vestnik Riazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Vestnik of Ryazan State Radio Engineering University], 2011, no. 35, pp. 126–128.
2. Vasilev R.A., Nikolaev D.B. Analiz vozmozhnostei primeneniia golosovoi identifikatsii v sistemakh razgranicheniia dostupa k informatsii [Analyzing the Possible Use of Voice Identification in the Systems of Access to Information]. *Nauchnyi rezultat. Informatsionnye tekhnologii* [Research Result. Information Technologies], 2016, vol. 1, no. 1, pp. 48–57.
3. Babanov N.Iu., Martynov A.P., Nikolaev D.B., Novikov A.V., Fomchenko V.N. Virtualnaia interaktivnaia sistema formirovaniia i otrabotki upravliaiushchei informatsii [Virtual Interactive System of Formation and Processing of Managing Information]. *Vestnik NGIEI* [Bulletin NGIEI], 2016, no. 4 (59), pp. 15–29.
4. Odintsov M.V., Spliukhin D.V., Nikolaev D.B. Issledovanie voprosov optimizatsii parametrov zashchishchennosti informatsii [Research of Optimization Issues of Information Security Parameters]. *Sb. mater. IX-i Vseros. molodezh. nauch.-innovats. shkoly "Matematika i matematicheskoe modelirovanie"* [Proc. of the 9th Russian Youth Sci. and Innovative Workshop on Mathematics and Mathematical Modelling]. Sarov, 2015, p. 75.
5. Gribunin V.G., Martynov A.P., Nikolaev D.B., Fomchenko V.N. *Sposob transliteratsionnogo preobrazovaniia informatsii i peredachi ee po kanalam sviazi* [A Method of Transliteration and Transmission of Information through Communications Channel]. Patent RF 2546238. Date of filling: October 07, 2013. Date of publications: April 10, 2015. Bull. no. 10.
6. Fomchenko V.N., Martynov A.P., Nikolaev D.B., Masyagin A.M., Martynov A.A. *Sposob preobrazovaniia informatsii s sinkhronnoi smenoi initsializiruiushchikh posledovatelnostei v blokakh, soedinennykh kanalom sviazi s neopredelennym periodom smeny* [A Method of Data Transformation with Synchronous Change of Initiating Sequences in Blocks Linked via a Communication Channel with an Indefinite Period of Change]. Patent RF 2554525. Date of filling: October 07, 2013. Date of publications: April 20, 2015. Bull. no.18.
7. 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. Textbook]. Sarov, FGUP RFYaTs-VNIEF Publ., 2019. 224 p.
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. 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.
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. ed. A.I. Astaikin]. Sarov, FGUP RFYaTs-VNIEF Publ., 2014. 636 p.
11. Van der Varden B.L. *Algebra* [Algebra]. Moscow, Nauka Publ., 1976. 648 p.
12. Vinberg E.B. *Kurs algebr* [Algebra Curriculum]. Moscow, Faktorial Publ., 1999. 528 p.
13. Martynova I.A., Mashin I.G., Fomchenko V.N. *Teoriia polia i zashchita informatsii*. Monografiia [The Field Theory and Information Protection. Monograph]. Sarov, FGUP RFYaTs-VNIEF Publ., 2017. 209 p.
14. Martynova I.A., Martynov A.P. Funktsii perestankovki 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.
15. Martynova I.A., Martynov A.P., Fomchenko V.N. *Aksiomaticheskie osnovy funktsii podstanovki v sisteme schisleniia riada faktorialnykh mnozhestv i ikh kharakteristiki*. Monografiia [Axiomatic Basis of Substitution Function in the Notation of Some Factorial Sets and their Properties]. Sarov, FGUP RFYaTs-VNIEF Publ., 2019. 210 p.
16. 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.
17. Martynova I.A., Spliukhin D.V. Metodicheskie aspekty ispolzovaniia sistemy schisleniia riada faktorialnykh mnozhestv dlia obespecheniia informatsionnoi bezopasnosti [Methodological Aspects for Implementing the Notation System of Some Factorial Sets to Support the Information Security]. *XXIII Nizhegorodskaiia sessiia molodykh uchenykh (tekhnicheskie, estestvennye i matematicheskie nauki). Mater. dokl. Nizhegorodskii Gosudarstvennyi inzhenerno-ekonomicheskii institut* [Proc. of the 23d Young Scientists Session in Engineering, Mathematics, and Nature at the Nizhny Novgorod State Institute of Engineering and Economics]. Kniaginino, 2018, pp. 208–209.