МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

На правах рукописи

Давыдов Степан Андреевич

Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах

Специальность 2.3.6 —
«Методы и системы защиты информации, информационная безопасность»

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
кандидат физико-математических наук
Чижов Иван Владимирович

Москва — 2025

Оглавление

Стр.

Введение 4

Обозначения, определения и общие сведения 22

Глава 1. Построение дифференциально 4-равномерных подстановок 30

1.1 Криптографические характеристики S-блоков 31

1.2 Развитие подхода к синтезу дифференциально 4-равномерных подстановок 33

Глава 2. Линейные преобразования, заданные умножением на элемент кольца 40

2.1 Линейные преобразования, заданные умножением на элемент кольца над $\mathbb{F}_2$ 40

2.2 Разложение матрицы в сумму матриц вида $A_{a(x),f(x)}$ 45

2.3 Разложение матриц-циркулянтов над полем $\mathbb{F}_{2^s}$ 47

Глава 3. Разложение рекурсивных матриц 51

3.1 Линейные преобразования, заданные через умножение на элемент кольца 52

3.2 Выбор матрицы перехода C в уравнении подобия рекурсивной матрицы 54

3.3 Разложение рекурсивных матриц 58

3.4 Реализации рекурсивных матриц 59

3.4.1 Известные реализации 59

3.4.2 Реализация через разложение рекурсивной матрицы . . . 60

3.4.3 Реализация через умножение на элемент кольца (поля) . . 61

3.4.4 Новые максимально рассеивающие преобразования 62

3.5 Сравнение реализаций шифрсистемы Кузнечик 62

Глава 4. Инвариантные подпространства матриц-циркулянтов и рекурсивных матриц 65

4.1 Основные определения и обозначения 66

Стр.

4.2 Подпространства, инвариантные относительно нелинейных преобразований $\overline{S}$ 68
4.3 Приведение матрицы-циркулянта к верхнетреугольному виду . . 73
4.4 Описание инвариантных подпространств одного класса матриц-циркулянтов 78
4.5 Инвариантные подпространства рекурсивных матриц 81
4.6 Инвариантные подпространства матриц, подобных рекурсивным 84

Заключение 86

Список литературы 88

Приложение А. Построенные дифференциально 4-равномерные подстановки 96

Введение

Актуальность темы.

Диссертация представляет результаты исследований в области математических проблем информационной безопасности. Работа посвящена задачам синтеза и анализа линейных и нелинейных преобразований, используемых в XSL-схемах. XSL-схемы являются одним из основных способов построения блочных шифрсистем и функций хэширования, используемых в криптографии.

Блочные шифрсистемы являются основным механизмом обеспечения конфиденциальности данных. Ещё в 70-е годы XX века американской компанией IBM был разработан алгоритм шифрования DES [1], утверждённый в 1977 г. правительством США как стандарт шифрования и использовавшийся до 2005 года. В 1989 г. в Советском Союзе был опубликован государственный стандарт шифрования ГОСТ 28147-89, стандартизированный в Российской Федерации как алгоритм Магма [2]. На сегодняшний день также используются такие алгоритмы блочного шифрования, как американский стандарт AES [3], российский стандарт Кузнечик [2], китайский стандарт SM4 [4] и др. Каждый из вышеперечисленных алгоритмов шифрования построен на основе XSL-схемы.

Существуют также более специфические задачи, основной составной частью которых являются блочные шифры, такие как вычисление имитовставки (режим CMAC [5]), аутентифицированное шифрование с дополнительными данными (режимы GCM [6], MGM [7]), алгоритм вычисления аутентификационных векторов в сетях мобильной связи MILENAGE [8], основанный на шифрсистеме AES, и т.д.

Среди функций хэширования, построенных на основе XSL-схем, можно выделить российский стандарт Стрибог [9], международные стандарты организации ISO PHOTON [10] и Whirlpool [11]. Функции хэширования используются при вычислении контрольных сумм и имитовставок (HMAC [12]), при хранении и проверке паролей, при генерации и проверке электронных подписей, разработке постквантовых электронных подписей (финалист конкурса NIST алгоритм SPHINCS+ [13]), вычислении аутентификационных векторов в сетях мобильной связи (алгоритм S3G [14], основанный на хэш-функции Стрибог) и др.

Несмотря на большое количество разработанных криптографических алгоритмов на основе XSL-схем, следующие вопросы, связанные с синтезом

преобразований, анализом и эффективной реализацией алгоритмов по-прежнему остаются актуальными:

1. Вопрос существования дифференциально 2-равномерных подстановок $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ для чётных $s \geqslant 8$ [15] . Данный показатель является оптимальным для защиты от разностного метода криптоанализа [16].
2. Вопрос существования подстановок $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ с нелинейностью, большей чем $2^{s-1} - 2^{\frac{s}{2}}$ для чётных s [15] . Данный показатель является важным для защиты от линейного метода криптоанализа [17].
3. Вопросы построения эффективно реализуемых линейных преобразований с высокими показателями рассеивания. В частности, не известны методы построения максимально рассеивающих циркулянтных матриц произвольной размерности [18]. Показатель рассеивания линейного преобразования важен для защиты от разностного и линейного методов криптоанализа.
4. Вопросы эффективных низкоресурсных реализаций существующих стандартизированных алгоритмов на основе XSL-схем.
5. Вопросы стойкости алгоритмов на основе XSL-схем к новым методам криптоанализа. Например, к методу анализа на основе инвариантных подпространств, предложенному в 2011 году [19].

Тема, объект и предмет исследований диссертации соответствуют паспорту научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) по следующим областям исследований:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

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.

История развития тематики и текущее состояние вопроса.

Идея использования XSL-схем основана на принципах Клода Шеннона из работы «Communication Theory of Secrecy Systems» [20]. В данной работе Шеннон постулирует, что используемые в шифрсистемах преобразования должны обеспечивать перемешивание и рассеивание поступающих на вход данных. Для обеспечивания перемешивания используются параллельно применяемые нелинейные преобразования $S = (S_{m-1},...,S_0), S_i$ — S-блоки, для обеспечения рассеивания используется линейное преобразование L. Помимо указанных преобразований в каждом раунде происходит наложение раундового ключа K операцией XOR для внесения энтропии в обрабатываемые данные. Таким образом возникла концепция XSL-схем. В литературе также встречаются такие названия как SP-сеть (линейное преобразование является перестановкой бит P), LSX-схема и XSPL-схема (линейное преобразование является композицией преобразования сдвига P и параллельно применяемых линейных преобразований L над меньшими блоками). Нетрудно видеть, что каждая из упомянутых выше схем является XSL-схемой, в диссертации будем придерживаться данного термина.

Отметим, что отказ от какого-либо из преобразований приведёт к потере некоторых важных криптографических или эксплуатационных свойств. Так, при отказе от нелинейных преобразований S один раунд схемы (как следствие, вся схема) вырождается в линейную функцию и восстановление секретных параметров сводится к решению системы линейных уравнений, что не представляет большой сложности. Отказ от линейного преобразования и замена его общим нелинейным приведёт к возрастанию эксплуатационных затрат на шифрование, что также является весьма существенным при разработке криптографических алгоритмов.

Концепции построения XSL-схем со временем незначительно менялись. В первых XSL-шифрах DES и Магма использовались различные S-блоки S_i, более того, в Магме 1989 г. S_i были секретными и определялись используемым ключом. Современные XSL-алгоритмы используют одинаковые S-блоки, что не понижает стойкость, но повышает эксплуатационные характеристики и упрощает анализ схемы. В DES в рамках раунда использовалось расширение входного блока, в Магме наложение ключа выполняется модульным сложением вместо XOR. Указанные операции сейчас также практически не используются при построении алгоритмов.

Одной из новых концепций в XSL-схемах является использование дополнительных несекретных параметров tweak [21], что позволяет проектировать режим шифрования на уровне блочного шифра.

Постоянно совершенствуются и методы анализа алгоритмов на основе XSL-схем. Наиболее значимыми методами являются разностный [16] и линейный [17], [22] методы криптоанализа. С помощью данных методов были построены атаки на алгоритм DES, требующие, однако, существенного объёма открытых текстов/шифртекстов. Для защиты от указанных методов к линейным преобразованиям предъявляются требования высокого показателя рассеивания матрицы и транспонированной матрицы линейного преобразования, а также обратных им матриц. Оптимальным в данном контексте является использование максимально рассеивающих матриц. На текущий момент известно (см. [18]) несколько теоретических методов построения максимально рассеивающих матриц над полями $GF(2^s)$ с использованием матриц Коши (хэш-функция Стрибог [9]), матриц Вандермонда, рекурсивных матриц (шифрсистема Кузнечик [2], хэш-функция PHOTON [10]), матриц Адамара (шифрсистема Khazad [23]) и др.

Другой подход к построению максимально рассеивающих матриц состоит в использовании переборных методов на множестве матриц определённого класса. За счёт особенностей строения матриц-циркулянтов переборные методы среди них работают эффективнее, чем в общем случае [18]. Максимально рассеивающие матрицы-циркулянты используются в шифрсистеме AES [3], шифрсистеме SM4 [4], хэш-функции Whirlpool [11]. Для матриц-циркулянтов не известны теоретические методы построения максимально рассеивающих матриц произвольной размерности.

Недостаток использования максимально рассеивающих матриц заключается в том, что их реализации требуют существенной трудоёмкости. Компромиссным вариантом является использование линейных преобразований с меньшим показателем рассеивания, при этом число раундов алгоритма необходимо увеличить для сохранения криптографической стойкости к разностному и линейному методам криптоанализа. Примерами такого подхода являются современные низкоресурсные блочные шифрсистемы PRESENT [24], Midori [25], SKINNY [26], QARMAv2 [27]. Задача построения низкоресурсных линейных преобразований с высокими показателями рассеивания остаётся актуальной на сегодняшний день.

Нелинейные преобразования S заключаются в параллельном применении S-блоков к векторам небольшой размерности $s \in \{4, 6, 8\}$. Основными криптографическими характеристиками S-блоков, характеризующими их стойкость к разностному и линейному методам криптоанализа являются дифференциальная равномерность и нелинейность. Алгебраическая степень характеризует стойкость к атаке на основе разностей высших порядков [28]. Графовая алгебраическая иммунность характеризует стойкость к алгебраическим методам, например, к XSL-методу [29].

