УДК 681.3

СИСТЕМА ПРОСТРАНСТВЕННО-ГРУППОВОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ

И. А. Мартынова, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко
(ОИВТ РАН, г. Москва; ФГУП "РФЯЦ-ВНИИЭФ", г. Саров Нижегородской области)

Развитие сложных вычислительных комплексов для классов задач, использующих параллельные вычисления, предопределило необходимость формирования новых подходов к управлению процессами обработки данных, что и является предметом данной статьи. Работа с многомерными динамическими структурами характеризуется повышенными требованиями к достоверности выполняемых операций, быстродействию и прозрачности управления вычислениями. Предложенная авторами функционально-алгоритмическая модель пространственно-группового перемещения предназначена для построения траекторий обработки данных и траекторий их верификации при заданных параметрах входных и выходных информационных массивов. Модель не накладывает ограничений на обрабатываемые данные и является основой универсального инструментария для описания и анализа процессов информационного взаимодействия в сложных динамических системах, использующих параллельную обработку данных. В качестве примера применения данной модели и соответствующей ей системы пространственно-группового преобразования информационных потоков представлены результаты анализа однопоточных информационно-криптографических систем.

Ключевые слова: информационная система, многомерные множества, преобразование данных, универсальная система управления, криптографические функции.

Введение

Развитие фундаментальных и прикладных наук в настоящее время невозможно без использования значительных вычислительных ресурсов. При этом требования к точности и скорости решения задач, возникающих в процессе исследования, постоянно возрастают. Одним из основных способов ускорения вычислений является создание параллельных вычислительных методов, систем и технологий.

Распараллеливание вычислительного процесса невозможно без представления о методах решения поставленных задач, архитектуре параллельных вычислительных систем, а также математическом обеспечении, которое имеют эти системы. Важно изучать, а при необходимости и создавать классы методов, удобных для реализации в параллельной системе и имеющих гибко адаптируемую алгоритмическую структуру.

Адаптируемая алгоритмическая структура позволяет увеличивать вариативность применения вычислительных методов для обработки информационных потоков и упрощать управление процессами обработки данных.

Использование такой структуры при реализации модулей обработки данных, представляющих собой сложные динамические системы, позволяет сформировать универсальную систему управления многомерными множествами. Особенно это актуально для решения задач верификации вычислительных процедур, требующих контроля вычислений по нескольким независимым траекториям внутри единого вычислительного модуля. Количество используемых параметров и траекторий контроля определяется сложностью и составом вычислительных модулей и резко возрастает при увеличении размерности входных данных.

Таким образом, разработка системы, позволяющей реализовать единую структуру управления многомерными вычислительными объектами с высокой степенью вариативности и адаптацией к решаемым задачам, является актуальной.

Она направлена на расширение понятийного аппарата исследования сложных процессов взаимодействия, протекающих при параллельной обработке информационных массивов в режиме реального времени и с использованием специализированных и суперЭВМ, обладающих большим быстродействием.

Наиболее наглядно процесс обработки информационных потоков и функциональные процедуры управления данными процессами могут быть показаны на примере систем обработки данных в каналах связи, в том числе криптографических систем.

Криптографические функции и криптоалгоритмы

Основными функциями в криптографических системах являются подстановки и перестановки, обеспечивающие рассеивание и перемешивание информации. Их изучение проводится в двух направлениях: анализ и систематизация процессов, происходящих внутри подстановок и перестановок, и анализ базовых криптографических функций, построенных на их основе. На основе базовых криптографических функций можно строить криптографические системы любой сложности. Более того, криптографические функции можно комбинировать различными способами для получения новой криптографической системы с определенными, заранее заданными, параметрами [1, 2].

Какой бы сложной криптографическая система ни была, в процессе проведения криптографического анализа ее можно разложить на ряд последовательно выполняемых функций

$$f(x) = f_0(x), f_1(x), f_2(x), \ldots, f_n(x). \qquad (1)$$

Это относится к подавляющему большинству известных криптографических функций и алгоритмов, например таких, как криптографические алгоритмы "Люцифер", DES, AES, алгоритм по ГОСТ 28147-89 и т. д. [1, 2]. Криптоалгоритм "Люцифер" напрямую состоит из чередующихся подстановок и перестановок, что соответствует выражению (1). Покажем это также на примере широко известных криптографических алгоритмов DES и ГОСТ 28147-89, являющихся каскадными (композиционными) шифрами, основанными на преобразовании Фейстеля [1, 2].

Криптоалгоритм DES можно представить в виде 16 одинаковых последовательно обрабатываемых блоков C_i (преобразований Фейстеля), приведенных на рис. 1 (K_i — ключевые последовательности). В нем циклы для прямого и обратного преобразований имеют одинаковую структуру. Схема преобразования $f(K_i, R_i)$ показана на рис. 2, где R_i — блок входной информации; IP — первичная перестановка; P — конечная перестановка; S_i — нелинейное преобразование (подстановка).

Алгоритм ГОСТ 28147-89, как и криптоалгоритм DES, можно представить в виде последовательно обрабатываемых 32 одинаковых блоков, показанных на рис. 3, где C_i — повторяющийся цикл (преобразование Фейстеля для ГОСТ 28147-89).

В ГОСТ 28147-89 циклы прямого и обратного преобразований имеют одинаковую структуру. Схема преобразования $f(K_i, R_i)$ для ГОСТ 28147-89 показана на рис. 4.

Появление суперЭВМ, развитие методов параллельных вычислений, новые алгоритмы фак-

