МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М.В.ЛОМОНОСОВА

Отзыв научного руководителя на диссертацию Давыдова Степана Андреевича «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах», представленную на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Общая характеристика соискателя. Давыдов Степан Андреевич окончил Институт криптографии связи и информатики Академии ФСБ России в 2017 году. В 2023 году он поступил в очную аспирантуру факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова, имея при этом богатый научный задел по теме представленной диссертации. Обучаясь всего около года в очной аспирантуре С.А.Давыдов подготовил текст диссертации на соискание ученой степени кандидата физико-математических наук. Во время обучения С.А.Давыдов также работал по совместительству на кафедре информационной безопасности в должности математика (основное место работы АО «НПК „Криптонит"»). Работая на кафедре С.А.Давыдов активно занимался преподавательской деятельностью. Он переработал программу курса «Элементы криптографического анализа» и в настоящий момент ведет занятия по курсу. Некоторые результаты, полученные в представленной диссертации были использованы в этом курсе и читаются студентам.

Актуальность темы. Кандидатская диссертация Давыдова Степана Андреевича посвящена вопросам синтеза и анализа линейных и нелинейных преобразований, используемых в современных блоковых шифрах и хеш-функциях.

В настоящее время одними из самых популярных криптографических механизмов, которые используются на практике для защиты коммуникаций, являются блоковые шифры и хеш-функции. Блоковые шифры обеспечивают защиту конфиденциальности практически всего сетевого трафика, который передается в глобальной сети интернет. Хеш-функции же с одной стороны являются

базовым элементом многих прикладных протоколов, а с другой, могут применяться для создания других криптографических механизмов. Достаточно отметить лишь перспективную схему электронной подписи SPHINCS+, которая принимала участие в конкурсе Национального агенства стандартов и технологий США (NIST USA) на постквантовые криптографические механизмы.

Сейчас разработано достаточно много подходов к построению как блоковых шифров, так и хеш-функций. Вместе с тем, наибольшей популярностью пользуется подход, восходящий к первым рассекреченным работам Клода Шеннона, посвященным теории связи, применяемых в секретных системах. Этот подход заключается в том, чтобы при проектировании шифра или хеш-функции выбирать преобразования, обеспечивающие достаточно хорошее перемешивание символов открытого текста, а также неплохое рассеивание секретного ключа в символах шифр-текста.

Известно, что наибольшее перемешивание дают нелинейные преобразования, которые заключаются в нелинейной замене одних битов на других. Такие преобразовании в криптографии обычно обозначаются символом S (от английского слова *substitution*), а узел криптографических механизмах, реализующих это преобразование обычно называют узлом замены или Sbox.

А вот рассеивание, как правило, гарантируется как раз линейными преобразованиями, которые обычно реализуются умножением некоторого вектора, состоящего из элементов в некотором конечном поле, на подходящую квадратную матрицу с элементами в том же поле. Линейное преобразование в криптографии обычно принято обозначать символом L (от английского *linear*).

Криптографические преобразования обычно зависят от параметра, который называется ключом и обозначается символом k. Для добавления ключа в криптографическое преобразование используется обычное сложение по модулю 2 (Xor) битов раундового ключа с каким-либо внутренним промежуточным состоянием. В силу приведенных обозначений описанная схема построения криптографических преобразований получила название XSL-схема.

Архитектуру XSL-схемы имеют практически все современные шифры. Здесь стоит отметить российские шифры «Кузнечик» и «Магма», которые явля-

ются межгосударственными стандартами, а также американский стандарт шифрования AES. Похоже построены и многие современные хеш-функции.

С одной стороны, наличие стандартов достаточно жестко регламентирует необходимость применения тех или иных криптографических механизмов. Однако во многих современных сценариях, особенно из-за развития интернета вещей, имеется запрос на создание новых перспективных механизмов с учетом новых функциональных и потребительских требований и характеристик.

Так, например, в рамках интернета вещей между собой взаимодействуют устройства, которые обладают ограниченными ресурсами. В первую очередь речь идет не о вычислительных ресурсах, а об ресурсах электропитания. Для таких устройств нужны шифры, которые обладают высокой энергоэффективностью, как в процессе работы, так и в состоянии покоя. Поэтому задача синтеза криптографических механизмов, предназначенных для работы именно на таких устройствах, является достаточно важной и практической. Это подтверждает актуальность представленной диссертации в части синтеза новых механизмов.