К настоящему времени известен ряд методов построения дифференциально 2-равномерных преобразований (почти совершенных нелинейных, almost perfect nonlinear, далее — APN) $S : V_s \longrightarrow V_s$ при нечётных $s = 2k+1$ (см. [15]). При $s = 6$ известна единственная с точностью до CCZ-эквивалентности APN-подстановка Дж. Диллона и др. [30]. При $s = 4$ APN-подстановок не существует. Вопрос о существовании APN-подстановок при чётных $s \geqslant 8$ является сложной нерешённой задачей. В этой связи актуальной является задача разработки способов построения дифференциально 4-равномерных подстановок двоичных векторных пространств чётной размерности $s = 2k$. К настоящему времени известен ряд подходов к решению данной задачи, см. [15], [31—40]. В работе [33] предлагается использовать подстановки вида $F(x) + f(x)\boldsymbol{\gamma}$, где $F(x)$ — известная дифференциально 4-равномерная подстановка, $f(x)$ — булева функция, $\boldsymbol{\gamma}$ — элемент поля $\mathbb{F}_{2^{2k}}$. В работе [36] предлагается использовать подстановки вида $I \cdot \boldsymbol{\pi}$ и $\boldsymbol{\pi} \cdot I$, где I — подстановка обращения элементов поля $\mathbb{F}_{2^{2k}}$, $\boldsymbol{\pi}$ — специальным образом подбираемая подстановка со сравнительно небольшим числом мобильных точек. В [38] применяются эвристические методы построения подстановок, в [39] изучаются кусочно-мономиальные подстановки. В результате применения эвристических методов на множестве кусочно-мономиальных подстановок построена дифференциально 4-равномерная подстановка с графовой алгебраической иммунностью 3 [40].

Другим методом анализа XSL-схем является метод, использующий инвариантные подпространства. Если для одного раунда XSL-схемы на некоторых, называемых слабыми, ключах удаётся построить инвариантное подпространство, указанное подпространство будет инвариантным и для всего алгоритма, построенного на основе данной XSL-схемы. Используя свойство инвариантности подпространств, можно определить принадлежность ключа множеству слабых

ключей шифрсистемы. При небольшой мощности указанного множества найти искомый ключ можно полным перебором.

Метод был предложен для атаки на низкоресурсную шифрсистему PRINT на конференции CRYPTO 2011 [19]. Развивая идею работы [19], в [41] авторы предложили вероятностный алгоритм для поиска инвариантных подпространств. Применяя данный алгоритм, авторы нашли инвариантные подпространства у раундовых преобразований шифрсистем Robin [42] и ZORRO [43]. В каждом из случаев авторам удалось построить практическую атаку и подтвердить её успешность на референсной реализации алгоритмов. В [44], используя инвариантные подпространства матрицы линейного преобразования, авторы провели атаку на низкоресурсный блочный шифр Midori64 [25]. Мощность множества слабых ключей составила 2^{32} при 128-битном ключе. В [45] были предложены различные атаки на 5 и 6 раундов 8-раундовой шифрсистемы Khazad [23]. Авторы использовали инвариантные подпространства матрицы линейного преобразования, в качестве которой используется матрица Адамара. В [46] авторы описали инвариантные подпространства матриц Адамара над конечным полем, а также нашли класс инвариантных подпространств для матриц-циркулянтов.

Авторы работы [47] на конференции ASIACRYPT 2016 предложили метод нелинейных инвариантов, обобщающий метод инвариантных подпространств. Были предложены атаки на схемы аутентифицированного шифрования SCREAM [48] и iSCREAM, а также на шифрсистему Midori64. Для последней было построено множество слабых ключей мощности 2^{64}, что существенно больше, чем в [44]. В [49] предложено рассматривать нелинейные инварианты более общего вида и показано отсутствие таких инвариантов для раундовых преобразований алгоритмов шифрования Кузнечик [2], Present, GIFT, AES [3], LED, Anubis. В [50] для шифрсистемы Кузнечик показано отсутствие нелинейных инвариантов на множествах вида $A_1 \times ... \times A_{16}$, где A_i — собственное подмножество V_8.

Работы [47], [49] демонстрируют, что изучение нелинейных инвариантов раундового преобразования является более перспективным для криптоанализа. Тем не менее, изучение инвариантных подпространств непосредственно матрицы линейного преобразования представляет интерес, поскольку некоторые подпространства всегда сохраняются S-блоками (см. раздел 4.2). В таком случае найденные инвариантные подпространства линейного преобразования

будут одновременно являться и нелинейными инвариантами раундовой функции (см., например, [45]).

Отметим, что полное описание инвариантных подпространств (нелинейных инвариантов) даже для одного раунда шифрсистемы представляется достаточно сложной задачей. В процитированных выше работах авторы изучали подпространства определённого вида и делали вывод о применимости (или неприменимости) метода с использованием только рассматриваемых подпространств или нелинейных инвариантов.

Вклад автора диссертации. В настоящей диссертации исследуются различные вопросы, связанные с XSL-схемами. В первой главе развивается подход к построению нелинейных преобразований S, применявшийся ранее в работах [34], [37] и заключающийся в ограничении квадратичных APN-подстановок пространства V_{2k+1} на подпространство размерности $2k$ с сохранением высоких показателей дифференциальной равномерности и нелинейности. Развивая указанный подход, автору диссертации удалось построить класс подстановок произвольных чётных размерностей с оптимальными значениями криптографических показателей (дифференциальной равномерностью и нелинейностью) для защиты от линейного и разностного методов криптоанализа.

Во второй главе изучаются эксплуатационные характеристики линейных преобразований L, заданных матрицами-циркулянтами. Такие матрицы используются в шифрсистемах AES, SM4, а также в хэш-функции Whirlpool. Для указанных матриц найдены разложения, позволяющие использовать эффективные программные реализации.

В третьей главе изучаются эксплуатационные характеристики линейных преобразований L, заданных рекурсивными матрицами. Такие матрицы используются в российском стандарте блочного шифрования Кузнечик, а также в хэш-функции PHOTON. Для произвольной рекурсивной матрицы найдены разложения, позволяющее использовать эффективные программные реализации. Результаты тестирования указанных реализаций шифрсистемы Кузнечик приведены в диссертации.

В четвёртой главе изучаются инвариантные подпространства линейных преобразований, заданных матрицами-циркулянтами и рекурсивными матрицами. Развивая идеи работы [46], автору диссертации удалось полностью описать инвариантные подпространства матриц-циркулянтов определённого вида и найти вторую нормальную форму таких матриц. В частности, результаты

справедливы для любой максимально рассеивающей матрицы-циркулянта. Для рекурсивных матриц представлены достаточные условия, при которых матрица не имеет инвариантных подпространств определённого вида, согласованного с размером S-блока. Указанные результаты показывают невозможность применения метода инвариантных подпространств в рассматриваемой конфигурации к шифрсистемам AES, Кузнечик и хэш-функциям PHOTON, Whirlpool.

Целью работы является повышение обоснованности анализа XSL-схем и улучшение их эксплуатационных характеристик. В рамках достижения цели S и L преобразования исследуются как по отдельности, так и в единой схеме.

Для достижения поставленной цели необходимо решить следующие **задачи**.

1. Предложить методы построения дифференциально 2 или 4-равномерных подстановок в пространствах чётных размерностей, обладающих высокими показателями нелинейности, алгебраической степени, степени нелинейности и графовой алгебраической иммунности.
2. Предложить методы построения эффективно реализуемых линейных преобразований с относительно высокими показателями рассеивания.
3. Предложить низкоресурсные реализации для наиболее важных практически классов матриц: циркулянтов, двоичных циркулянтов, рекурсивных матриц, используемых в линейных преобразованиях шифрсистем Кузнечик, AES и SM4 и хэш-функций PHOTON и Whirlpool.
4. Найти инвариантные подпространства преобразования, заданного параллельным применением одинаковых S-блоков, линейных циркулянтных и рекурсивных преобразований. Наиболее важен случай максимально рассеивающих матриц, использующихся во всех перечисленных выше алгоритмах шифрования и хэширования.

Основные положения, выносимые на защиту: на защиту выносятся обоснование актуальности решаемой задачи, методология, принятая для исследования, научная новизна, теоретическая и практическая значимости работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в диссертации.

1. *Конструкция 1*, позволяющая строить преобразования пространств размерности s путём ограничения преобразований пространств размерности $s+1$ на некоторую гиперплоскость.

2. Теорема 1.2 о дифференциальной 4-равномерности подстановок, построенных при помощи *Конструкции 1*. Теорема 1.5 об описании степенных подстановок, к которым применима *Конструкция 1*. Теорема 1.6 о применимости *Конструкции 1* к дифференциально 2-равномерным преобразованиям определённого вида, с построением дифференциально 4-равномерных подстановок с максимально известной нелинейностью.
3. Теорема 2.1 о минимальном числе слагаемых в разложении матрицы в сумму произведений диагональных матриц и матриц, реализуемых через умножение на элемент кольца.
4. Теорема 3.1 об описании всех решений уравнения подобия для сопровождающей матрицы. Теорема 3.2 о разложении произвольной рекурсивной матрицы в произведение двух матриц, имеющих эффективную реализацию.
5. Предложены к рассмотрению и описаны подпространства *вида 1*, инвариантные относительно нелинейного преобразования $\overline{S} = (S,S,...,S)$, заключающегося в параллельном применении одинаковых S-блоков S.
6. Теорема 4.1 о подобии матрицы-циркулянта верхнетреугольной матрице Тёплица. Теорема 4.2 об описании инвариантных подпространств матрицы-циркулянта при определённом условии и следствие 4.2 о выполнимости указанных условий для максимально рассеивающих матриц-циркулянтов. Теорема 4.3 об отсутствии инвариантных подпространств *вида 1* у рекурсивных матриц при определённом условии.

Научная новизна: в диссертации получены следующие новые результаты.

1. Предложена *Конструкция 1*, позволяющая строить дифференциально 4-равномерные подстановки размерности s из некоторых APN-преобразований размерности $s + 1$. Доказана теорема о дифференциальной равномерности построенных подстановок. Приведены достаточные условия применимости *Конструкции 1* и полностью описаны степенные подстановки, к которым данная конструкция применима. Представлен класс APN-преобразований, позволяющий с использованием *Конструкции 1* строить дифференциально 4-равномерные подстановки с максимально известной нелинейностью.

2. Предложено 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. На основе указанных решений получены разложения для произвольной рекурсивной матрицы.
4. Полностью описаны инвариантные подпространства максимально рассеивающих матриц-циркулянтов. Показано отсутствие инвариантных подпространств *вида 1* для рекурсивных матриц, характеристический многочлен которых не имеет кратных корней в поле разложения.

Теоретическая значимость работы заключается в развитии существующей теории по выбранным направлениям исследований. Результаты могут быть использованы в задаче синтеза нелинейных подстановок (S-блоков) с низкими показателями дифференциальной равномерности, при изучении криптографических свойств рекурсивных и циркулянтных матриц.

