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

Актуальность избранной темы: диссертация Давыдова Степана Андреевича посвящена вопросам анализа и синтеза линейных и нелинейных преобразований, используемых в XSL-схемах. Такие схемы часто используются при построении блочных шифрсистем и функций хэширования.

Концепция XSL-схем призвана обеспечить перемешивание и рассеивание обрабатываемых вместе с ключом входных данных. Нелинейные преобразования S обеспечивают перемешивание, линейные преобразования L обеспечивают рассеивание. Операция наложения ключа, как правило, реализована через побитовое сложение векторов по модулю 2 (XOR). На основе XSL-схем построены шифрсистемы: AES, DES, Кузнечик, Магма, SM4, хэш-функции Стрибог, PHOTON и многие другие.

Выбор преобразований в XSL-схеме является важной задачей. Уже более 30 лет известны линейный и разностный методы криптоанализа, позволяющие осуществлять атаки на шифрсистемы с плохо выбранными подстановками и рассеивающими преобразованиями.

Для защиты от линейного метода необходимо выбирать S-блоки с высоким показателем нелинейности. Максимальное значение в общем случае показателя нелинейности для S-блоков чётной размерности на сегодняшний день неизвестно.

Для защиты от разностного метода необходимо выбирать S-блоки с низким показателем разностной характеристики. В общем случае минимально достижимое значение показателя разностной характеристики для S-блоков чётной размерности тоже неизвестно.

Линейный и разностный методы также накладывают требования на линейное преобразование XSL-схемы: показатели рассеивания соответствующей матрицы и транспонированной к ней должны быть большими, в идеале – максимальными для заданной размерности.

Существуют и другие методы анализа XSL-схем: алгебраические методы, метод разностей высшего порядка, метод инвариантных подпространств и др. В части последнего необходимо рассматривать инвариантные подпространства для преобразований S и L, а также для XSL-схемы в целом.

Общая характеристика работы: диссертация состоит из 4-х глав.

В первой главе исследуются вопросы построения нелинейных преобразований с близкими к оптимальным значениями криптографических характеристик. Автор развил метод построения нелинейных подстановок, предложенный криптографами из Китая. В результате была предложена Конструкция 1, впоследствии примененная к различным классам преобразований. Построенные подстановки обладают наилучшими из известных значениями дифференциальной равномерности и нелинейности для подстановок четной размерности.

Вторая и третья главы посвящены эффективной программной реализации линейных преобразований. Во второй главе рассматривается случай циркулянтных матриц. Показано, что двоичные циркулянтные матрицы реализуются за две команды процессора CLMUL и XOR. Для произвольных циркулянтных матриц представлено разложение в сумму произведений диагональных и двоичных циркулянтных матриц, получены верхние и нижние оценки на число слагаемых в указанном разложении. Результаты главы справедливы для матриц, используемых в шифрсистемах AES, SM4, хэш-функции Whirlpool.

В третьей главе рассматриваются рекурсивные матрицы. Для сопровождающей матрицы найдены все решения уравнения подобия для матрицы и транспонированной матрицы. На их основе получены разложения произвольной рекурсивной матрицы. Предложены новые реализации рекурсивных матриц с оценкой числа команд процессора и объема памяти, требуемых для реализации. Реализации представляют интерес для низкоресурсных устройств с ограниченным объемом памяти.

В четвертой главе изучаются инвариантные подпространства циркулянтных и рекурсивных матриц. Полностью описаны инвариантные подпространства максимально рассеивающих циркулянтных матриц размерности, равной степени двойки. Результат представляет как

теоретический, так и практический интерес в силу использования указанных матриц в шифрсистеме AES и хэш-функции Whirlpool. Для рекурсивных матриц размерности, равной степени двойки, показано отсутствие инвариантных подпространств определённого вида, согласованного с размером S-блока. Результат применим для линейного преобразования шифрсистемы Кузнечик.

Степень обоснованности положений, выносимых на защиту, научных выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна: все полученные в диссертации результаты сопровождаются строгими математическими доказательствами, представлены на конференциях и научных семинарах, опубликованы в рецензируемых научных журналах. Выносимые на защиту положения следуют из результатов, полученных в диссертации. Представленные результаты являются новыми.

Результаты других авторов, упомянутые в тексте диссертации, отмечены ссылками на соответствующие публикации.

Замечания оппонента:

1. В первой главе работы хотелось бы увидеть таблицы, где проведено сравнение параметров подстановок, построенных различными методами.
2. Вызывает трудности восприятие результатов диссертационного исследования из-за того, что нумерация строк матриц начинается снизу и знаки линейных рекуррентных последовательностей «раскручиваются» в левую сторону, что не является общепринятым подходом.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Диссертационное исследование оформлено согласно требованиям Положения о совете по защите диссертаций на соискание ученой

степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В. Ломоносова.

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

Официальный оппонент:
доктор физико-математических наук,
доцент, профессор кафедры 252
Института искусственного интеллекта РТУ МИРЭА

Камловский Олег Витальевич

05.11.2025 г.

Контактные данные:
тел.: , e-mail:

Специальность, по которой официальным оппонентом защищена диссертация: 6.4.4. Теоретическая криптография.

Адрес места работы:
119454, г. Москва, проспект Вернадского, д. 78.

Подпись руки Камловского О.В.
удостоверяю

Ведущий специалист
Управления кадров Н.Ю. Гладкая