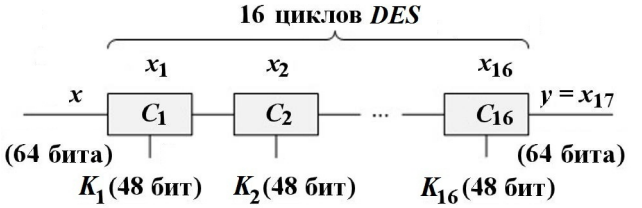

Рис. 1. Каскадный криптоалгоритм DES

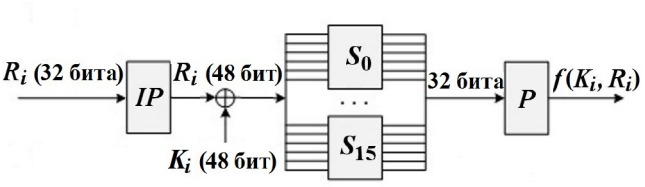

Рис. 2. Преобразование $f(K_i, R_i)$ криптоалгоритма DES

Рис. 3. Каскадный криптоалгоритм ГОСТ 28147-89

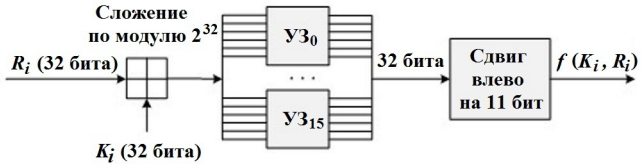

Рис. 4. Преобразование $f(K_i, R_i)$ криптоалгоритма ГОСТ 28147-89

торизации чисел, перспективы создания квантовых компьютеров и теория несепарабельных состояний многокубитных квантовых систем [3, 4] ставят под угрозу большинство классических криптографических систем, криптосистем на базе односторонних функций (типа RSA, Эль-Гамаля и др.), а также значительное количество протоколов распределения ключей [5, 6]. Все это приводит к необходимости поиска и создания новых криптографических функций и алгоритмов [1, 2, 7—10]. Перспективными в данном направлении являются исследования криптографических операций, алгоритмов преобразования информации на базе пространственно-группового перемещения функциональных элементов упорядоченных множеств [11—14].

Пространственно-групповое перемещение элементов произвольного конечного множества

Одномерное множество A_x и способы задания ключа. Рассмотрим некоторое одномерное конечное множество

$$A_x = \{a_0, a_1, a_2, \ldots, a_n\}.$$

Количество элементов множества равно n (мощность множества).

Данное множество можно представить как вектор или матрицу, состоящую из одной строки:

$$A = (a_x)_{x=\overline{0,n}} = (a_0, a_1, a_2, \ldots, a_n).$$

Опираясь на результаты исследований, приведенные в работах [7, 8, 10, 15], представим данное множество как циклическую группу, для которой определена операция циклического сдвига влево. Пространственно-групповое перемещение элементов множества осуществляется в одной строке по оси OX. При циклическом сдвиге на один шаг все элементы множества сдвигаются на одну позицию влево, a_0 переходит в конец множества (рис. 5).

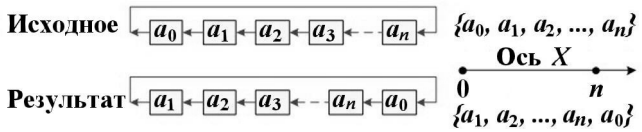

Рис. 5. Циклический сдвиг влево элементов множества A_x в графическом представлении

С точки зрения теории графов, циклическая группа множества A_x относительно операции циклического сдвига образует полный граф, поскольку все его вершины (элементы множества) связаны между собой линиями (рис. 6).

Относительно порядка следования элементов множества граф уже нельзя назвать полным, однако линии такого частичного графа образуют полную цепь. Головой цепи до циклического сдвига на один шаг является вершина a_0, после сдвига — a_1. Хвостом цепи до циклического сдвига на один шаг является вершина a_n, после сдвига — a_0.

Однако теория графов является менее удобной для анализа пространственно-группового перемещения элементов множества (особенно при значительном увеличении его мощности и размерности), поэтому в дальнейшем возьмем за основу матричное представление множества как наиболее наглядное и компактное [7, 8, 10]. Циклический сдвиг для одномерного множества будем трактовать как циклическую перестановку элементов множества по оси OX или как циклическую перестановку элементов матрицы в строке. Количество шагов сдвига может быть произвольным: от 0 до n. Количество вариантов перестановки элементов множества равно n.

Перемещение элементов (ключ) можно задавать следующими способами:

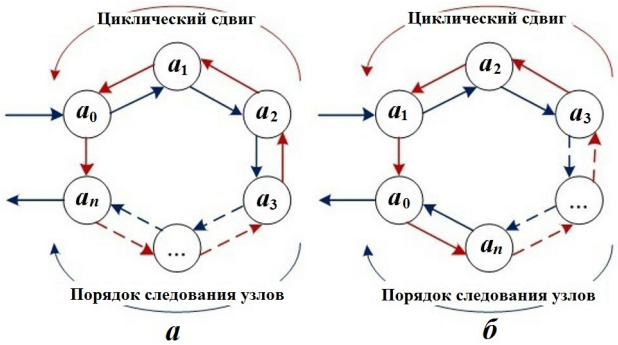

Рис. 6. Полный граф ($а$) и полная цепь ($б$) множества A_x

1) выбрать некоторый элемент множества, например a_2, и задать число шагов сдвига, например 3, — ключ в этом случае будет иметь два аргумента: $K(a_2, 3)$;
2) выбрать некоторый элемент множества, например a_3, и задать элемент множества, на место которого необходимо его переместить, например a_1, — ключ в этом случае будет содержать также два аргумента: $K(a_3, a_1)$;
3) выбрать заранее элемент, до которого будет осуществляться сдвиг, например a_0 (эта операция вводится в алгоритм по умолчанию). Ключ в этом случае можно задавать номером элемента, который необходимо переместить в выбранную точку: если выбрать элемент a_3, ключ можно представить как $K(a_3)$ или просто $K(3)$.

Последний вариант является наиболее предпочтительным, так как длина ключа* является минимальной. В дальнейшем остановимся на этом варианте. В этом случае число шагов сдвига равно номеру элемента множества. Для множества A_x возможные варианты циклического сдвига влево приведены в табл. 1.

Таблица 1

Результаты циклического сдвига влево для множества $A_x = \{a_0, a_1, a_2, a_3, \ldots, a_n\}$

Ключ	Результат
$K(0)$	$\{a_0, a_1, a_2, a_3, \ldots, a_n\}$
$K(1)$	$\{a_1, a_2, a_3, \ldots, a_n, a_0\}$
$K(2)$	$\{a_2, a_3, \ldots, a_n, a_0, a_1\}$
$K(3)$	$\{a_3, \ldots, a_n, a_0, a_1, a_2\}$
$\ldots$	$\ldots$
$K(n)$	$\{a_n, a_0, a_1, a_2, a_3, \ldots\}$

Двумерное множество A_{yx}. Рассмотрим двумерное конечное множество A_{yx}, $y = 0 \ldots m$, $x = 0 \ldots n$.

Данное множество можно представить как матрицу, состоящую из строк y и столбцов x:

$$A = (a_{yx})_{\substack{y=\overline{0,m};\\ x=\overline{0,n}}} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & \ldots & a_{0n} \\ a_{10} & a_{11} & a_{12} & \ldots & a_{1n} \\ a_{20} & a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ddots & \ldots \\ a_{m0} & a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Количество элементов множества (мощность) равно $m \times n$.