Результаты также могут быть использованы в развитии метода криптоанализа на основе инвариантных подпространств.

Практическая значимость заключается в возможности использовать результаты диссертации для синтеза, эффективной реализации и обоснования стойкости блочных шифрсистем и функций хэширования.

Реализация циркулянтной матрицы через умножение на элемент кольца может быть использована в разработке эффективной программной реализации шифрсистемы SM4. Разложения линейных рекурсивных преобразований могут быть использованы для низкоресурсных реализаций шифрсистемы Кузнечик и хэш-функции PHOTON.

Результаты о единственном классе инвариантных подпространств матриц-циркулянтов и об отсутствии инвариантных подпространств согласованного с размером S-блока *вида 1* у рекурсивных матриц могут быть использованы в обосновании невозможности применения метода анализа на основе инвариантных подпространств в определённой конфигурации к шифрсистемам AES и Кузнечик, а также хэш-функциям Whirlpool и PHOTON.

Методология и методы исследования. В рамках диссертационного исследования применяются математические методы из алгебры, теории чисел, теории булевых и векторных булевых функций.

Достоверность. Все полученные в диссертации результаты сопровождаются строгими математическими доказательствами, представлены на конференциях и научных семинарах, опубликованы в рецензируемых научных журналах.

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

Апробация работы. Основные результаты работы докладывались на международных конференциях:

- XXIII Международной научно-практической конференции «РусКрипто'2021», Солнечногорск, 23–26 марта 2021 года.
- XXIV Международной научно-практической конференции «РусКрипто'2022», Солнечногорск, 22–25 марта 2022 года.
- XII симпозиуме «Современные тенденции в криптографии» (CTCrypt 2023), Волгоград, 6–9 июня 2023 года.
- XIII симпозиуме «Современные тенденции в криптографии» (CTCrypt 2024), Петрозаводск, 3–6 июня 2024 года.

А также на научных семинарах:

- Специальном семинаре под руководством кандидата физико-математических наук Чижова И.В. 4 марта 2025 года.
- На семинаре кафедры информационной безопасности 6 марта 2025 года.

Объем и структура работы. Диссертация состоит из введения, 4 глав, заключения и 1 приложения. Полный объём диссертации составляет 96 страниц, включая 2 таблицы, без рисунков. Список литературы содержит 72 наименования.

Публикации. Основные результаты по теме диссертации изложены в 4 печатных изданиях общим объемом 3.4375 п.л. в журналах, рекомендованных ВАК Минобрнауки России. Из них 3, общим объемом 2.875 п.л., — в изданиях, индексируемых в Web of Science, Scopus, RSCI, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Статьи в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова.

[69] С. А. Давыдов, И. А. Круглов. Метод синтеза дифференциально 4-равномерных подстановок пространства V_m для четных m // Дискрет. матем. —

2019. — Т. 31, № 2. — С. 69—76. — (0.5 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.220) // Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%, 0.465 п.л., EDN: ZJDZIL.

[70] С. А. Давыдов, Ю. Д. Шкуратов. Использование матриц-циркулянтов над $\mathbb{F}_2$ при построении эффективных линейных преобразований с высокими показателями рассеивания // Матем. вопр. криптогр. — 2024. — Т. 15, № 2. — С. 29—46. — (1.125 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.143) // Соавтору принадлежат лемма 1 и теорема 2. Остальные результаты получены Давыдовым С.А. – 86%, 0.9675 п.л., EDN: WYZJQK.

[71] С. А. Давыдов. Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц // Дискрет. матем. — 2024. — Т. 36, № 4. — С. 44—63. — (1.25 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.220) – 100%, EDN: YWWKFP.

Другие публикации автора по теме диссертации.

[72] С. А. Давыдов, В. А. Шишкин. Способы разложения рекурсивных матриц и их применение к реализации линейных преобразований // International Journal of Open Information Technologies. — 2023. — Т. 11, № 7. — С. 30—38. — (0.5625 п.л., ВАК, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.492) // Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%, 0.534 п.л., EDN: EVYWMG.

Содержание работы

Во **введении** обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В разделе **обозначения, определения и общие сведения** приводятся используемые в работе обозначения, общие для всей работы и ключевые определения: XSL-схемы, дифференциальной равномерности преобразования, максимально рассеивающих, циркулянтных и рекурсивных матриц. Приводится разбиение двоичного вектора на s-подвекторы и связь результатов, справедливых для векторов, состоящих из двоичных s-подвекторов и из элементов поля $\mathbb{F}_{2^s}$.

Определения и обозначения, актуальные только в конкретной главе приводятся в соответствующей главе.

Глава 1 посвящена построению дифференциально 4-равномерных подстановок с использованием *Конструкции 1*, являющейся обобщением метода построения подстановок, предложенного в теореме 2 работы [37]. Метод заключается в ограничении значений известных APN-преобразований пространства V_{s+1} на некоторую гиперплоскость, представимую как пространство V_s. *Конструкция 1* основана на введённых автором диссертации подмножествах, порождающих простое разбиение. Любая гиперплоскость, в том числе гиперплоскость, используемая в работе [37], является подмножеством, порождающим простое разбиение. Авторы работы [37] для построения использовали квадратичные APN-подстановки, в то время как *Конструкция 1* допускает использование APN-преобразований любой алгебраической степени. Теоретически и экспериментально подтверждается, что каждое из вышеупомянутых обобщений является существенным, то есть расширяет множество преобразований, пригодных для построения дифференциально 4-равномерных подстановок рассматриваемым способом.

В начале **главы 1** приводятся определения изучаемых криптографических характеристик S-блоков: алгебраической степени, степени нелинейности, нелинейности и графовой алгебраической иммунности. Далее вводится понятие подмножества, порождающего простое разбиение, формулируются утверждение о его эквивалентных определениях и определяется *Конструкция 1*.

В теореме 1.2 формулируется основной результат: полученное в соответствии с *Конструкцией 1* преобразование является дифференциально 4-равномерной подстановкой. В соответствии с замечанием 1.4, в случае использования в *Конструкции 1* почти бент преобразований в V_{2s+1} нелинейность полученной подстановки будет максимальной из всех известных значений нелинейности для подстановок в V_{2s}.

Теорема 1.4 показывает эквивалентные условия, при которых возможно применение *Конструкции 1*. Условие *(b)* удобно проверять экспериментально. Условие *(c)* будет использовано в доказательстве следствия 1.1, в котором показано, что *Конструкцию 1* можно применять к APN-подстановкам, обратным квадратичным, таким образом конструкция является обобщением метода из работы [37].

Теорема 1.5 даёт полное описание степенных подстановок, допускающих применение *Конструкции 1*. С учётом следствия 1.1 достаточно показать, что к неквадратичным степенным подстановкам *Конструкция 1* неприменима. При-

мер 1.1 показывает возможность применения *Конструкции 1* к подстановке, обратная подстановка к которой не является квадратичной.

Теорема 1.6 показывает возможность применения *Конструкции 1* к классу кубических APN-преобразований, не являющихся подстановками. Построенные дифференциально 4-равномерные подстановки в соответствии с замечанием 1.4 обладают максимально известной нелинейностью среди подстановок на множестве V_{2s}. Построенная с использованием теоремы 1.6 подстановка в V_8 имеет следующие криптографические параметры: дифференциальная равномерность 4, алгебраическая степень 3, степень нелинейности 3, нелинейность 112, графовая алгебраическая иммунность 2. Параметры обратной подстановки: дифференциальная равномерность 4, алгебраическая степень 5, степень нелинейности 5, нелинейность 112, графовая алгебраическая иммунность 2. Указанные подстановки приведены в приложении А.

Глава 2 посвящена изучению преобразований, заданных через умножение на элемент кольца многочленов. Такие преобразования могут иметь эффективную программную реализацию, поскольку умножение многочленов реализуется одной командой процессора CLMUL [55]. Для получения результата линейного преобразования остаётся выполнить приведение по модулю, сложность которого зависит от многочлена модуля. В утверждении 2.2 представлены случаи, когда приведение по модулю требует небольшого числа команд процессора и минимального объёма памяти.

Наиболее эффективным оказывается случай $f(x) = x^n + 1$, который задаёт кольцо матриц-циркулянтов над полем $\mathbb{F}_2$. Реализация матрицы-циркулянта может быть выполнена за две команды процессора CLMUL и XOR, а в памяти необходимо хранить лишь одну строку длины n бит, где n — размер блока, обрабатываемого линейным преобразованием. Двоичная матрица-циркулянт используется в китайском стандарте шифрования SM4. В утверждении 2.3 приведены другие свойства двоичных матриц-циркулянтов. Показатель рассеивания транспонированной матрицы-циркулянта совпадает с показателем рассеивания исходной, что важно для защиты от линейного метода криптоанализа [22].

Однако теоретических методов построния максимально рассеивающих матриц-циркулянтов автору не известно. Переборные методы также не позволяют найти максимально рассеивающие матрицы-циркулянты (как и матрицы, заданные через умножение на элемент кольца) над полем $\mathbb{F}_2$ большего разме-

ра, чем 32×32, см. таблицу 1. В связи с этим предлагается к рассмотрению новый подход: выбирать известные максимально рассеивающие матрицы и раскладывать их в сумму произведений диагональных матриц и матриц, заданных через умножение на элемент кольца (см. формулу (2.3)). В утверждении 2.4 оценивается число команд процессора, требуемое для реализации матрицы через указанное разложение. Число команд прямо пропорционально количеству слагаемых. Минимальное число слагаемых в разложении при заданном многочлене-модуле позволяет найти теорема 2.1. Простота формулировки и реализации позволяет использовать указанную теорему как для практической проверки матриц, так и для получения теоретических результатов о разложении определённых классов матриц, что показано в следующем разделе 2.3.

Для матриц-циркулянтов над $\mathbb{F}_{2^s}$ минимальное количество слагаемых в разложении (2.3) при многочлене модуле $x^n + 1$ не превосходит s, что показано в утверждении 2.5. В некоторых частных случаях, например для матриц, используемых в линейных преобразованиях шифрсистемы AES и хэш-функции Whirlpool, число слагаемых может быть ещё меньше за счёт выбора элементов матрицы-циркулянта. Соответствующие разложения из двух слагаемых для матрицы AES и четырёх слагаемых для матрицы Whirlpool приведены в примерах 2.3 и 2.1 соответственно.

Стоит отметить, что скорость выполнения команд процессора разная [55], и количество команд в разложении не является метрикой скорости линейных преобразований в программной реализации. Тем не менее, небольшое число команд даёт основание предполагать существование эффективной программной реализации. Для получения точных результатов необходимо проведение экспериментов.

