ПРЕОБРАЗОВАНИЕ ОБРАЗОВ ФУНКЦИЙ ПЕРЕСТАНОВКИ В РЯДАХ ФАКТОРИАЛЬНЫХ МНОЖЕСТВ В ПРОЦЕССЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Д. В. Сплюхин[1], *И. А. Мартынова*[1]

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.
[1]ФГУП «ВНИИА им. Н. Л. Духова», Москва

Новые технологии построения многопрофильных инженерно-технических систем, а также сложная коммуникация технологичных объектов требуют более высокоскоростные информационные протоколы передачи данных для обеспечения бесперебойности и гарантированности в различных режимах работы. Немаловажную роль в данном вопросе занимает процесс защиты информационных систем. Но прогресс не стоит на месте, и следует реформировать существующие операции прямого и обратного преобразования информации, которые являются основными составными частями процесса защиты информационных систем.

При разработке протоколов информационной безопасности необходимо использование современных подходов преобразования информации, одним из таких является использование математических преобразований, которые основываются на взаимообратимых биекциях конечного множества E ($y = F(x)$, $x = F^{-1}(y)$, $x, y \in E$). В качестве функции F может использоваться функция, перемешивающая элементы множества E в случайном порядке. Упорядоченное множество, состоящее из всех n элементов E и имеющее общее количество элементов n! называется рядом факториальных множеств.

Использование рядов факториального множества в процессах защиты информационных систем обеспечивает формирование научно-методологического базиса повышения эффективности решения задач защиты информации в виде совокупности методов анализа классической теории систем, предусматривающих непосредственное участие в фундаментальном процессе принятия решений.

В работе рассматриваются новые способы формирования и преобразования функций перестановки в рядах факториальных множеств в процессе защиты информационных систем.

Основными операциями в криптографических системах защиты информации являются операции подстановки (когда одни элементы сообщения заменяются другими) и перестановки (когда элементы сообщения переставляются местами). В качестве отдельных элементов подстановки и перестановки могут выбираться слова, символы, биты информации и даже целые предложения [1, 2].

До последнего времени подстановки рассмотрены довольно подробно в алгебре и дискретной математике, но как отдельные структуры. При их объединении в конечные множества не существовало единого признанного способа нумерации элементов данных множеств. В 2016 г. авторами выделен специальный ряд факториальных множеств существование, которого всеми подразумевалось, но никто его официально и целенаправленно не исследовал. В работе [3] предложена система счисления ряда факториальных множеств, представлены способы преобразования чисел из десятичной системы счисления в систему счисления факториальных множеств и обратно, обеспечивающие обратимое и взаимно однозначное преобразование и нумерацию элементов факториальных множеств любой размерности. Предложен способ преобразования образов ряда факториальных множеств в конкретные перестановки, имеющий большое значение для теории защиты информации и криптографии. Это позволило углубить и систематизировать процесс анализа подстановок и перестановок, начатый в работах [4].

Рассмотрим ряд факториальных множеств Φ_1, Φ_2, Φ_3, …, Φ_n., где n – порядок факториального множества, $n!$ – мощность факториального множества или, иными словами, количество входящих в него элементов (рис. 1).

Количество перестановок (P_n) и количество подстановок (S_n) для них равно

$$P_n = S_n = n!$$

В общем виде подстановки и перестановки отличаются только терминологическим первоисточником (подстановки – это алгебраический термин, а перестановки – комбинаторный термин).

Подстановки (перестановки) записывают в виде двухрядных таблиц, но для анализа их удобно записывать в циклической форме, например

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 2 & 4 & 3 & 7 & 6 \end{pmatrix} = (1)(253)(4)(67)$$

Как видно из примера не все подстановки равнозначны по своему функциональному воздействию на преобразуемую информацию. В их состав входит