Объединим элементы данного двумерного множества в циклические группы по строкам и столбцам. Элементами данного множества A_{yx} будут уже не отдельные элементы, а группы элементов в строках и столбцах. Определим для этих групп операции циклического сдвига влево.

Пространственно-групповое перемещение групп элементов данного двумерного множества (циклический сдвиг) можно осуществлять по двум осям — OY и OX, что отражено на рис. 7.

Число шагов сдвигов может быть произвольным: по строкам от 0 до m, по столбцам от 0 до n. Количество вариантов перестановки элементов множества равно $m \times n$.

Пространственно-групповое перемещение групп элементов множества A_{yx} для $y = 0 \ldots m$, $x = 0 \ldots n$ и ключа $K(a_{12})$ показано в табл. 2.

Трехмерное множество A_{zyx}. Рассмотрим трехмерное множество A_{zyx}, $z = 0 \ldots l$, $y = 0 \ldots m$, $x = 0 \ldots n$. Количество элементов множества (мощность) равно $l \times m \times n$.

Определим группы элементов, составляющих циклические группы двумерных матриц, в которых выполняются циклические сдвиги по столбцам и строкам множества. Помимо строк и столбцов матриц, осуществляется также циклический сдвиг (перестановка) матриц в целом.

Данное множество можно представить как z-матрицы A_{yx}, состоящие из строк y и столбцов x и аналогичные матрице [11]. Число матриц равно l.

Циклический сдвиг элементов данного множества в целом можно осуществлять по трем осям: OZ, OY, OX. Циклический сдвиг по оси OZ

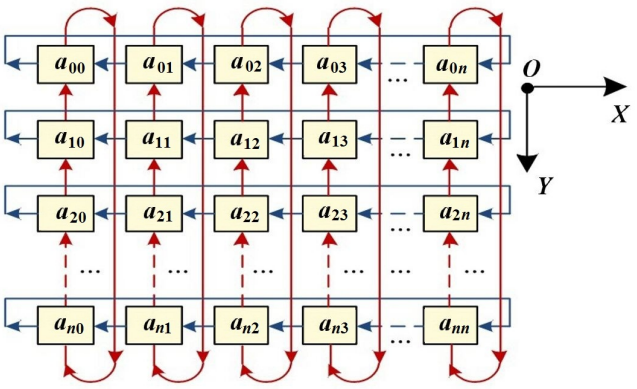

Рис. 7. Циклические сдвиги групп элементов множества A_{yx}

*Длина ключа — это объем информации, используемой в криптографическом ключе, измеряемый в битах.

Таблица 2

Пространственно-групповое перемещение групп элементов двумерного множества

Исходное состояние	Сдвиг по оси Y $(y=1)$	Сдвиг по оси X $(x=2)$ (результат)
$\begin{pmatrix} a_{00} & a_{01} & a_{02} & \dots & a_{0n} \\ a_{10} & a_{11} & \boldsymbol{a_{12}} & \dots & a_{1n} \\ a_{20} & a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{n0} & a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$	$\begin{pmatrix} a_{10} & a_{11} & \boldsymbol{a_{12}} & \dots & a_{1n} \\ a_{20} & a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{n0} & a_{n1} & a_{n2} & \dots & a_{nn} \\ a_{00} & a_{01} & a_{02} & \dots & a_{0n} \end{pmatrix}$	$\begin{pmatrix} \boldsymbol{a_{12}} & \dots & a_{1n} & a_{10} & a_{11} \\ a_{22} & \dots & a_{2n} & a_{20} & a_{21} \\ \dots & \ddots & \dots & \dots & \dots \\ a_{n2} & \dots & a_{nn} & a_{n0} & a_{n1} \\ a_{02} & \dots & a_{0n} & a_{00} & a_{01} \end{pmatrix}$

осуществляется циклическим сдвигом матриц. Циклические сдвиги по осям OY, OX осуществляются внутри каждой матрицы (рис. 8). Перемещения по оси OZ показаны в табл. 3.

Пространственно-групповое перемещение групп элементов множества A_{zyx}, для $z = 0 \dots n$, $y = 0 \dots n$, $x = 0 \dots n$ и ключа $K\,(a_{212})$ можно представить, как показано на рис. 9.

Процесс преобразования данного множества по ключу представляет собой последовательное циклическое изменение его элементов (объединенных в группы) сначала по оси OZ, затем по оси OY, а затем еще по оси OX. После окончания каждого процесса циклического изменения множество превращается в пространственную фигуру, трансформируемую при каждой перестановке элементов. Последовательность операций в общем случае может быть произвольной: ZYX, ZXY, XYZ и т. д.

Варианты увеличения размерности множества. Увеличение размерности множества можно продолжить, выбирая множество, в котором изменение его параметров происходит не по трем, а по четырем и более направлениям (осям) [3, 4]. Введение четвертого и более параметров множества (время не учитываем) трудно представить с использованием традиционной геометрии. Существует два варианта введения направлений (осей).

Вариант 1. Переходим условно в пространство, которое имеет больше чем три измерения. Это можно записать следующим образом:

A_{vzyx} при $v = 0 \dots k,\ z = 0 \dots l,$
$\quad y = 0 \dots m,\ x = 0 \dots n;$
A_{wvzyx} при $w = 0 \dots p,\ v = 0 \dots k,$
$\quad z = 0 \dots l,\ y = 0 \dots m,\ x = 0 \dots n;$
и т. д.

Таблица 3

Пространственно-групповое перемещение по оси OZ групп элементов трехмерного множества

Сдвиг	Результат
$z = 0$	$\begin{pmatrix} a_{000} & a_{001} & a_{002} & \dots & a_{00n} \\ a_{010} & a_{011} & a_{012} & \dots & a_{01n} \\ a_{020} & a_{021} & a_{022} & \dots & a_{02n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{0n0} & a_{0n1} & a_{0n2} & \dots & a_{0nn} \end{pmatrix}$
$z = 1$	$\begin{pmatrix} a_{100} & a_{101} & a_{102} & \dots & a_{10n} \\ a_{110} & a_{111} & a_{112} & \dots & a_{11n} \\ a_{120} & a_{121} & a_{122} & \dots & a_{12n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{1n0} & a_{1n1} & a_{1n2} & \dots & a_{1nn} \end{pmatrix}$
$z = 2$	$\begin{pmatrix} a_{200} & a_{201} & a_{202} & \dots & a_{20n} \\ a_{210} & a_{211} & a_{212} & \dots & a_{21n} \\ a_{220} & a_{221} & a_{222} & \dots & a_{22n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{2n0} & a_{2n1} & a_{2n2} & \dots & a_{2nn} \end{pmatrix}$
$\dots$	$\dots$
$z = n$	$\begin{pmatrix} a_{n00} & a_{n01} & a_{n02} & \dots & a_{n0n} \\ a_{n10} & a_{n11} & a_{n12} & \dots & a_{n1n} \\ a_{n20} & a_{n21} & a_{n22} & \dots & a_{n2n} \\ \dots & \dots & \dots & \ddots & \dots \\ a_{nn0} & a_{nn1} & a_{nn2} & \dots & a_{nnn} \end{pmatrix}$