Глава 3 посвящена изучению рекурсивных матриц над произвольным конечным полем $\mathbb{F}_{q^s}$. В начале главы показано, что транспонированная сопровождающая матрица $S^\top = S(f(x))^\top$, также как и матрица-циркулянт, задаётся через умножение на элемент кольца (пример 3.2). Это означает, что в определённом базисе сопровождающая матрица $S(f(x))$ и рекурсивная матрица S^m тоже задаются через умножение на элемент кольца и могут быть реализованы в три этапа:

1. переход в соответствующий базис;
2. умножение на элемент кольца;
3. возврат в исходный базис.

Для эффективной программной реализации рекурсивной матрицы необходимо, чтобы матрицы перехода и возврата в исходный в базисы были эффективно реализуемы программно. Нахождению соответствующих матриц и их эффективных реализаций посвящена настоящая глава.

В теореме 3.1 приводится полное описание решений уравнения подобия для матриц $S(f(x))$ и $S(f(x))^\top$. Все решения имеют взаимно однозначное соответствие с множеством линейных рекуррентных последовательностей (далее — ЛРП) с характеристическим многочленом $f(x)$. Таким образом, задать матрицу подобия можно через отрезок из m подряд идущих элементов ЛРП, где m — степень многочлена $f(x)$. В утверждениях 3.2 и 3.3 приведены два способа выбора отрезков ЛРП, позволяющих получать эффективно реализуемые матрицы перехода C и C^{-1}. На основе утверждения 3.3 в теореме 3.2 приведено разложение рекурсивной матрицы, полученное перемножением C^{-1} и $(S^\top)^m$ в уравнении $S^m = C^{-1}(S^\top)^m C$. Соответствующее разложение состоит из двух эффективно реализуемых матриц F и C. Частный случай соответствующего разложения для рекурсивной матрицы линейного преобразования шифрсистемы Кузнечик был получен в работе [53].

В разделе 3.4 приведены известные и предложены новые реализации рекурсивных матриц. Известная реализация с использованием предвычисленных LUT-таблиц является самой быстрой на процессорах с достаточным объёмом кэш-памяти. Предвычисленные таблицы содержат $m^2 2^s$ элементов поля и для шифрсистемы со 128-битным блоком и 8-битными S-блоками занимают 64 Кбайта памяти. В условиях отсутствия достаточного объёма памяти (быстродоступной памяти) на вычислителе возникает необходимость в низкоресурсных реализациях. Разложения рекурсивной матрицы из теоремы 3.2 и утверждения 3.2 позволяют предложить новые реализации, представленные в пунктах 3.4.2 и 3.4.3 соответственно. Реализация 3.4.2 позволяет сократить объём памяти в $m/2$ раз по сравнению с LUT-таблицами. Преимуществом представленных разложений является возможность объединить преобразования S и L в предвычисленных таблицах, то есть для хранения и реализации S-блока не требуются вычисления и дополнительная память.

В таблице 2 представлено сравнение параметров и скорости различных реализаций шифрсистемы Кузнечик, выполненных на языке программирования C++. Второй и третий столбцы содержат полученные теоретически оценки памяти и трудоёмкости. Результаты скорости шифрования во многом согласуются

с полученными оценками и позволяют предположить, что на вычислителях с небольшим объёмом быстродоступной памяти реализация 4, основанная на теореме 3.2 о разложении рекурсивной матрицы, будет наиболее эффективной.

Реализация 5 рекурсивной матрицы (см. 3.4.3) помимо преобразования, заданного через умножение на элемент кольца $(S^\top)^m$, использует матрицы перехода C^{-1} и C. В случае максимально рассеивающей рекурсивной матрицы S^m преобразование $(S^\top)^m$ также является максимально рассеивающим преобразованием и может применяться в качестве линейного преобразования в XSL-схемах, см. пункт 3.4.4. Скорость его работы будет, очевидно, быстрее, чем скорость работы линейного преобразования в реализации 5. Требуемая память будет в два раза меньше, чем в реализации 4 и в m раз меньше по сравнению с LUT-таблицами, что может быть важно в случае реализации алгоритмов на малоресурсных устройствах. Недостатком указанного преобразования является невозможность объединения таблиц вычисления преобразований S и L в одну таблицу, то есть для преобразования $L = (S^\top)^m$ дополнительно требуется реализация S-блока и хранение соответствующей таблицы в памяти. На ядре процессора Intel Core i5-8265U реализация XSL-схемы с линейным преобразованием $(S^\top)^m$ работает в два раза медленнее, чем реализация 4.

В **главе 4** изучаются инвариантные подпространства матриц-циркулянтов и рекурсивных матриц. Наиболее распространён случай использования нелинейного преобразования S, как параллельного применения одинаковых S-блоков. В таком случае можно выделить класс подпространств, инвариантных относительно преобразования S независимо от выбора S-блока. Раздел 4.2 содержит вспомогательные результаты и основное утверждение 4.2, полностью описывающее соответствующий класс подпространств, названный подпространствами *вида 1*. Если подпространство *вида 1* инвариантно относительно линейного преобразования, оно является инвариантным относительно преобразования SL и необходимым условием стойкости шифрсистемы будет использование раундовых ключей, не лежащих в соответствующем подпространстве. Если инвариантное относительно L подпространство не является подпространством *вида 1*, можно выбрать такой S-блок S, что соответствующее подпространство не будет инвариантным относительно преобразования SL.

В утверждении 4.3 [46] найден класс вложенных инвариантных подпространств матриц-циркулянтов. Каждое подпространство указанного класса является подпространством *вида 1*. Теорема 4.1 уточняет результат утвержде-

ния 4.3: помимо найденной цепочки инвариантных подпространств показано, что матрица-циркулянт подобна верхнетреугольной матрице Тёплица и найдены элементы соответствующей матрицы. Результат теоремы 4.1 позволяет полностью описать инвариантные подпространства матриц-циркулянтов при некотором условии, представленном в теореме 4.2. Указанное условие справедливо для любой максимально рассеивающей матрицы-циркулянта (утверждение 4.2). При том же условии в следствии 4.3 найдена вторая нормальная форма матрицы-циркулянта.

Максимально рассеивающие матрицы-циркулянты используются в шифрсистеме AES и хэш-функции Whirlpool. В соответствии с результатами утверждений 4.2 и 4.3 существует цепочка вложенных подпространств, инвариантных относительно преобразований SL указанных криптоалгоритмов. Тем не менее, раундовые ключи (раундовые константы в случае хэш-функции) не лежат в соответствующих подпространствах, что не позволяет провести атаку.

В теореме 4.3 представлены условия, при которых рекурсивная матрица не имеет инвариантных подпространств *вида 1*. Указанные условия справедливы для любой рекурсивной матрицы, построенной на основе БЧХ-кода. В частности, условия справедливы для матрицы линейного преобразования шифрсистемы Кузнечик (следствие 4.4).

В разделе 4.6 представлен алгоритм поиска инвариантных подпространств линейных преобразований $(S^\top)^m$, подобных рекурсивным линейным преобразованиям и представленных в разделе 3.4.4.

В **заключении** сформулированы основные результаты работы и представлены сферы их применения. В **приложении** представлены два примера построенных дифференциально 4-равномерных подстановок.

Благодарности. Автор выражает глубокую благодарность своему научному руководителю кандидату физико-математических наук Чижову Ивану Владимировичу, а также кандидату физико-математических наук Шишкину Василию Алексеевичу, доктору физико-математических наук Круглову Игорю Александровичу за советы по выбору направлений исследований и внимание к работе. Автор также благодарит кандидата физико-математических наук Бурова Дмитрия Александровича за ценные рекомендации при написании диссертационной работы.

Обозначения, определения и общие сведения

Обозначим за $\mathbb{F}_{q^s}$ конечное поле из q^s элементов. V_s — множество двоичных векторов длины s. $\mathbb{F}_q[x]$ — кольцо многочленов над полем $\mathbb{F}_q$. Элементы поля $\mathbb{F}_{q^s} = \mathbb{F}_q[x]/f(x)$, $f(x)$ — некоторый неприводимый многочлен степени s над полем $\mathbb{F}_q$, будем отождествлять с векторами длины s над полем $\mathbb{F}_q$. При необходимости будем указывать конкретный вид многочлена $f(x)$. Добавлением стрелки $\overrightarrow{a}$ будем акцентировать внимание, что элемент рассматривается именно как вектор. Единицу и ноль поля $\mathbb{F}_q$ будем обозначать как 1 и 0 соответственно.

Линейные преобразования будут отождествляться с матрицами, как правило, соответствующими линейному преобразованию в стандартном базисе из единичных векторов. В иных случаях и при необходимости будем уточнять базис, в котором построена матрица.

Нумерация координат векторов ведется справа налево, а нумерация строк матриц — снизу вверх. Все нумерации начинаются с нуля.

Под раундом XSL-схемы понимается последовательность следующих трёх преобразований:

- покоординатное наложение ключа по модулю 2 (XOR);
- применение нелинейного преобразования (слой S-блоков);
- применение линейного преобразования (L-слой).

Определение 1.1. [15] Преобразование

$$S : V_s \longrightarrow V_s$$

называется *дифференциально d-равномерным преобразованием*, если для любых $\alpha \in V_s \backslash 0, \beta \in V_s$ уравнение

$$S(x + \alpha) + S(x) = \beta$$

имеет не более, чем d решений $x \in V_s$. Дифференциально 2-равномерные преобразования также называются *APN-преобразованиями.*

Чем ниже показатель дифференциальной равномерности преобразования, тем меньше вероятность сохранения необходимой разности в разностном методе

криптоанализа [16] в случае, когда соответствующий S-блок является активным. Для полей характеритики два показатель всегда чётный (x и $x + \alpha$) являются (или не являются) решениями одновременно. Вопрос существования APN-подстановок при чётном s больше 6 является нерешённой задачей.

В шифрсистеме AES используется S-блок с дифференциальной равномерностью 4, в Магме для всех S-блоков показатель также равен 4. В шифрсистеме Кузнечик показатель равен 8, что не является оптимальным, но вполне достаточно. В шифрсистеме DES используются нелинейные преобразования $S : V_6 \longrightarrow V_4$ с показателем дифференциальной равномерности 16.

Определение 1.2. ([15], см. также определение 1.22). *Нелинейностью* $nl(S)$ преобразования S называется минимальное из расстояний Хемминга между всеми нетривиальными линейными комбинациями координатных функций преобразования S и аффинными булевыми функциями от s переменных.