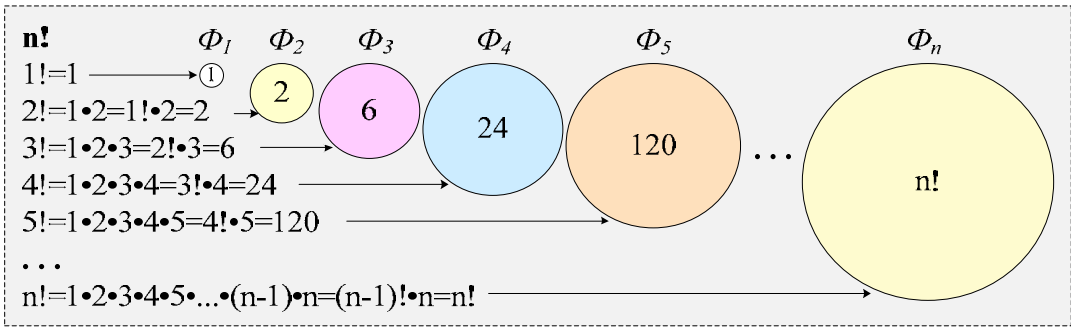

Рис. 1. Ряд факториальных множеств

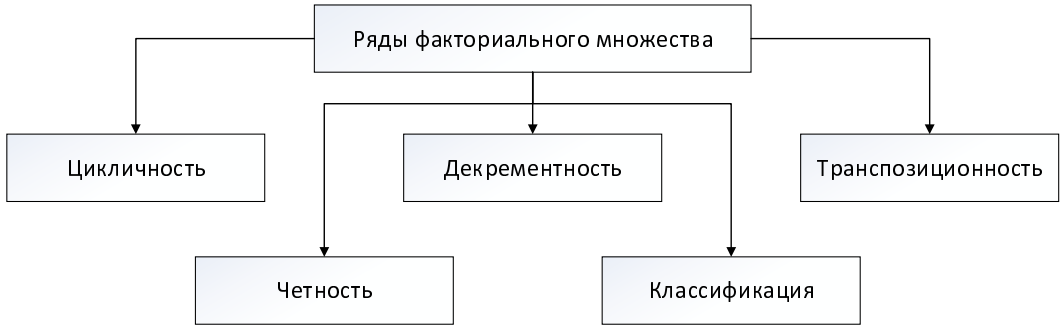

Рис. 2. Основные характеристические свойства элементов рядов факториального множества

разное количество циклов, и циклы эти могут быть различной длины. Структура и количество комбинаций циклов, входящих в подстановку, поддается классификации.

В ходе выполнения работы проведено исследование процессов защиты информационных систем при применении современных математических преобразований информации, выработано техническое решение о внедрении рядов факториальных множеств в процесс защиты информационных систем для анализа основных характеристических свойств элементов рядов.

При выполнении работ сформированы основные характеристические свойства элементов рядов факториальных множеств, такие как декрементность, четность, классификация, цикличность, транспозиционность и дано обоснование выбора данного способа в использовании современных стандартов в области защиты информации и высокотехнологичных технических средств защиты информации.

Рассмотрим основные характеристические свойства элементов рядов факториальных множеств. Цикличность – это свойство, описывающее все элементы заданного ряда факториального множества, начиная с некоторого $a_i \in E_k$ и возвращающегося в него. Например, ряд 6741253 – обладает полной цикличностью, так как начиная с первого элемента ряда возвращаемся в него же проходя все элементы, а ряд 4762351 – состоит из двух циклов (1427) (365).

Классификация – свойство, описывающее классы эквивалентности ряда факториального множества согласно цикловой структуре. Ряд факториального множества образует класс $(k) = (k_1, k_2, \ldots, k_n)$, если для каждого ряда факториального множества из этого подмножества число 1-циклов равно k_1, число 2-циклов равно k_2, …, число n-циклов равно k_n.

Транспозиционность – это свойство, характеризующее ряд факториального множества из класса $(n - 2, 1, 0, \ldots, 0)$, то есть два элемента переставляются между собой, не меняя расположения остальных.

Четность – это свойство, определяющее четность числа транспозиций, на которые раскладывается ряд факториального множества.

Декрементность – свойство, описывающее разность числа всех индексов ряда факториального множества и количества циклов, включая циклы единичной длины.

Оперируя данными свойствами, в дальнейшем можно описывать концептуальные особенности задания рядов факториального множества и применять их в теоретических основах построения систем защиты информации.

Классификация основных характеристических свойств элементов рядов факториального множества представлена на рис. 2.

Предложенные характеристические свойства рядов факториального множества позволяют использовать построенный на их основе математический аппарат в процессе преобразования информации при реализации современных стандартов и в построении высокотехнологичных технических средств защиты информации. При этом с помощью рядов происходит «перемешивание» элементов множества с заданными характеристиками, которые могут варьироваться