Вариант 2. Используем операцию подстановки, широко применяемую в алгебре и криптографии, например $B = A_{xyz}$ при $z = 0 \dots l$, $y = 0 \dots m$, $x = 0 \dots n$. В этом случае используется трехмерное измерение, и весь процесс можно продолжить по аналогии с множествами A,

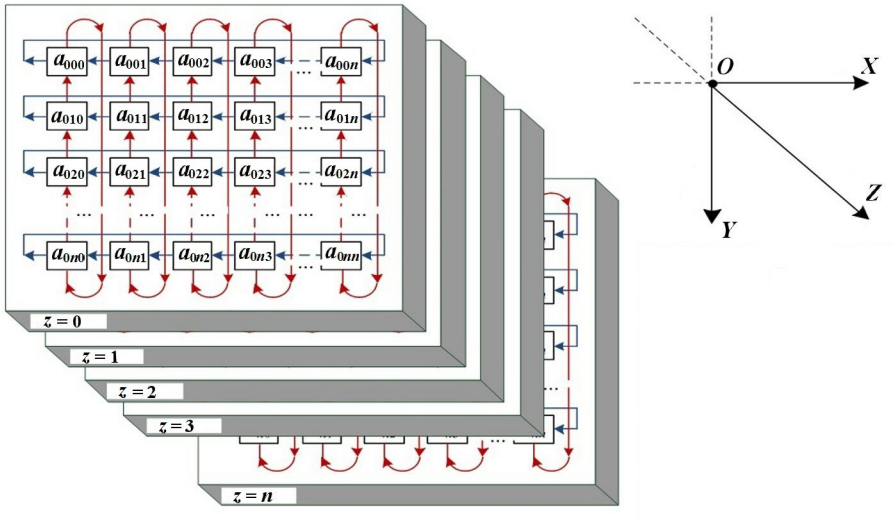

Рис. 8. Циклические сдвиги внутри матриц групп элементов множества A_{zyx}

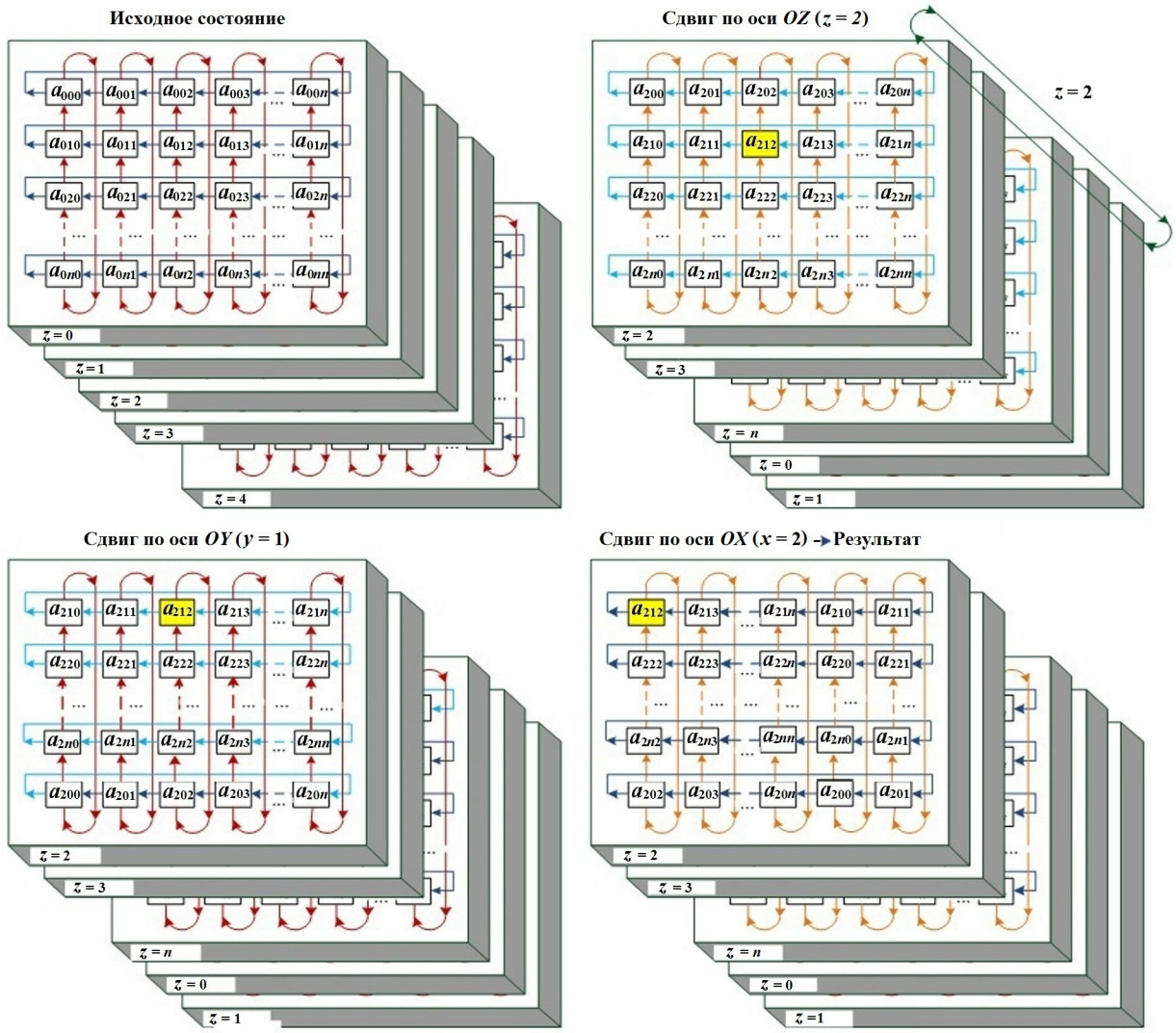

Рис. 9. Пример пространственно-группового перемещения элементов множества A_{zyx}

получая B_x, B_{xy}, B_{xyz}. По каждой оси максимальный параметр также может быть своим. Процесс подстановки можно бесконечно продолжать в двух направлениях как в сторону увеличения размерности множества, так и в сторону его уменьшения.