Вместе с тем, при создании новых механизмов возникает важная проблема обоснования их криптографической стойкости.

Наиболее значимыми методами криптоанализа современных шифров являются дифференциальный и линейный методы. С помощью этих методов была понижена стойкость, например, шифра DES. Для нейтрализации атака, базирующихся на этих методах к матрице линейного преобразования предъявляются требования максимального рассеивания. На текущий момент известно некоторое количество теоретических методов построения максимально рассеивающих матриц в случае матриц произвольного вида. Но если ограничить выбор матрицы из какого-либо класса, допускающего оптимизацию программной, аппаратной реализации, то построение таких матриц становится уже сложной и обычно для важных практических случаев теоретических методов уже не известно. Например, так обстоит дело для матриц-циркулянтов.

Таким образом, задача построения «хороших» линейных преобразований с высокими показателями рассеивания является достаточно актуальной.

Методы противодействия линейному и дифференциальному криптоанализу также заключаются в правильном выборе нелинейного преобразования. Требу-

ется использовать, так называемые, почти совершенно нелинейные преобразования или APN-преобразования. Однако часто строить такие преобразования крайне сложно. Особенно вопрос усложняется при условии использования четного числа переменных (≥ 8) в нелинейном преобразовании. По этой причине актуальной является задача разработки способов построения дифференциально 4-равномерных подстановок двоичных векторных пространств четной размерности.

Для XSL-схем также разработан особый метод криптоанализа, который использует инвариантные подпространства. Если для одного раунда XSL-схемы на некоторых ключах можно построить инвариантное подпространство, то указанное подпространство окажется инвариантным и для всего механизма, основанного на этой XSL-схеме. Таким образом, задача поиска инвариантных подпространств является крайне актуальной при синтезе механизмов.

Таким образом, в диссертации Давыдова Степана Андреевича решаются актуальные и практически значимые для защиты информации задачи.

Цели и задачи. Целью диссертационной работы С.А.Давыдова является повышение обоснованности анализа XSL-схем и улучшение их эксплуатационных характеристик.

Для достижения поставленной цели решались следующие задачи:

1. Построение новых дифференциально 4-равномерных подстановок, обладающих максимально известной нелинейностью.
2. Предложить способы эффективной программной реализации линейных преобразований, заданных умножением на элемент кольца, а также рекурсивных линейных преобразований.
3. Описать алгебраическую и/или комбинаторную структуру инвариантных подпространства максимально рассеивающих матриц-циркулянтов.

Степень достижения целей и задач. В результате автором получены следующие результаты:

1. Предложена конструкция, позволяющая строить дифференциально 4-равномерные подстановки из некоторых APN-преобразований размерности на единицу большей размерности. Приведены достаточные условия

применения новой конструкции и полностью описаны степенные подстановки.

2. Предложен способ улучшения программной реализации линейных преобразований специального типа. Этот способ использует разложение произвольной матрицы в сумму произведений диагональных матриц и матриц, реализуемых через умножение на элемент кольца, имеющих эффективную реализацию. Получены верхняя и нижняя оценки на число слагаемых в указанном разложении.
3. Найдены все решения уравнения подобия для сопровождающей матрицы многочлена над конечным полем. И далее на основе этих решений построено разложение для произвольной рекурсивной матрицы, которое может быть использована для оптимизации программной реализации линейных преобразований на основе рекурсивных матриц.
4. Полностью описаны инвариантные подпространства максимально рассеивающих матриц-циркулянтов.

Таким образом, поставленные задачи полностью выполнены и цель работы достигнута.

Структура работы. Работа состоит из введения, четырех глав, заключения, одного приложения и списка литературы. Общий объем работы 96 страниц. Текст работы содержит 2 таблицы, рисунки отсутствуют. Список литературы содержит 72 источника.

Во введении работы обосновывается актуальность выбранной темы диссертации, сформулированы цели и задачи исследований.

Глава 1 посвящена построению дифференциально 4-равномерных подстановок на основе конструкции специального вида.