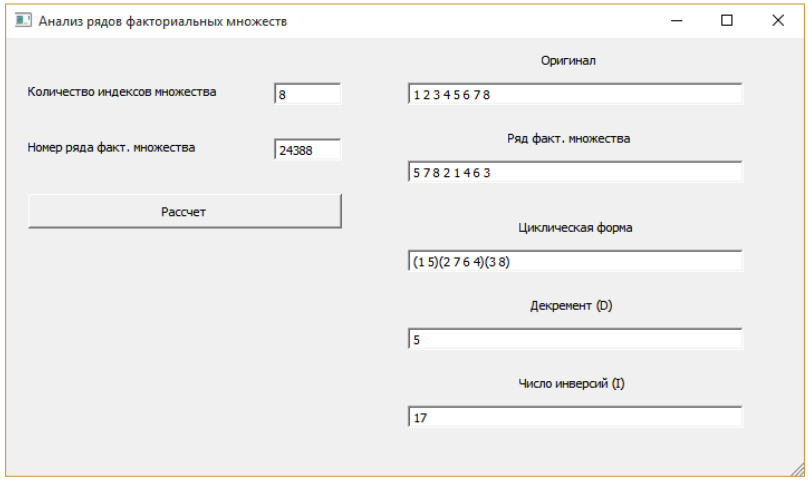

Рис. 3. Пример работы программной среды анализа рядов факториального множества

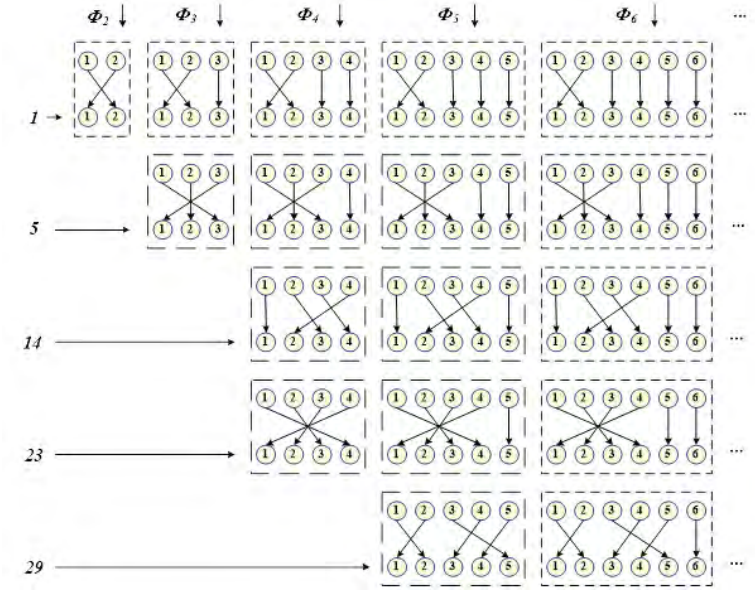

Рис. 4. Пример перестановок для рядов факториальных множеств Φ_2 , …, Φ_6, соответствующих десятичным числам 1, 5, 14, 23 и 29

в зависимости от заданных свойств рядов факториального множества.

Разработана программная среда анализа рядов факториального множества, оперирующая информацией по задаваемому ряду факториального множества. На рис. 3 приведен пример работы программной среды анализа рядов факториальных множеств. В данном примере задается ряд факториального множества с количеством элементов $n = 8$, порядковый номер ряда = 24388. Оригинал – это первый ряд с n-элементами, далее записывается полученный ряд факториального множества, затем – циклическая форма полученного ряда, а также производится подсчет декремента и числа инверсий ряда факториального множества.

В работе [3] приведена таблица соответствия десятичных чисел и образов рядов факториальных множеств для n от 1 до 5. Предложен способ преобразования образов рядов факториальных множеств в конкретные перестановки, имеющий большое значение для теории защиты информации и криптографии. Также представлены способы преобразования чисел из десятичной системы счисления в систему счисления ряда факториальных множеств и обратно, обеспечивающие обратимое и взаимно однозначное преобразование и нумерацию элементов факториальных множеств любой размерности.

Пример реализации перестановок для рядов факториальных множеств Φ_2, …, Φ_6, соответствующих десятичным числам 1, 5, 14, 23 и 29 приведен на рис. 4.

Литература

1. Мартынов А. П., Фомченко В. Н. Криптография и электроника / Под ред. А. И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2006. С. 452.

2. Мартынов А. П., Николаев Д. Б., Седаков А. В., Фомченко В. Н. Современные направления развития симметричных криптографических систем / Под ред. В. Н. Фомченко. ФГБОУ НИЯУ МИФИ СарФТИ. – Саров, 2010. С. 160.

3. Мартынов А. П., Мартынова И. А. Функции перестановки в системе счисления ряда факториальных множеств. Вестник ВГУ, Серия: Системный анализ и информационные технологии, № 3, 2016. С. 42–49.

4. Мартынова И. А., Машин И. Г., Фомченко В. Н. Введение в теорию поля и ее приложения: Монография. – Саров ФГУП «РФЯЦ-ВНИИЭФ», 2014. С. 108: ил.