Опираясь на вышеизложенное, можно отметить следующее:

1) используя для пространственно-группового перемещения элементов множества их представление и объединение в циклические группы, определяя для них операцию циклического сдвига влево, можно получить сравнительно простой способ перестановки всех элементов множества по ключу малой длины, в котором количество возможных ключей равно количеству всех возможных вариантов;
2) операцию циклического сдвига можно выполнять и вправо — суть преобразования от этого не изменится, изменится только порядок расположения элементов множества на каждом шаге;
3) операции перестановки при пространственно-групповом перемещении элементов множества просты и прозрачны, а их количество значительно превышает длину ключа. Это свойство становится наиболее существенным при увеличении мощности множества;
4) способ пространственно-группового перемещения элементов множества по заданному ключу не зависит от природы элементов множества, и его можно распространить на пространственно-групповое перемещение криптографических функций.

Пространственно-групповое перемещение криптографических функций

Одномерное множество криптографических функций $F(A_x)$. Выберем в качестве отдельных элементов одномерного множества некоторые криптографические функции

$$F(A_x) = \{f(a_0), f(a_1), f(a_2), \ldots, f(a_n)\}.$$

Никаких особых требований к свойствам криптографических функций не предъявляется, кроме того, что результирующая функция должна представлять собой последовательное произведение — выполнение функций в том порядке, в котором они записаны, т. е. криптографические функции должны быть некоммутативны. В этом случае любая перестановка функций дает новую результирующую криптографическую функцию, соответствующую требованиям, изложенным в работе К. Шеннона [16].

Модель криптографической системы одномерного множества криптографических функций $F(A_x)$ показана на рис. 10. В ней предполагается, что сначала выполняется циклический сдвиг функций по ключу (верхние стрелки), а затем — преобразование исходного сообщения в криптограмму (нижние стрелки) в зависимости от конкретной криптографической системы. Преобразование криптограммы в исходное сообщение производится в обратном направлении при том же состоянии криптографической системы. Это традиционные операции в криптографии, и на данном этапе никаких особых преимуществ от такой интерпретации криптографических преобразований не прослеживается, так как традиционно идет преобразование одного исходного сообщения. Отличие заключается только в том, что ключ в данном случае применяется не к конкретной функции, а к порядку следования самих функций. На ключевые системы отдельных функций ограничений не накладывается.

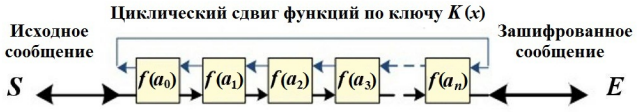

Рис. 10. Модель криптографической системы одномерного множества криптографических функций

Двумерное множество криптографических функций $F(A_{yx})$. Модель криптографической системы двумерного множества криптографических функций $F(A_{yx})$ для $y = 0, \ldots, n$; $x = 0, \ldots, n$ показана на рис. 11. В ней предполагается, что сначала выполняется циклический сдвиг функций по ключу, а затем — преобразование потока исходных сообщений в криптограммы. Преобразование криптограмм в исходные сообщения производится в обратном направлении при том же состоянии криптографической системы.

Рассматривая модель криптографической системы двумерного множества криптографических функций, можно выделить ряд новых преимуществ.

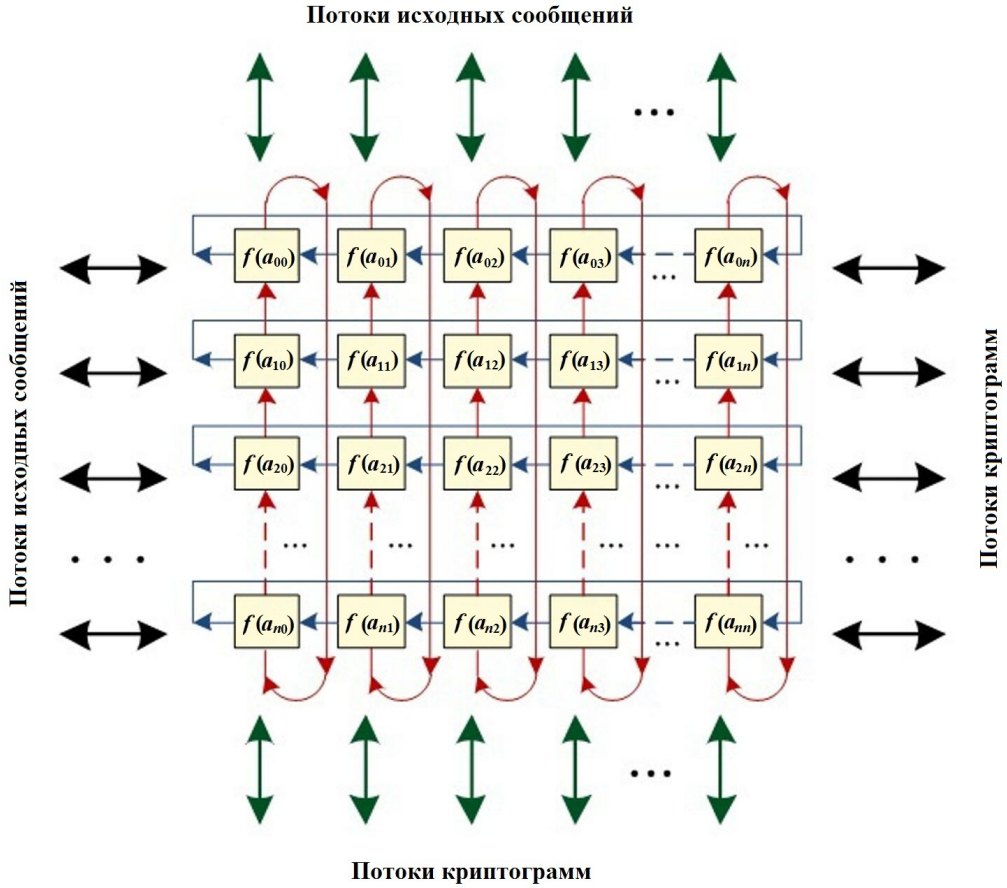

Рис. 11. Модель криптографической системы двумерного множества криптографических функций

Появилась возможность преобразования не одного исходного сообщения, а двух потоков исходных сообщений, что значительно усложняет задачу злоумышленника. Один поток направлен по оси OY, другой поток — по оси OX. При этом обратное преобразование потоков исходных сообщений можно производить как по оси OY, так и по оси OX в обратном, по отношению к прямому, направлении. Если $y = 0 \dots m$, $x = 0 \dots n$, то общее количество элементов множества будет равно $m \times n$.