Чем выше показатель нелинейности преобразования S, тем меньше вероятность приближения соответствующего S-блока линейной функцией в линейном методе криптоанализа [17]. Максимальным показателем $nl(S)$ для функций $S : V_s \longrightarrow V_s$ является $nl(S) = 2^{s-1} - 2^{\frac{s-1}{2}}$. Очевидно, что граница достигается лишь для нечётных s. Функции, достигающие границу называются *почти бент функциями.*

Пусть далее $Q = \mathbb{F}_{q^s}$.

Определение 1.3. [18] *Весом* $\omega(\overrightarrow{a})$ вектора $\overrightarrow{a} \in Q^m$ будем называть число ненулевых координат вектора $\overrightarrow{a}$.

Показателем рассеивания матрицы $A \in Q_{m,m}$ будем называть следующее число:

$$\tau(A) = \min_{\overrightarrow{a} \neq \overrightarrow{0}} [\omega(\overrightarrow{a}) + \omega(\overrightarrow{a}A)].$$

Нетрудно показать, что $\tau(A) = \tau(A^{-1})$ и $\tau(A) \leqslant m + 1$.

Определение 1.4. [18] Если $\tau(A) = m + 1$, матрицу A будем называть *максимально рассеивающей матрицей.*

Показатель рассеивания матрицы отражает возможность линейного преобразования увеличивать количество активных S-блоков, что важно для защиты от разностного метода криптоанализа [16]. Показатель рассеивания

транспонированной матрицы $L^\top$ отражает возможность линейного преобразования увеличивать количество бит в линейных соотношениях при линейном методе криптоанализа [17]. Если матрица L является максимально рассеивающей, то и матрица $L^\top$ также является максимально рассеивающей.

Максимальный показатель рассеивания является оптимальным с точки зрения криптографии. В шифрсистеме Кузнечик используется максимально рассеивающее линейное преобразование $L \in Q_{16,16}$. В шифрсистеме AES к блоку данных параллельно применяются 4 одинаковых максимально рассеивающих преобразования $L \in Q_{4,4}$. В шифрсистемах DES и Магма используются линейные преобразования — перестановки бит, что недостаточно для обеспечения необходимых рассеивающих свойств.

Пусть $f(x) = x^m - f_{m-1}x^{m-1} - ...f_1x - f_0$ — унитарный многочлен степени m над полем Q.

Определение 1.5. [18] *Сопровождающей матрицей* многочлена $f(x)$ назовем следующую матрицу над полем Q:

$$S_{m\times m} = S(f(x)) = \begin{pmatrix} f_{m-1} & 1 & 0 & ... & 0 \\ f_{m-2} & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ f_1 & 0 & 0 & ... & 1 \\ f_0 & 0 & 0 & ... & 0 \end{pmatrix}.$$

При $k > 1$ матрицу $S^k = S(f)^k$ будем называть *рекурсивной матрицей.*

При некоторых ограничениях, накладываемых на многочлен $f(x)$, матрица $S(f(x))^m$ является максимально рассеивающей матрицей. Линейные преобразования, реализуемые рекурсивными максимально рассеивающими матрицами, используются в качестве линейных преобразований в шифрсистеме Кузнечик и семействе хэш-функций PHOTON.

Матрица S обратима тогда и только тогда, когда $f_0 \neq 0$.

Определение 1.6. [57] *Линейной рекуррентной последовательностью* (ЛРП) над полем Q с характеристическим многочленом $f(x)$ и начальным вектором $\overrightarrow{u} = (u_{m-1},...,u_0) \in Q^m$ назовем последовательность, в которой $u_{i+m} = u_{i+m-1}f_{m-1} + ... + u_if_0$ при всех $i \geqslant 0$.

Пусть $S = S(f(x))$. Для всех $k > 0$ справедливо равенство:

$$(u_{k+m-1},...,u_k) = (u_{k+m-2},...,u_{k-1})S = ... = (u_{m-1},...,u_0)S^k \tag{1.1}$$

Определение 1.7. [57] Многочлен

$$f^*(x) = (f(0))^{-1}x^m f(\frac{1}{x}) = x^m + f_0^{-1}f_1x^{m-1} + ... + f_0^{-1}f_{m-1}x - f_0^{-1} \tag{1.2}$$

будем называть *двойственным многочленом* к многочлену $f(x)$. Если $f(x)$ — характеристический многочлен последовательности $(...,u_{i+m},...,u_1,u_0)$, то $f^*(x)$ — характеристический многочлен последовательности элементов u_i, взятых в обратном порядке: $(...,u_0,u_1,...,u_{i+m-1},u_{i+m})$.

Определение 1.8. [18] Матрицей-циркулянтом размера $m \times m$ над полем $Q = \mathbb{F}_{q^s}$ будем называть матрицу, у которой каждая строка $\overrightarrow{C}_i$ есть циклический сдвиг на одну позицию влево строки $\overrightarrow{C}_{i-1}, i \in \overline{1,m-1}$.

$$C_{m\times m} = Circ_{q^s}(c_{m-1},...,c_0) = \begin{pmatrix} c_0 & c_{m-1} & ... & c_2 & c_1 \\ c_1 & c_0 & ... & c_3 & c_2 \\ ... & & & & \\ c_{m-2} & c_{m-3} & ... & c_0 & c_{m-1} \\ c_{m-1} & c_{m-2} & ... & c_1 & c_0 \end{pmatrix}$$

Замечание 1.1. В матрице-циркулянте любая строка определяет оставшиеся строки, поэтому следующая формулировка будет корректной: матрица-циркулянт C задана строкой $\overrightarrow{A}_i$ матрицы A, что означает $\overrightarrow{A}_i = \overrightarrow{C}_i$, а оставшиеся строки матрицы C определены строкой $\overrightarrow{C}_i$.

Максимально рассеивающие матрицы-циркулянты используются в линейных преобразованиях шифрсистемы AES и хэш-функции Whirlpool.

Вектор $(0,...,0,1,0,...,0) \in Q^m$ с единицей на i-м месте будем обозначать $\overrightarrow{E}_i$. Единичная матрица равна

$$E_{m\times m} = \begin{pmatrix} \overrightarrow{E}_{m-1} \\ \overrightarrow{E}_{m-2} \\ ... \\ \overrightarrow{E}_0 \end{pmatrix}.$$

Обозначим за T следующую перестановочную матрицу:

$$T_{m\times m} = \begin{pmatrix} \overrightarrow{E}_0 \\ \overrightarrow{E}_1 \\ \dots \\ \overrightarrow{E}_{m-1} \end{pmatrix}. \tag{1.3}$$

Справедливы следующие факты:

1. $T = T^{-1}$.
2. Произведение TA меняет в матрице A порядок строк на противоположный, т. е. i-я строка матрицы A равна $(m-1-i)$-й строке матрицы TA: $\overrightarrow{A}_i = \overrightarrow{(TA)}_{m-1-i}$.
3. Произведение AT меняет в матрице A порядок столбцов на противоположный, т. е. i-й столбец матрицы A равен $(m-1-i)$-му столбцу матрицы TA: $A^{\downarrow}_i = (TA)^{\downarrow}_{m-1-i}$.
4. Произведение TAT отображает в матрице A все элементы относительно центра, т. е. $a_{i,j} = (tat)_{m-1-i,m-1-j}$, где tat — соответствующий элемент матрицы TAT.

Под умножением матрицы $A \in Q_{m,m}$ на элемент $a \in Q$ будем понимать умножение каждого элемента матрицы A на элемент a.

Определение 1.9. Преобразование φ множества M называется инволюцией (или является инволютивным), если для любого элемента $m \in M$ справедливо $\varphi(\varphi(m)) = m$. Иными словами $\varphi = \varphi^{-1}$.

Определение 1.10. Блочно-диагональной матрицей будем называть матрицу следующего вида:

$$D_{n\times n} = \mathrm{diag}_{m\times m}(A_{m-1},\dots,A_0) = \begin{pmatrix} A_{m-1} & O_{s\times s} & \dots & O_{s\times s} \\ O_{s\times s} & A_{m-2} & \dots & O_{s\times s} \\ \dots & & & \\ O_{s\times s} & O_{s\times s} & \dots & A_0 \end{pmatrix}_{m\times m},$$

где $O_{s\times s}$ — нулевая матрица, $O_{s\times s}, A_i \in Q_{s\times s}$, $n = ms$. При $s = 1$ матрица D называется *диагональной матрицей*.

Определение 1.11. Блочно-перестановочной матрицей будем называть матрицу следующего вида:

$$U_{n\times n} = \begin{pmatrix} \dots & O_{s\times s} & \dots & E_{s\times s} & \dots & O_{s\times s} & \dots & O_{s\times s} \\ \dots & O_{s\times s} & \dots & O_{s\times s} & \dots & E_{s\times s} & \dots & O_{s\times s} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & E_{s\times s} & \dots & O_{s\times s} & \dots & O_{s\times s} & \dots & O_{s\times s} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}_{m\times m},$$

где $O_{s\times s}, E_{s\times s} \in Q_{s,s}, n = ms$, в каждой строке и в каждом столбце блочной матрицы размера $n \times n$ стоит в точности одна единичная матрица $E_{s\times s}$. При $s = 1$ матрица U называется *перестановочной матрицей.*

Поскольку домножение вектора на невырожденную диагональную D и перестановочную U матрицы не меняет его вес, показатель рассеивания произвольной матрицы A не меняется при её домножении на соответствующие матрицы D и U слева и справа.

Пусть $P = \mathbb{F}_2$ — поле из двух элементов.

Определение 1.12. Пусть $Q = (P[x]/g(x), +, \cdot)$, где $g(x)$ — неприводимый многочлен степени s над полем P. Поле Q изоморфно полю $\mathbb{F}_{2^s}$. Пусть $B_{m\times m}$ — матрица над полем Q, реализующая линейное преобразование векторов-строк из Q^m. Поскольку элементы поля Q есть также векторы-строки над полем P, можно считать, что B задаёт линейное преобразование векторов-строк длины $n = ms$ над полем P и существует матрица $A_{n\times n}$ над полем P, реализующая соответствующее преобразование. В условиях определения будем говорить, что матрица $A = A(B,g(x))$ реализует линейное преобразование B на двоичных векторах.

Пусть $\overrightarrow{a} \in P^{ms}$. Разобьем вектор $\overrightarrow{a}$ на *s-подвекторы*, на которых действуют S-блоки: подвектор $\overrightarrow{a}(i,s)$ с номером i есть подвектор длины s вида $(a_{(i+1)s-1},a_{(i+1)s-2},\dots,a_{is}), i \in \{0,\dots,m-1\}$.

Тогда вектор $\overrightarrow{a} = (\overrightarrow{a}(m-1,s),\dots,\overrightarrow{a}(0,s))$.