В главе 2 изучаются преобразования пространства двоичных векторов, заданные через умножение на элемент кольца многочленов. Рассматривается вопрос сложности их реализации системой команд процессора общего назначения. Устанавливаются значения показателей рассеивания матриц-циркулянтов для некоторых типов таких матриц. Предложен подход к реализации линейных преобразований на основе разложения этих матриц в сумме произведений диагональных матриц и матриц, заданных через умножение на элементы кольца.

Глава 3 посвящена изучению рекурсивных матриц над произвольным конечным полем. В ней предлагается подход к получению относительно легковесных рекурсивных матриц, а также метод декомпозиции таких матриц для оптимизации программных реализаций криптографических механизмов, в которых линейное преобразование использует рекурсивные матрицы.

В главе 4 изучаются инвариантные подпространства матриц-циркулянтов и рекурсивных матриц. Фактически эта глава посвящена вопросам стойкости механизмов, построенных с использованием линейных преобразований, изучаемых в главах 2 и 3 диссертации. В этой главе устанавливается теорема о структуре инвариантных подпространств линейных преобразований, заданных матрицами-циркулянтами. Это позволяет полностью их описать при выполнении некоторого условия, справедливого для любой максимально рассеивающей матрицы-циркулянта. Также в этой главе получены условия, при которых рекурсивная матрица не имеет инвариантных подпространств специального вида. В заключении диссертации сформулированы основные результаты работы и описаны сферы их возможного применения.

В приложении содержатся два примера построенных дифференциально 4-равномерных подстановок.

Оригинальность работы. Все полученные в диссертации результаты получены автором диссертации самостоятельно. В публикациях, выполненных в соавторстве, другим авторам принадлежат либо постановка задачи, либо доказательства вспомогательных утверждений.

Диссертация представляется к защите впервые.

Научная новизна. Все результаты работы являются новыми и представляют существенную научную ценность.

Практическая и теоретическая значимость. Диссертация носит в основном теоретический характер и представляет собой цельное законченное исследование.

Результаты работы значительно развивают теоретические конструкции в области синтеза булевых отображений с хорошими криптографическими свойствами, теорию циркулянтных матриц, а также общую теорию программной и

аппаратной реализации линейных преобразований, построенных на базе максимально рассеивающих матриц.

Результаты могут быть использованы при синтезе перспективных криптографических механизмов, построенных на базе XSL-схем. Кроме того, результаты могут применяться разработчиками, как программных, так и аппаратных средств криптографической защиты информации для оптимизации реализации криптографической подсистемы и увеличения пропускной способности средств защищенной обработки информации.

Достоверность положений. Достоверность полученных результатов подтверждается строгими математическими доказательствами, приведенными в тексте диссертации, а также программной реализацией предложенных методов. Доказательства существенно используют методы теории булевых отображений, методы дискретной математики, комбинаторики и линейной алгебры.

Основные результаты, полученные в диссертации, излагались на международных и всероссийских конференциях и научно-исследовательских семинарах, и опубликованы в печатных рецензируемых научных журналах.

Вывод. Диссертация Давыдова Степана Андреевича «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах» соответствует паспорту специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки): полученные в ней результаты соотносятся с разделами 11 «Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты», 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности», 19 «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов».

Считаю, что диссертационная работа Давыдова Степана Андреевича «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах» удовлетворяет всем требованиям «Положения о

присуждении ученых степеней в МГУ имени М.В. Ломоносова» и рекомендую ее к защите в диссертационном совете МГУ.012.3 на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Научный руководитель:
доцент кафедры информационной
безопасности факультета
ВМК МГУ имени М.В.Ломоносова,
канд. физ.-мат. наук И.В. Чижов

17.02.2025

Контактные данные.

ФИО: Чижов Иван Владимирович.

Ученая степень: кандидат физико-математических наук.

E-mail: chizhoviv@my.msu.ru, тел.: 8(495)930-43-76 (раб.).

Специальность, по которой И.В. Чижовым была защищена кандидатская диссертация: 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Адрес места работы: 119234, Москва, Ленинские горы, дом 1, стр. 52, МГУ имени М.В. Ломоносова, 2-й учебный корпус, факультет ВМК, кафедра информационной безопасности.

Должность: доцент кафедры информационной безопасности.

Подпись Чижова Ивана Владимировича удостоверяю:

Декан факультета ВМК МГУ имени
М.В. Ломоносова,
академик И.А. Соколов