Здесь необходимо отметить появление важного свойства пространственно-группового перемещения криптографических функций: возможность выполнения параллельных операций не только в процессе криптографического анализа, но и в процессе криптографического преобразования информации (не одного исходного сообщения, а сразу нескольких потоков исходных сообщений).

Это свойство является удобным применительно к специализированным и суперЭВМ, обладающим большим быстродействием и возможностью выполнения параллельных операций над информационными потоками.

Дополнительно необходимо отметить, что в ряде конкретных случаев в процессе реализации двумерного множества $F(A_{yx})$ и перестановки его элементов по ключу $K(a_{yx})$ реальную перестановку элементов множества можно не производить, а ограничиться лишь их переадресацией в определенных регистрах системы адресации. Это позволит выполнять пространственно-групповое перемещение виртуально и сократить время выполнения операций. Таким образом, в случае криптографических систем становится возможным через несколько шагов уйти от конкретной привязки элементов множества к определенной позиции, что будет сбивать накопленную статистику злоумышленника.

Ключ можно задавать с помощью генератора псевдослучайных последовательностей, обладающего определенными наперед заданными характеристиками. Ключ в зависимости от назначения системы может быть долговременным или выбираться как ключ сеанса. Этот вывод мож-

но распространить на множества криптографических функций $F(A_{zyx})$ любой размерности.

Трехмерное множество криптографических функций $F(A_{zyx})$. Рассмотрим трехмерное множество криптографических функций

$$F(A_{zyx}),\ z = 0 \dots l,\ y = 0 \dots m,\ x = 0 \dots n.$$

Данное множество можно представить как z-матрицы, состоящие из строк y и столбцов x.

Модель криптографической системы трехмерного множества криптографических функций $F(A_{zyx})$ для $l = m = n$ приведена на рис. 12. Эта модель дает еще больше преимуществ разработчику при ее реализации с применением специализированных и суперЭВМ. Она позволяет производить преобразование потоков информации по всем трем осям: OZ, OY и OX. Их общее количество значительно возрастает, особенно по отношению к длине ключа, что не влияет существенно на общую криптографическую стойкость системы. Таким образом, резко увеличивается возможность выполнения параллельных операций не только в процессе криптографических преобразований потоков информации, но и при обработке и передаче данных в многоуровневых и иерархических информационных системах. Как было отмечено ранее, это очень удобно для реализации на специализированных и суперЭВМ.

При увеличении размерности множества функций количество потоков исходных сообщений и криптограмм резко возрастает при

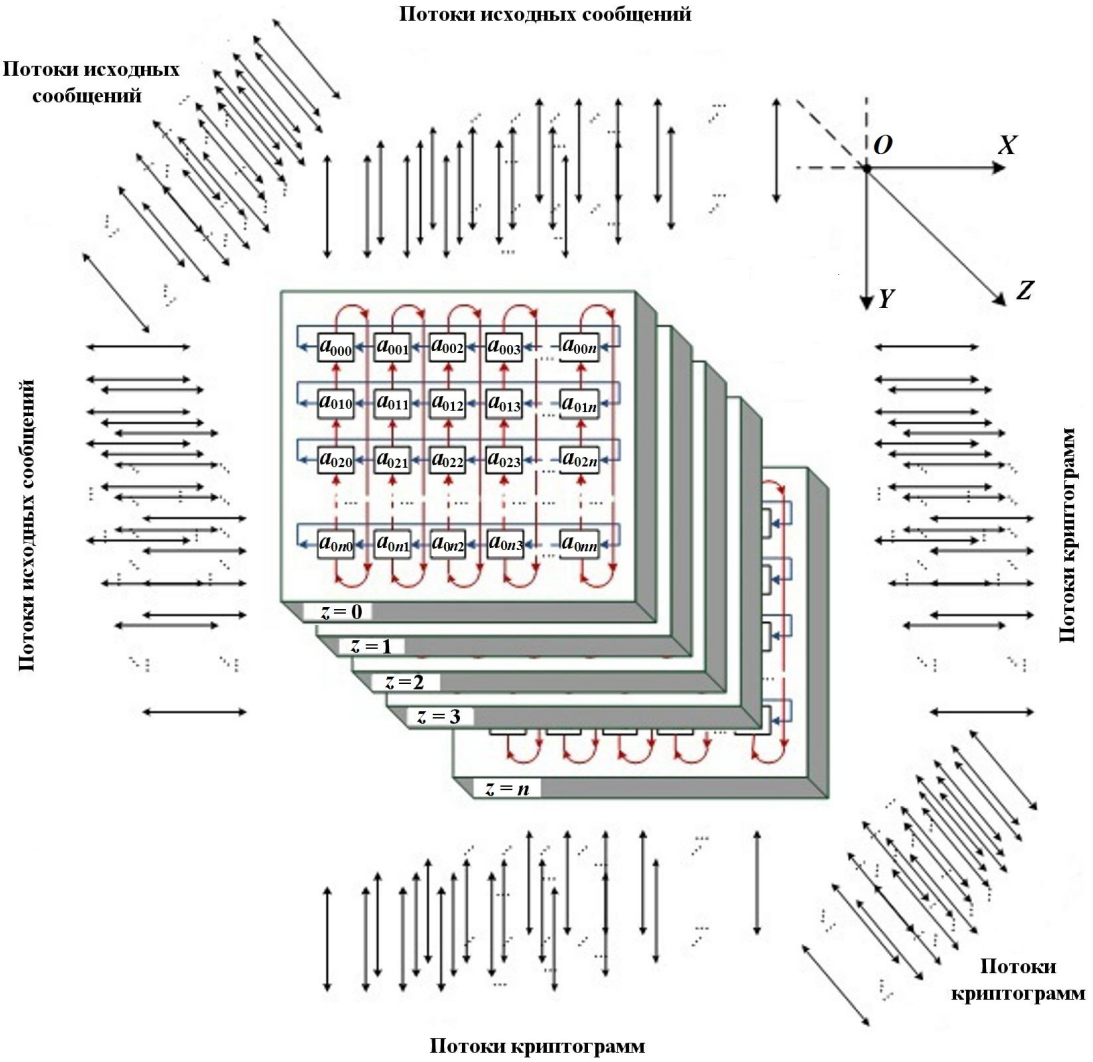

Рис. 12. Модель криптографической системы трехмерного множества криптографических функций

незначительном увеличении длины ключа. Например:

1) при $n = m = l = 8$:
   - длина ключа равна $3 + 3 + 3 = 9$ бит;
   - количество потоков по одной оси равно 64;
   - общее количество потоков равно 192;
2) при $n = m = l = 16$:
   - длина ключа равна $4 + 4 + 4 = 12$ бит;
   - количество потоков по одной оси равно 256;
   - общее количество потоков равно 768;
3) при $n = m = l = 32$:
   - длина ключа равна $5 + 5 + 5 = 15$ бит;
   - количество потоков по одной оси равно 1 024;
   - общее количество потоков равно 3 072;
4) при $n = m = l = 64$:
   - длина ключа равна $6 + 6 + 6 = 18$ бит;
   - количество потоков по одной оси равно 4 096;
   - общее количество потоков равно 12 288.