Разбиение двоичного вектора на подвекторы используется при изучении свойств шифрсистемы с блоками, представленными двоичными векторами. В таком случае s-битные S-блоки действуют на s-подвекторах и показатель рассеивания линейного преобразования необходимо оценивать также на s-подвекторах.

Определение 1.13. Будем называть *s-весом* $wt_s(\overrightarrow{a})$ вектора $\overrightarrow{a} \in P^{ms}$ количество его ненулевых *s-подвекторов*.

Определение 1.14. Показателем рассеивания на s-подвекторах матрицы $A \in P_{ms,ms}$ будем называть число:

$$\tau_s(A) = \min_{\overrightarrow{a} \in P^{ms} \setminus \overrightarrow{0}} [wt_s(\overrightarrow{a}) + wt_s(\overrightarrow{a}A)].$$

Замечание 1.2. Пусть $B_{m \times m}$ — матрица над полем $Q = \mathbb{F}_{2^s}$, $A_{n \times n}$ реализует преобразование B на двоичных векторах, $A = A(B,g(x))$ при некотором $g(x)$. Тогда показатель рассеивания матрицы B над полем Q совпадает с показателем рассеивания на s-подвекторах матрицы A над полем $\mathbb{F}_2$.

Замечание 1.3. Аналогично случаю с матрицами над полем $\mathbb{F}_{q^s}$ показатель рассеивания на s-подвекторах не меняется при домножении матрицы слева и справа на невырожденные блочно-диагональные и блочно-перестановочные матрицы с размером блока равным s, поскольку домножение двоичного вектора на такие матрицы сохраняет его вес на s-подвекторах.

В шифрсистеме SM4 используются 8-битные S-блоки и двоичная матрица-циркулянт размера 32×32, являющаяся максимально рассеивающей матрицей на s-подвекторах при $s = 8$.

Следующие матрицы будут использоваться для получения вспомогательных результатов.

Определение 1.15. [18] Матрицей Тёплица размера $m \times m$ над полем Q будем называть матрицу, у которой на каждой диагонали, параллельной главной, элементы равны между собой. Пример при $m = 4$.

$$T_{4\times 4} = \begin{pmatrix} t_0 & t_4 & t_5 & t_6 \\ t_1 & t_0 & t_4 & t_5 \\ t_2 & t_1 & t_0 & t_4 \\ t_3 & t_2 & t_1 & t_0 \end{pmatrix}.$$

Определение 1.16. [18] Ганкелевой матрицей размера $m \times m$ над полем Q будем называть матрицу, у которой на каждой диагонали, параллельной побочной, элементы равны между собой. Пример при $m = 4$.

$$\Gamma_{4\times 4} = \begin{pmatrix} g_6 & g_5 & g_4 & g_3 \\ g_5 & g_4 & g_3 & g_2 \\ g_4 & g_3 & g_2 & g_1 \\ g_3 & g_2 & g_1 & g_0 \end{pmatrix}.$$

В диссертации будем использовать булевы переменные $x \in V_1$ и булевы функции $f(x_{n-1},...,x_0)\colon V_n \to V_1$. $\overline{x} = x + 1$ — функция отрицания x. Строка значений булевой функции есть вектор длины 2^n: $(f(1,...,1), f(1,...,1,0),..., f(0,...,0,1), f(0,...,0))$.

Глава 1. Построение дифференциально 4-равномерных подстановок

В первой главе диссертации изучается вопрос синтеза нелинейных преобразований XSL-схем (S-блоков, $S : V_s \to V_s$). Как было упомянуто ранее, наиболее важными криптографическими параметрами S-блоков, характеризующими стойкость схемы к разностному и линейному методам криптоанализа являются дифференциальная равномерность и нелинейность. Для нечётных s оптимальные значения показателей известны: 2 и $2^{s-1} - 2^{\frac{s-1}{2}}$ соответственно. Они достигаются для APN и почти бент преобразований. Для подстановок при чётных s вопрос оптимальных показателей остаётся нерешённой задачей, как для дифференциальной равномерности, так и для нелинейности.

Оптимальными из известных показателей для подстановок чётной размерности являются показатели подстановки инверсии элементов поля $S(x) = x^{-1}$, равные 4 и $2^{s-1} - 2^{\frac{s}{2}}$. В качестве S-блока AES используется подстановка аффинно эквивалентная инверсии. Недостатком указанной подстановки является её достаточно «простое алгебраическое строение», например, справедливо квадратичное соотношение $x^2 S(x) = x$. Подобные квадратичные соотношения используются в алгебраических атаках [66] на XSL-схемы, заключающихся в составлении и решении системы квадратичных булевых уравнений. Однако конкретных атак с использованием указанного недостатка S-блока AES не предложено.

Криптографическим показателем, характеризующим стойкость S-блока к алгебраическим атакам является графовая алгебраическая иммунность ($AI(S)$, см. определение 1.23). Оптимальным значением AI при $s = 8$ является значение 3. При выборе S-блока $s = 8$ случайным образом, почти всегда получается значение $AI(S) = 3$ [39], в частности для S-блока шифрсистемы Кузнечик $AI(S) = 3$. Для S-блоков, построенных алгебраическими методами, $AI(S)$ почти всегда равно 2. В частности, для S-блока AES $AI(S) = 2$. На конференции CTCrypt 2023 впервые представлена 8-битная дифференциально 4-равномерная подстановка с $AI(S) = 3$ [40].

Несмотря на то, что для S-блока шифрсистемы Кузнечик $AI(S) = 3$, другие его показатели не являются оптимальными. В частности, дифференциальная равномерность S-блока равна 8. В S-блоке Кузнечика также найдена TU-декомпозиция [67]. Как и в случае с AES, конкретных атак использующих

недостатки S-блока Кузнечика не найдено. Тем не менее, всегда хорошо иметь варианты про запас, и разработка новых нелинейных преобразований с хорошими криптографическими характеристиками является актуальной.

В настоящей главе развивается подход в построении дифференциально 4-равномерных подстановок, применявшийся ранее в работах [34], [37]. Суть данного подхода заключается в использовании ограничений известных дифференциально d-равномерных преобразований (при $d = 2, 4$) пространства V_{s+1} на его линейные подмногообразия размерности s. В результате удаётся построить подстановки чётной размерности с оптимальными из известных показателями дифференциальной равномерности 4 и нелинейности $2^{s-1} - 2^{\frac{s}{2}}$. В следующем разделе вводятся криптографические характеристики S-блоков. Построение подстановок представлено в разделе 1.2.

Результаты главы опубликованы в работе [69].

1.1 Криптографические характеристики S-блоков

Преобразование $S(x) = S(x_{s-1},...,x_0)$ можно задать системой координатных булевых функций $S(x_{s-1},...,x_0) = (S_{s-1}(x_{s-1},...,x_0),...,S_0(x_{s-1},...,x_0))$.

Определение 1.17. [15] *Алгебраической степенью* $deg(S)$ преобразования S называется максимальная из степеней многочленов Жегалкина булевых функций $S_{s-1},...,S_0$.

Определение 1.18. [15] Преобразования степени 1 называются *аффинными преобразованиями*, степени 2 — *квадратичными преобразованиями*, степени 3 — *кубическими преобразованиями*.

Для любых $u,v \in V_s$ определим значение билинейной формы

$$\langle u,v \rangle = u_{s-1}v_{s-1} + ... + u_0v_0 \in \mathbb{F}_2.$$

Определение 1.19. [15] Для любого $v \in V_s \backslash 0$ булеву функцию $\langle v,S \rangle = v_{s-1}S_{s-1}(x) + ... + v_0S_0(x)$ будем называть *компонентной функцией преобразования* S.

В некоторых работах, например в [40], алгебраической степенью называют следующий показатель. Чтобы исключить совпадение понятий, автор диссертации будет называть его степенью нелинейности.

Определение 1.20. [40] *Степенью нелинейности* $nldeg(S)$ преобразования S называется минимальная из степеней многочленов Жегалкина среди всех компонентных функций преобразования S.

Определение 1.21. [15] *Коэффициентами Уолша-Адамара* преобразования $S : V_s \to V_s$ называются следующие целые числа:

$$W_{u,v}^S = \sum_{x \in V_s} (-1)^{\langle v, S(x) \rangle + \langle u, x \rangle}, \quad u,v \in V_s.$$

Спектр Уолша-Адамара преобразования S — система коэффициентов Уолша-Адамара

$$W_{u,v}^S, \quad u \in V_s, \quad v \in V_s \backslash 0.$$

Определение 1.22. [15] *Нелинейностью* $nl(S)$ преобразования S называется минимальное из расстояний Хемминга между всеми компонентными функциями преобразования S и аффинными булевыми функциями от s переменных.

Для нелинейности известно выражение через спектр Уолша-Адамара [15]:

$$nl(S) = 2^{s-1} - \frac{1}{2} \cdot \max\{|W_{u,v}^S|, u \in V_s, \quad v \in V_s \backslash 0\}.$$

Определение 1.23. [40] *Графовой алгебраической иммунностью* $AI(S)$ преобразования S называется алгебраическая иммунность [65] булевой функции-индикатора множества $\Gamma_f = \{(x, f(x)) | x \in V_s\}$. Булева функция-индикатор равна 1 на векторах, лежащих в Γ_f, и только на них.

Обозначим через

$$tr_2^s(x) = x + x^2 + \ldots + x^{2^{s-1}}, \quad x \in \mathbb{F}_{2^s},$$

функцию «след» со значениями в подполе $\mathbb{F}_2$. Через $gcd(i,j)$ будем обозначать наибольший общий делитель ненулевых целых чисел i,j.

Определение 1.24. *Гиперплоскостью* в векторном пространстве V_{s+1} назовем любое его подпространство H размерности s. Выбрав базис гиперплоскости, мы можем естественным образом отождествить её элементы с элементами пространства V_s.

В случае, когда для некоторых непересекающихся подмножеств M_1, M_2 пространства V_{s+1} мощности 2^s выполнено равенство $V_{s+1} = M_1 \cup M_2$, мы будем использовать обозначение $V_{s+1} = M_1 \sqcup M_2$.

1.2 Развитие подхода к синтезу дифференциально 4-равномерных подстановок

Следующая теорема сформулирована и доказана в работе [37]

Теорема 1.1. *[37] Пусть s — чётное, $F(x) : V_{s+1} \to V_{s+1}$ — квадратичная APN-подстановка, $F(0) = 0$. Пусть $L_u(x) = F(x) + F(x+u) + F(u)$, $H_u = \{L_u(a) | a \in V_{s+1}\}$ и $F_u(x)$ есть ограничение $L_u(F^{-1}(x))$ на H_u. Тогда при любом $u \neq 0$ $F_u(x)$ является дифференциально 4-равномерной подстановкой.*

H_u является гиперплоскостью в V_{s+1}. В теореме 1.1 для построения используются обратные квадратичным APN-подстановки и гиперплоскости. Далее в главе обобщается понятие гиперплоскости, что позволит расширить класс преобразований, допускающих применение соответствующей конструкции.

