

Отзыв

официального оппонента на диссертацию Аборнева Александра Викторовича на тему «Нелинейные подстановки, линейно представимые над кольцами Галуа, и их приложения в задачах защиты информации», представленной на соискание учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел

Разработка методов построения биективных нелинейных преобразований векторного пространства над полем Галуа является актуальной задачей. В связи с приложениями в задачах защиты информации особый интерес представляют подстановки с заданными алгебраическими и комбинаторными свойствами. В том числе подстановки, полученные с использованием итерационного принципа их построения. При этом помимо алгебраических и комбинаторных свойств используемых подстановок (алгебраическая степень нелинейности координатных функций, их линейные аналоги, разностные характеристики и др.) важным параметром является сложность реализации соответствующего преобразования, оцениваемая числом типовых вычислительных операций и объемом требуемой памяти.

Рассматриваемая диссертация посвящена методам построения и исследованию свойств нелинейных подстановок на пространстве над полем Галуа, а также на модуле над кольцом Галуа, которые индуцируются линейными преобразованиями модуля над кольцом Галуа. Данные подстановки, называемые линейно представимыми, задаются на основе разрядно подстановочных (а также разрядно инъективных) матриц и операции выделения разряда в p -адическом разложении элементов кольца Галуа. Соответствующие преобразования допускают эффективную реализацию на современных вычислительных платформах.

Диссертация состоит из двух глав. В первой главе описываются нетривиальные классы линейно представимых подстановок. Основная часть результатов получена для случая кольца Галуа характеристики 4. В этом случае

задача построения разрядно подстановочных матриц сводится к построению ортогональных систем булевых функций, являющимися квадратичными формами специального вида. Разработанные в диссертации критерии ортогональности систем квадратичных форм являются существенным продвижением в данном направлении и позволяют строить широкие классы разрядно подстановочных матриц и соответствующих им линейно представимых подстановок. В том числе описаны широкие классы линейно представимых подстановок, допускающих эффективную реализацию с помощью регистра сдвига.

Во второй главе диссертации решаются актуальные задачи описания алгебраических и комбинаторных свойств смежных классов по различным регулярным подгруппам симметрической группы подстановок, соответствующих линейно представимым подстановкам. В частности, построены классы подстановок, для которых соответствующий смежный класс по регулярной подгруппе порождает 2-транзитивную группу, знакопеременную или симметрическую группу.

В качестве недостатков диссертации можно отметить следующее.

1. Некоторые из предложенных в главе 1 нелинейных отображений для кольца Галуа характеристики 4 обладают слабыми нелинейными свойствами, так как среди их координатных функций только две нелинейные. Следовательно, для получения отображения со всеми нелинейными координатными функциями потребуется многократное применение соответствующих преобразований.

В этой связи было бы уместным привести в работе оценки для числа итераций, приводящих к нелинейным координатным функциям.

2. В работе отсутствуют сравнительные оценки соответствующих параметров предложенных итеративных преобразований с уже применяющимися на практике. Например, с алгоритмом ГОСТ 28147-89 (алгоритм «Магма» в рамках государственного стандарта ГОСТ Р 34.12.2015), в котором нелинейный блок (S-боксы) представляет собой набор нелинейных подстановок на векторах длины 4 и также просто реализуется.

Данные недостатки не влияют на общую положительную оценку диссертации, хотя и несколько снижают обоснованность рекомендаций о возможностях использования предложенных решений в алгоритмах защиты информации.

Теоретические результаты диссертации получены лично автором, являются новыми, сопровождаются строгими алгебраическими доказательствами и в полной мере опубликованы в 4 статьях в рецензируемых научных изданиях, индексируемых в базе данных RSCI. Кроме того, в работе приведены многочисленные примеры и результаты вычислений на ЭВМ.

Автореферат верно и полно отражает основные результаты диссертационной работы.

Диссертация соответствует критериям, установленным «Положением о присуждении учёных степеней в Московском государственном университете имени М.В.Ломоносова», утверждённым Ректором МГУ 27 октября 2016 г. Автор заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 01.01.06 – «Математическая логика, алгебра и теория чисел».

Профессор кафедры компьютерной безопасности
Московского института электроники и математики
имени А.Н. Тихонова НИУ ВШЭ
(123458, г. Москва, ул. Таллинская, д.34,
Телефон: 8(495) 916-88-29, электронная почта: miem@hse.ru)

доктор технических наук

М.И. Рожков

(телефон: +7 (495) 772-9590 доб. 15125, e-mail: mirozhkov@hse.ru)

Подпись заверяю

Подпись профессора М.И. Рожкова и сведения заверяю.