Пространственно-групповые модели и ключевая система многопоточного преобразования информационных потоков

Прямое преобразование потоков исходных сообщений и обратное преобразование криптограмм могут быть однонаправленными (ориентированными по одной из осей OZ, OY, OX) (рис. 13) или мультинаправленными (проходить по нескольким осям).

Мультинаправленное преобразование потоков исходных сообщений производится в следующем порядке (рис. 14):

1) по оси OX: от входа через плоскость $x = 0$ к выходу через плоскость $x = n$;

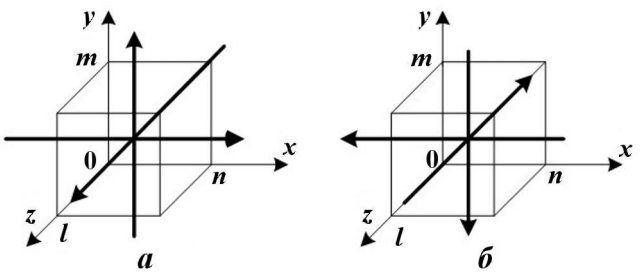

Рис. 13. Однонаправленное прохождение информационных потоков: *а* — прямое преобразование; *б* — обратное преобразование

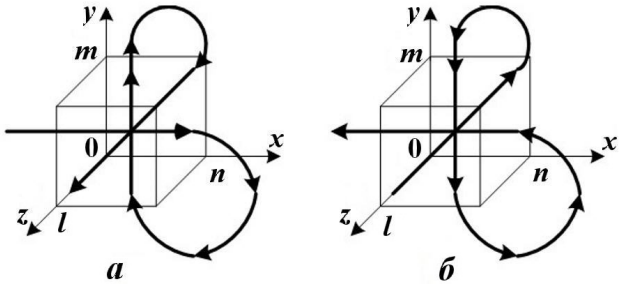

Рис. 14. Мультинаправленное прохождение информационных потоков: *а* — прямое преобразование; *б* — обратное преобразование

2) по оси OY: от входа через плоскость $y = 0$ к выходу через плоскость $y = m$;
3) по оси OZ: от входа через плоскость $z = 0$ к выходу через плоскость $z = l$.

Мультинаправленное восстановление криптограмм производится в обратном порядке:

1) по оси OZ: от входа через плоскость $z = l$ к выходу через плоскость $x = 0$;
2) по оси OY: от входа через плоскость $y = m$ к выходу через плоскость $y = 0$;
3) по оси OX: от входа через плоскость $x = n$ к выходу через плоскость $x = 0$.

В зависимости от требований, предъявляемых к системе, данные алгоритмы могут применяться полностью или частично, т. е. информационные потоки могут проходить по всем осям или только по части осей. Последовательность прохождения информационных потоков по осям также может быть произвольной.

Заключение

Проведенные исследования позволяют сделать следующие выводы:

1. Предложенный способ пространственно-группового перемещения элементов множества дает сравнительно простой способ вариативного преобразования информационных потоков путем формирования траектории преобразования с заданным числом вариантов трансформации (перестановки всех элементов информационного потока по заданному алгоритму).
2. Результаты анализа способа пространственно-группового перемещения наиболее наглядно продемонстрированы на криптогра-

фических системах, основными операциями в которых являются операции подстановки и перестановки. Криптографические функции можно комбинировать различными способами для получения новой криптографической системы с определенными, заранее заданными, параметрами.

3. Способ пространственно-группового перемещения элементов множества по заданному алгоритму не зависит от природы элементов множества. Операции перестановки просты и прозрачны, а их количество значительно превышает длину ключа.
4. Способ пространственно-группового перемещения элементов множеств применительно к многомерным множествам позволяет производить преобразование не одного исходного сообщения, как это было в классических криптографических системах, а целых потоков исходных сообщений одновременно. Траектория преобразования зависит от обрабатываемых информационных потоков и резко усложняется при увеличении их количества.
5. Важным свойством пространственно-группового перемещения является возможность выполнения параллельных операций не только в процессе обработки данных, но и в процессе анализа. Это свойство является наиболее эффективным применительно к специализированным и суперЭВМ, обладающим большим быстродействием и возможностью выполнения параллельных операций над информационными потоками.
6. Преобразование потоков исходных сообщений может быть однонаправленным (ориентированным по одной из осей множества) или мультинаправленным (проходить по всем или нескольким осям множества последовательно) в зависимости от требований, предъявляемых к информационной системе.
7. Алгоритм преобразования в информационной системе можно задавать с помощью генератора псевдослучайных последовательностей, обладающего определенными, наперед заданными, характеристиками. Алгоритм преобразования в зависимости от назначения может быть долговременным или сеансовым.

Список литературы

1. *Мартынов А. П., Фомченко В. Н.* Криптография и электроника / Под ред. А. И. Астайкина. Саров: РФЯЦ-ВНИИЭФ, 2006.
   Martynov A. P., Fomchenko V. N. Kriptografiya i elektronika / Pod red. A. I. Astaykina. Sarov: RFYaTs-VNIIEF, 2006.
2. *Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.* Современные методы обеспечения безопасности информации в атомной энергетике / Под ред. А. И. Астайкина. Саров: РФЯЦ-ВНИИЭФ, 2014.
   Gribunin V. G., Kostyukov V. E., Martynov A. P., Nikolaev D. B., Fomchenko V. N. Sovremennye metody obespecheniya bezopasnosti informatsii v atomnoy energetike / Pod red. A. I. Astaykina. Sarov: RFYaTs-VNIIEF, 2014.
3. *Мартынова И. А., Смуров С. В., Волков Г. Г., Кукин Н. С., Мурадова А. Р., Корчевая И. О.* Квантовая взаимосвязь групп симметрии NV-центра и многоэлектронных спиновых структур // Известия института инженерной физики. 2017. № 4 [46]. С. 31—37.
   Martynova I. A., Smurov S. V., Volkov G. G., Kukin N. S., Muradova A. R., Korchevaya I. O. Kvantovaya vzaimosvyaz grupp simmetrii NV-tsentra i mnogoelektronnykh spinovykh struktur // Izvestiya instituta inzhenernoy fiziki. 2017. № 4 [46]. S. 31—37.
4. *Мартынова И. А., Волков Г. Г., Кукин Н. С., Мурадова А. Р., Корчевая И. О.* SU(2) — кубит-нутритовое управление NV-центрами в алмазе // Там же. 2018. № 2 [48]. С. 63—71.
   Martynova I. A., Volkov G. G., Kukin N. S., Muradova A. R., Korchevaya I. O. SU(2) — kubit-nutritovoe upravlenie NV-tsentrami v almaze // Tam zhe. 2018. № 2 [48]. S. 63—71.
5. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003.
   Shnayder B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. M.: Triumf, 2003.