Определение 1.25. Подмножество K пространства V_{s+1} будем называть подмножеством, порождающим простое разбиение, если существует такой вектор $\boldsymbol{\gamma} \in V_{s+1}$, что справедливо равенство

$$V_{s+1} = K \sqcup K + \boldsymbol{\gamma}, \tag{1.1}$$

где $K + \boldsymbol{\gamma} = \{\boldsymbol{\alpha} + \boldsymbol{\gamma} | \boldsymbol{\alpha} \in K\}$.

Непосредственно из определения следуют эквивалентные условия.

Утверждение 1.1. *Для любого подмножества $K \subset V_{s+1}$ и вектора $\boldsymbol{\gamma} \in V_{s+1}$ эквивалентны следующие свойства:*

(a) K порождает простое разбиение, и имеет место равенство (1.1);

(b) мощность $|K| = 2^s$, и вектор $\boldsymbol{\gamma} \in V_{s+1}$ не содержится в множестве $K + K = \{\boldsymbol{\alpha} + \boldsymbol{\beta} | \boldsymbol{\alpha}, \boldsymbol{\beta} \in K\}$;

(c) K есть множество представителей смежных классов пространства V_{s+1} по одномерному подпространству, порождённому вектором $\boldsymbol{\gamma}$.

Нетрудно видеть, что любая гиперплоскость будет порождать простое разбиение. Если множество K порождает простое разбиение, то и дополнение $V_{m+1}\backslash K$ также порождает простое разбиение.

Докажем одно вспомогательное утверждение о простых разбиениях.

Лемма 1.1. *Предположим, что множество K порождает простое разбиение, имеет место равенство (1.1), и A — произвольное линейное преобразование пространства V_{s+1}, ядром которого является множество векторов $\{0,\gamma\}$. Тогда образ $A(K)$ является гиперплоскостью в V_{s+1}.*

Доказательство. Предположим, что $A(\alpha) = A(\beta)$, $\alpha,\beta \in K$. Тогда $A(\alpha+\beta) = 0$, и так как $\alpha + \beta \neq \gamma$, то $\alpha = \beta$. Значит, A инъективно на множестве K, и $|A(K)| = 2^s$. Но $|A(V_{s+1})| = 2^s$, следовательно, $A(K) = A(V_{s+1})$ — гиперплоскость в V_{s+1}. □

На основе доказанной леммы 1.1 определим следующую общую конструкцию построения преобразований пространства V_s.

Конструкция 1. Пусть $G(x) : V_{s+1} \longrightarrow V_{s+1}$ — дифференциально 2-равномерное преобразование и существует такая гиперплоскость H, что множество $K = G(H)$ порождает простое разбиение. Пусть также выполнено равенство (1.1). Выберем произвольное линейное преобразование A пространства V_{s+1}, ядром которого является множество $\{0,\gamma\}$. Рассмотрим гиперплоскость $A(K) = W$ и выберем произвольное невырожденное линейное преобразование B пространства V_{s+1}, для которого $B(W) = H$. Пусть S — ограничение преобразования $G\cdot A\cdot B$ на гиперплоскость H.

Теорема 1.2. *Преобразование S, полученное в соответствии с Конструкцией 1, является дифференциально 4-равномерной подстановкой на H.*

Доказательство. По построению преобразование S является инъективным, следовательно, S — подстановка на H.

Обоснуем свойство дифференциальной 4-равномерности S. Для любых ненулевых $\alpha, \beta \in H$ рассмотрим уравнение:

$$S(x + \alpha) + S(x) = \beta, \quad x \in H. \tag{1.2}$$

Воспользовавшись линейностью преобразований A и B, получим: (1.2) равносильно совокупности уравнений

$$G(x + \alpha) + G(x) \in A^{-1}(B^{-1}(\beta)), \quad x \in H. \tag{1.3}$$

Элемент $\varepsilon = B^{-1}(\beta)$ определен однозначно, а $|A^{-1}(\gamma)| = 2$. Так как преобразование G — дифференциально 2-равномерное, то для каждого из возможных двух векторов в правой части уравнения (1.3) существует не более двух решений $x \in V_{s+1}$. Значит, общее число решений (1.2) не превосходит четырёх. □

Теорема 1.3. *[37] Пусть $F_u(x)$ построена в условиях теоремы 1.1. Тогда $F^{-1}(x)$ является почти бент функцией и $nl(F_u) = 2^{s-1} - 2^{s/2}$.*

Замечание 1.4. Если *Конструкция 1* применяется к некоторому почти бент преобразованию G, для нелинейности преобразования S справедливо утверждение теоремы 1.3 (вместе с доказательством). Таким образом, в этом случае S обладает максимально известной нелинейностью для чётных s, равной $nl(S) = 2^{s-1} - 2^{s/2}$.

Приведем общий критерий, при выполнении которого возможна реализация *Конструкции 1.*

Теорема 1.4. *Пусть $G(x) : V_{s+1} \longrightarrow V_{s+1}$ — подстановка. Тогда следующие условия равносильны:*

(a) Существует такая гиперплоскость H в V_{s+1}, что множество $G(H)$ порождает простое разбиение;

(b) Существует такой ненулевой вектор α, что преобразование

$$G_\alpha^{-1}(x) = G^{-1}(x + \alpha) + G^{-1}(x), \quad x \in V_{s+1},$$

имеет компонентную функцию, тождественно равную единичному элементу поля 1.

Если в условиях теоремы $G(x)$ — APN-подстановка, то условия (a) и (b) равносильны следующему условию:

(c) Существует ненулевой вектор α, такой, что множество

$$G_\alpha^{-1}(V_{s+1}) = \{G^{-1}(x + \alpha) + G^{-1}(x) | x \in V_{s+1}\}$$

является аффинным многообразием размерности s, не являющимся подпространством.

Доказательство. Предположим, что выполнено условие (a),

$$G(H) \sqcup G(H) + \alpha = V_{s+1}, H \sqcup H + \beta = V_{s+1}, \alpha \in V_{s+1}, \beta \in V_{s+1} \backslash H.$$

Так как G — подстановка, то имеем равенство $G(H) + \alpha = G(H + \beta)$. Для любого $x \in V_{s+1}$ ровно один элемент из пары $x, x + \alpha$ содержится в $G(H)$, а другой содержится в $G(H + \beta)$. Следовательно, из пары элементов $G^{-1}(x + \alpha), G^{-1}(x)$ один содержится в H, а другой содержится в $H + \beta$. Значит, их сумма лежит в $H + \beta$ и потому имеет место включение:

$$G_\alpha^{-1}(V_{s+1}) = \{G^{-1}(x + \alpha) + G^{-1}(x) | x \in V_{s+1}\} \subset H + \beta.$$

Многообразие $H + \beta$ размерности s задается некоторым аффинным соотношением

$$H + \beta = \{h \in V_{s+1} | \langle v, h \rangle = 1\}, \quad v \in V_{s+1} \backslash 0.$$

Из включения $G_\alpha^{-1}(V_{s+1}) \subset H + \beta$ следует, что компонентная функция $\langle v, G_\alpha^{-1} \rangle$ преобразования G_α^{-1} тождественно равна 1. Импликация из (a) в (b) доказана.

Предположим, что выполнено условие (b), т.е. для некоторого вектора $v \in V_{s+1} \backslash 0$ компонентная функция $\langle v, G_\alpha^{-1} \rangle$ преобразования G_α^{-1} тождественно равна 1. Тогда, положив $H = \{h \in V_{m+1} | \langle v, h \rangle = 0\}$ и выбрав вектор $\beta \notin H$ получим включение $G_\alpha^{-1}(V_{s+1}) \subset H + \beta$. Предположим, что существуют такие $k_1, k_2 \in G(H)$, что $k_1 + k_2 = \alpha$. Тогда элемент $G_\alpha^{-1}(k_1) = G^{-1}(k_1) + G^{-1}(k_2) \in H$. Получено противоречие, значит $G(H) \sqcup G(H) + \alpha = V_{s+1}$, т.е. выполнено условие (a). Равносильность (a) и (b) показана.

Пусть теперь $G(x)$ — APN подстановка. Тогда G^{-1} тоже APN подстановка и $|G_\alpha^{-1}(V_{s+1})| = 2^s$, после чего равносильность условий (b) и (c) очевидна. □

Следствие 1.1. *Пусть $G(x) : V_{s+1} \longrightarrow V_{s+1}$ — подстановка, для которой $G^{-1}(x)$ — квадратичное преобразование. Тогда существует такая гиперплоскость H в V_{s+1}, что множество $G(H)$ порождает простое разбиение.*

Доказательство. Рассмотрим произвольный вектор $\alpha \in V_{s+1} \backslash 0$. Так как G^{-1} — квадратичная подстановка, то $G_\alpha^{-1}(x) = G^{-1}(x + \alpha) + G^{-1}(x)$ - аффинное преобразование. Это преобразование не является линейным и не является сюръективным, поскольку $0 \notin G_\alpha^{-1}(V_{s+1})$. Отсюда следует, что для некоторой гиперплоскости H в V_{s+1} и некоторого вектора $\beta \in V_{s+1} \backslash H$ выполнено включение $G_\alpha^{-1}(V_{s+1}) \subset H + \beta$. При доказательстве теоремы показано, что в этом случае имеет место равенство $G(H) \sqcup G(H) + \alpha = V_{s+1}$. □

Из доказательства следствия 1.1 видно, что теорема 1.1 является частным случаем *Конструкции 1.*

Следующая теорема полностью описывает множество степенных подстановок, удовлетворяющих условиям *Конструкции 1.*

Теорема 1.5. *Если $S(x)$ — степенная APN-подстановка, то Конструкция 1 применима к S тогда и только тогда, когда $S^{-1}(x)$ — квадратичная функция.*

Доказательство. Случай, когда $S^{-1}(x)$ — квадратичная функция следует из *Следствия 1.*

Предположим теперь, что $S^{-1}(x) = x^d$ — неквадратичная степенная APN-подстановка и множество $S_\alpha^{-1}(V_{s+1})$ является аффинным многообразием размерности s. Тогда, поскольку произвольный ненулевой вектор ε можно представить в виде $\varepsilon = \alpha\beta$, справедлива следующая цепочка равенств:

$S_\varepsilon^{-1}(x) = (x+\varepsilon)^d + x^d = (x+\alpha\beta)^d + x^d = \beta^d((\beta^{-1}x+\alpha)^d + (\beta^{-1}x)^d)$. Следовательно, множество $S_\varepsilon^{-1}(V_{s+1}) = \beta^d S_\alpha^{-1}(V_{s+1})$ является многообразием размерности s для произвольного ненулевого ε. Это означает, что функция $S^{-1}(x) = x^d$ является скрученной функцией. Однако, неквадратичных скрученных степенных функций не существует [51], что противоречит предположению. □

До сих пор все подстановки, которые допускают использование *Конструкции 1* были квадратичными. Следующий пример показывает, что *Конструкция 1* допускает использование APN-подстановок большей алгебраической степени.

