ОТЗЫВ

на автореферат диссертации Пудовкиной Марины Александровны «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации», представленной на соискание учёной степени доктора физико-математических наук по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность

В последние годы теоретико-групповой подход все чаще применяется при решении разнообразных задач, возникающих при защите информации, особенно в криптографических приложениях при разработке и анализе криптосистем. При этом шифрование информации часто выполняется с помощью множества подстановок шифруемого алфавита. В связи с этим в криптографии широко применяются группы подстановок. В последние годы также используется теория представлений и характеров групп, например, для описания криптографических параметров дискретных функций. Кроме того, как правило, встречающиеся структуры криптографических функций связаны с сохраняющими их группами (как группами автоморфизмов).

Диссертационная работа Пудовкиной М.А. посвящена решению оригинальной научной проблеме, заключающейся в разработке комбинаторно-алгебраического направления по описанию структур итерационных криптографических функций. В работе широко применена геометрическая интерпретация структур. Придерживаясь «эрлангенской программе» Ф. Клейна, рассматриваемым структурам сопоставляются их группы автоморфизмов, различные свойства которых изучаются. Такие структуры задаются разными комбинаторными объектами, например, метриками, графами и разбиениями конечных множеств, а группами автоморфизмов этих структур выступают соответственно группы изометрий метрик, группы автоморфизмов графов, и группы, сохраняющие разбиения.

В связи с приложениями в криптографии рассматриваются метрики близкие по свойствам к метрике Хемминга χ на n-мерном векторном пространстве V над полем $GF(2)$, являющиеся надгруппами или подгруппами группы изометрий $\mathrm{Isom}\chi$ (равной группе экспоненцирования $S_2 \uparrow S_n$ симметрических групп S_2, S_n). Используя классификацию подсхем схемы Хемминга [Музычук М. Е. Подсхемы схемы Хемминга. Исследования по алгебраической теории комбинаторных объектов. ВНИИ системных исследований //Труды семинара.– 1985. – С. 49 – 76] и надгрупп группы $S_2 \uparrow S_n$ [Погорелов Б. А. Подметрики метрики Хемминга и теорема А.А. Маркова// Труды по дискретной математике. – 2006. –Т. 9.– С. 190 – 219], полностью классифицированы подметрики метрики Хемминга и их группы изометрий. Описаны также свойства графов, естественным образом задаваемых подметриками метрики Хемминга, при этом множество рёбер

каждого такого графа суть орбита при действии надгруппы группы $S_2 \uparrow S_n$ на упорядоченных парах векторов пространства V.

В диссертационной работе применяется разнообразный математический аппарат. Используются понятия и результаты как теории групп подстановок, так и теории цепей Маркова.

Диссертационная работа носит не только теоретический, но и практический характер (согласно автореферату имеются различные акты о внедрении результатов работы). Её результаты прошли апробацию на ряде международных и республиканских математических конференций и научных семинаров.

Автореферат написан в строгом стиле. Однако можно высказать пожелания: 1) было бы интересно классифицировать надгруппы группы экспоненцирования $S_q \uparrow S_n$ при $q \geq 3$; 2) было бы интересно идентифицировать также графы, задаваемые подметриками метрики Хемминга, которые не являются дистанционно-транзитивными.

В целом, диссертационная работа Пудовкиной Марины Александровны на тему «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» является законченным научным трудом, содержащим решение актуальной научной проблемы, удовлетворяет всем требованиям ВАК РФ, предъявляемым к докторским диссертациям по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, а её автор заслуживает присуждения учёной степени доктора физико-математических наук.

доктор физико-математических наук
(специальность 01.01.06 – математическая логика,
алгебра и теория чисел), профессор,
учреждение образования «Гомельский государственный
университет имени Франциска Скорины»,
профессор кафедры алгебры и геометрии

Александр Николаевич Скиба

Подпись профессора Скибы А.Н.
удостоверяю

Подпіс А. Н. Скіба
ЗАВЯРАЮ
Начальнік аддзела кадраў
установы адукацыі "Гомельскі дзяржаўны
ўніверсітэт імя Францыска Скарыны"

14 марта 2017 г.

Республика Беларусь, 246019, г. Гомель, ул. Кирова, 119
Тел.: +375 (232) 6087512
Интернет-адрес: http://gsu.by/mathsite/index.php/ch/aig
E-mail: algebra@gsu.by