6. *Запонов Э. В., Мартынов А. П., Машин И. Г., Николаев Д. Б., Сплюхин Д. В., Фомченко В. Н.* Методы и средства комплексной защиты информации в технических системах: Уч. пособие. Саров: РФЯЦ-ВНИИЭФ, 2019.
Zaponov E. V., Martynov A. P., Mashin I. G., Nikolaev D. B., Splyukhin D. V., Fomchenko V. N. Metody i sredstva kompleksnoy zashchity informatsii v tekhnicheskikh sistemakh: Uch. posobie. Sarov: RFYaTs-VNIIEF, 2019.

7. *Мартынова И. А., Машин И. Г., Фомченко В. Н.* Введение в теорию поля и ее приложения. Саров: РФЯЦ-ВНИИЭФ, 2014.
Martynova I. A., Mashin I. G., Fomchenko V. N. Vvedenie v teoriyu polya i eye prilozheniya. Sarov: RFYaTs-VNIIEF, 2014.

8. *Мартынова И. А., Машин И. Г., Фомченко В. Н.* Теория поля и защита информации. Саров: РФЯЦ-ВНИИЭФ, 2017.
Martynova I. A., Mashin I. G., Fomchenko V. N. Teoriya polya i zashchita informatsii. Sarov: RFYaTs-VNIIEF, 2017.

9. *Мартынов А. П., Мартынова И. А.* Функции перестановки в системе счисления ряда факториальных множеств // Вестник Воронежского государственного университета. Сер. Системный анализ и информационные технологии. 2016. № 3. С. 42—49.
Martynov A. P., Martynova I. A. Funktsii perestanovki v sisteme schisleniya ryada faktorialnykh mnozhestv // Vestnik Voronezhskogo gosudarstvennogo universiteta. Ser. Sistemnyy analiz i informatsionnye tekhnologii. 2016. № 3. S. 42—49.

10. *Мартынова И. А., Мартынов А. П., Фомченко В. Н.* Аксиоматические основы функций подстановки в системе счисления ряда факториальных множеств и их характеристики. Саров: РФЯЦ-ВНИИЭФ, 2019.
Martynova I. A., Martynov A. P., Fomchenko V. N. Aksiomaticheskie osnovy funktsiy podstanovki v sisteme schisleniya ryada faktorialnykh mnozhestv i ikh kharakteristiki. Sarov: RFYaTs-VNIIEF, 2019.

11. *Мартынов А. П., Мартынова И. А., Николаев Д. Б., Сидюхин Д. В., Фомченко В. Н.* Подгруппы симметрических групп подстановок ряда факториальных множеств // Вестник Воронежского гос. ун-та. Сер. Системный анализ и информационные технологии. 2021. № 1. С. 53—62.
Martynov A. P., Martynova I. A., Nikolaev D. B., Sidyukhin D. V., Fomchenko V. N. Podgruppy simmetricheskikh grupp podstanovok ryada faktorialnykh mnozhestv // Vestnik Voronezhskogo gos. un-ta. Ser. Sistemnyy analiz i informatsionnye tekhnologii. 2021. № 1. S. 53—62.

12. Патент на изобретение № 2623894 C1 РФ, МПК H04L 9/16. Способ преобразования данных с равновероятностной инициализацией / А. П. Мартынов, И. А. Мартынова, М. В. Марунин, Д. Б. Николаев, В. Н. Фомченко. 29.06.2017. Бюллетень № 19.
Patent na izobretenie № 2623894 S1 RF, MPK H04L 9/16. Sposob preobrazovaniya dannykh s ravnoveroyatnostnoy initsializatsiey / A. P. Martynov, I. A. Martynova, M. V. Marunin, D. B. Nikolaev, V. N. Fomchenko. 29.06.2017. Byulleten № 19.

13. Патент на изобретение № 2699589 C1 РФ, МПК H04L 9/18. Способ динамического преобразования данных при хранении и передаче / К. О. Волков, А. П. Мартынов, И. А. Мартынова, Д. Б. Николаев, И. А. Николаева, В. Н. Фомченко. 06.09.2019. Бюллетень № 25.
Patent na izobretenie № 2699589. S1 RF, MPK H04L 9/18. Sposob dinamicheskogo preobrazovaniya dannykh pri khranenii i peredache / K. O. Volkov, A. P. Martynov, I. A. Martynova, D. B. Nikolaev, I. A. Nikolaeva, V. N. Fomchenko. 06.09.2019. Byulleten № 25.

14. Патент на изобретение № 2700401 C1 РФ, МПК H04L 9/32, G06K 1/12. Способ формирования идентификационных признаков для группы объектов / К. О. Волков, А. П. Мартынов, И. А. Мартынова, Д. Б. Николаев, И. А. Николаева, В. Н. Фомченко. 16.09.2019. Бюллетень № 26.
Patent na izobretenie № 2700401. S1 RF, MPK H04L 9/32, G06K 1/12. Sposob formirovaniya identifikatsionnykh priznakov dlya gruppy obyektov / K. O. Volkov, A. P. Martynov, I. A. Martynova, D. B. Nikolaev, I. A. Nikolaeva, V. N. Fomchenko. 16.09.2019. Byulleten № 26.

15. *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.
Martynova I. A., Martynov A. P., Nikolaev D. B. Kriptograficheskie sistemy i metod faktorialnogo szhatiya informatsii // Izvestiya instituta inzhenernoy fiziki. 2016. № 42. S. 54—58.

16. *Shannon C.* Communication theory of secret system // Bell System Techn. J. 1949. Vol. 28, No 4. P. 656—715.

Статья поступила в редакцию 08.06.21.