ОТЗЫВ
на автореферат диссертации Давыдова Степана Андреевича на тему: «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах» на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

В кандидатской диссертации Давыдова Степана Андреевича исследуются линейные и нелинейные преобразования, используемые в блочных шифрсистемах и хэш-функциях. В частности, предложен подход к построению нелинейных подстановок с разностной δ-равномерностью 4, рассмотрены вопросы эффективной реализации циркулянтных и рекурсивных матриц, а также изучены инвариантные подпространства указанных классов матриц.

Тематика диссертации актуальна, поскольку исследуемые преобразования используются в таких распространенных шифрсистемах как AES, Кузнечик, SM4, хэш-функциях PHOTON и Whirlpool. Кроме того, в настоящий момент в мире ведутся активные исследования по разработке низкоресурсных шифрсистем, для которых важным аспектом является эффективность реализации.

Автором получены значимые теоретические результаты в вопросе построения нелинейных подстановок. Предложенная Конструкция 1 позволяет строить подстановки пространства $\mathbb{F}_2^{2m}$ с лучшими из известных нелинейностью и разностной δ-равномерностью. Экспериментально показано, что построенные подстановки пространства $\mathbb{F}_2^8$ также обладают высокой алгебраической степенью.

В рамках исследования циркулянтных и рекурсивных матриц автор получил разложения, которые могут быть использованы в программных реализациях на низкоресурсных устройствах.

Автор диссертации также исследовал метод инвариантных подпространств. Автором получены новые результаты для нелинейных преобразований, состоящих из одинаковых S-блоков, и для линейных рекурсивных преобразований. Отдельно стоит отметить полное описание инвариантных подпространств максимально рассеивающих циркулянтных матриц размера 2^n, что существенно развивает предшествующие результаты по указанной тематике.

Практически важным аспектом диссертации является неприменимость некоторых конфигураций метода криптоанализа на основе инвариантных подпространств к шифрсистемам AES и Кузнечик.

К автореферату диссертации имеются следующие незначительные замечания:

1. В тексте работы используются термины «разностный» и «дифференциальный», которые по сути определяют одно и то же (в переводе с англ. differential – разностный). Для лучшего восприятия работы следует использовать единую терминологию.
2. В качестве рекурсивной матрицы не упомянута матрица шифрсистемы LED. Также не указано применима ли теорема 4.3 к рекурсивным матрицам семейства хэш-функций PHOTON, которые неоднократно упоминаются в тексте.

Указанные замечания не умаляют значимости диссертационного исследования. Результаты работы представляют как теоретическую, так и практическую значимость.

Считаю, что соискатель Давыдов Степан Андреевич заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Автор отзыва:
кандидат физико-математических наук, доцент,
ведущий научный сотрудник
лаборатории математических проблем теоретической криптографии
Научно-исследовательского Центра
Академии криптографии Российской Федерации

Буров Дмитрий Александрович

01 ноября 2025 г.

Контактные данные:
тел.: , e-mail:

Адрес места работы:
Академия криптографии Российской Федерации

Подпись Бурова Д.А. удостоверяю.
Управляющий делами аппарата президиума
Академии криптографии Российской Федерации

А.Н. Андреев

5 ноября 2025 г.