Пример 1.1. Рассмотрим единственную известную на данный момент APN-подстановку от четного числа переменных $s = 6$ Дж. Диллона, алгебраическая степень которой совпадает с алгебраической степенью обратной подстановки и равна 3. Компьютерные вычисления показывают, что для 7 гиперплоскостей H из 63 возможных множество $K = G(H)$ порождает простое разбиение, что делает возможным применение *Конструкции 1.*

Покажем, что *Конструкцию 1* можно использовать для построения дифференциально 4-равномерных подстановок из преобразований, которые не являются подстановками.

В работе [68] были построены следующие кубические почти бент-преобразования для четных $s \geqslant 2$:

$$G(x) = x^{2^j+1} + \left(x^{2^j} + x\right) \cdot \mathrm{tr}_2^{s+1}\left(x^{2^j+1} + x\right), \tag{1.4}$$

где $x \in V_{s+1}, \quad gcd(s+1,j) = 1.$

Преобразование (1.4) не является подстановкой на пространстве V_{s+1}.

Покажем, что *Конструкция 1* применима к преобразованиям (1.4). Рассмотрим гиперплоскость $H_0 = \{u \in V_{s+1} | \mathrm{tr}_2^{s+1}(u) = 0\}$ в пространстве V_{s+1}.

Теорема 1.6. *Преобразование (1.4) инъективно на H_0, и $\alpha+\beta \neq 1$ для любых $\alpha,\beta \in G(H_0)$.*

Доказательство. Будем использовать обозначение $\mathrm{tr}_2^{s+1} = \mathrm{tr}$. Имеют место равенства

$$G(x) = x^{2^j+1} + \left(x^{2^j} + x\right) \mathrm{tr}\left(x^{2^j+1}\right), \quad x \in H_0. \tag{1.5}$$

$$\mathrm{tr}\left(\left(x^{2^j} + x\right) \mathrm{tr}\left(x^{2^j+1}\right)\right) = 0, \quad x \in V_{s+1}. \tag{1.6}$$

Покажем, что преобразование (1.4) инъективно на H_0. Предположим, что для $x,y \in H_0$ справедливо равенство $G(x) = G(y)$, т.е. (см. (1.5)):

$$x^{2^j+1} + \left(x^{2^j} + x\right) \cdot \mathrm{tr}\left(x^{2^j+1}\right) = y^{2^j+1} + \left(y^{2^j} + y\right) \cdot \mathrm{tr}\left(y^{2^j+1}\right). \tag{1.7}$$

Применим функцию след к обеим частям равенства (1.7) и воспользуемся (1.6). Получим равенство $\mathrm{tr}\left(x^{2^j+1}\right) = \mathrm{tr}\left(y^{2^j+1}\right)$. Возможны два случая:

a) $\mathrm{tr}\left(x^{2^j+1}\right) = \mathrm{tr}\left(y^{2^j+1}\right) = 0.$

Подставим в (1.7), получим $x^{2^j+1} = y^{2^j+1}$. Из условия $gcd(s+1,j) = 1$ и чётности s следует, что $gcd(2^{s+1}-1, 2^j+1) = 1$, а тогда $x = y$.

b) $\mathrm{tr}\left(x^{2^j+1}\right) = \mathrm{tr}\left(y^{2^j+1}\right) = 1.$

Подставив в (1.7), получим $x^{2^j+1} + x^{2^j} + x = y^{2^j+1} + y^{2^j} + y$, следовательно $(x+1)^{2^j+1} = (y+1)^{2^j+1}$, что также приводит к равенству $x = y$.

Инъективность преобразования (1.4) на H_0 доказана.

Далее, предположим, что для некоторых $x,y \in H_0$ справедливо равенство $G(x) + G(y) = 1$, т.е.

$$x^{2^j+1} + \left(x^{2^j} + x\right) \mathrm{tr}\left(x^{2^j+1}\right) = y^{2^j+1} + \left(y^{2^j} + y\right) \mathrm{tr}\left(y^{2^j+1}\right) + 1 \tag{1.8}$$

Применим функцию след к обеим частям равенства (1.8), согласно (1.6), получим $\mathrm{tr}\left(x^{2^j+1}\right) = \mathrm{tr}\left(y^{2^j+1}\right) + 1$. Без ограничения общности будем считать, что $\mathrm{tr}\left(x^{2^j+1}\right) = 0$ и $\mathrm{tr}\left(y^{2^j+1}\right) = 1$, подставим в (1.8): $x^{2^j+1} = y^{2^j+1} + y^{2^j} + y + 1$ или $x^{2^j+1} = (y+1)^{2^j+1}$. Следовательно, $x = y+1$. Применим функцию след к последнему равенству. Получим $\mathrm{tr}(x) = \mathrm{tr}(y) + 1$, что противоречит условию $x,y \in H_0$. □

Таким образом, согласно теоремам 1.4 и 1.6 и замечанию 1.4, применяя *Конструкцию 1* к преобразованию (1.4) и подпространству H_0, получаем дифференциально 4-равномерную подстановку S на V_s. На момент написания диссертации автору не известны подстановки на V_s, обладающие большей нелинейностью, чем полученная выше подстановка.

Для $s = 8$ указанная выше подстановка S была вычислена на компьютере, это дифференциально 4-равномерная подстановка с алгебраической степенью 3, степенью нелинейности 3, нелинейностью 112, графовой алгебраической иммунностью 2. Обратная к ней подстановка S^{-1} имеет следующие параметры: дифференциальная равномерность 4, алгебраическая степень 5, степень нелинейности 5, нелинейность 112, графовая алгебраическая иммунность 2. Данные подстановки представлены в приложении А.

Выводы по главе. В главе 1 предложен метод построения подстановок чётной размерности с оптимальными (из известных на данный момент) показателями дифференциальной равномерности и нелинейности, что важно для защиты XSL-схем от разностного и линейного методов криптоанализа. Метод построения развивает результаты работ [34] и [37], позволяя использовать в построении новые классы преобразований. Характеристики построенных подстановок совпадают с характеристиками подстановок из работы [37]. Некоторые из характеристик не являются оптимальными. Для использования построенных подстановок в XSL-схемах необходимо рассмотреть их криптографические свойства в сочетании с выбранным L-преобразованием, а также оценить их эксплуатационные характеристики.

Глава 2. Линейные преобразования, заданные умножением на элемент кольца

В главе 1 изучались нелинейные преобразования XSL-схем. В главах 2, 3 будут изучаться линейные преобразования. Основными криптографическими характеристиками линейных преобразований являются показатели рассеивания матрицы L и транспонированной матрицы $L^\top$. Указанные показатели отражают стойкость схемы к разностному и линейному методам криптоанализа. Существует немало различных классов максимально рассеивающих матриц (см. введение). При выборе конкретной матрицы для XSL-схемы необходимо также обращать внимание на эксплуатационные характеристики матрицы.

В данной главе будут рассмотрены максимально рассеивающие матрицы-циркулянты с точки зрения их эксплуатационных характеристик. Для матриц-циркулянтов будут найдены разложения, позволяющие предложить программные реализации с использованием небольшого числа команд процессора. Для указанных разложений получены верхние и нижние оценки на число слагаемых. Максимально рассеивающие матрицы-циркулянты используются в шифрсистеме AES и хэш-функции Whirlpool. Максимально рассеивающая на s-подвекторах (см. определение 1.14) двоичная матрица-циркулянт используется в шифрсистеме SM4.

Теоретические результаты главы получены в общем виде: для матриц, заданных умножением на элемент кольца над полем $\mathbb{F}_2$. С практической точки зрения лучших представителей данного класса, чем матрицы циркулянты не известно.

Результаты главы опубликованы в работе [70].

2.1 Линейные преобразования, заданные умножением на элемент кольца над $\mathbb{F}_2$

Пусть $f(x)$ — многочлен степени m над полем $Q = \mathbb{F}_{q^s}$, $R = Q[x]/f(x)$ — факторкольцо многочленов, которое можно также рассматривать как векторное пространство размерности m над полем Q с операциями сложения

многочленов и умножения многочлена на элемент $a \in Q$. Пусть $\varphi : Q^m \to R$ — отображение, переводящее строку вектора в соответствующий многочлен:

$$\varphi(b_{m-1},...,b_1,b_0) = b_{m-1}x^{m-1} + ... + b_1x + b_0.$$

Нетрудно видеть, что φ — изоморфизм векторных пространств. Поскольку умножение на элемент $a(x)$ кольца R является линейным преобразованием кольца R, соответствующее ему преобразование $\overrightarrow{b} \to \varphi^{-1}(a(x)\cdot \varphi(\overrightarrow{b}))$ пространства Q^m можно задать матрицей $A \in Q_{m,m}$, которую будем обозначать $A_{a(x),f(x)}$.

Определение 2.1. Пусть $f(x)$ — многочлен степени m над полем Q. Линейным преобразованием, заданным через умножение на элемент $a(x)$ кольца $R = Q[x]/f(x)$, будем называть следующее преобразование:

$$\widehat{a}_{f(x)} : h(x) \mapsto h(x)a(x) \bmod f(x),\ h(x) \in R.$$

Утверждение 2.1. *Пусть $f(x)$ — многочлен степени m над полем Q, $R = Q[x]/f(x)$ — факторкольцо многочленов. Матрица $A \in Q_{m,m}$ равна матрице $A_{a(x),f(x)}$ для некоторого $a(x) \in R$ тогда и только тогда, когда для любого $i \in \overline{1,m-1}$: $\varphi(\overrightarrow{A}_i) = x^i\varphi(\overrightarrow{A}_0)$ в кольце R. В условиях утверждения $a(x) = \varphi(\overrightarrow{A}_0)$.*

Доказательство. **Необходимость.** Пусть $A = A_{a(x),f(x)}$. Заметим, что $\varphi(\overrightarrow{E}_i) = x^i$. Тогда $\varphi(\overrightarrow{A}_i) = \varphi(\overrightarrow{E}_i\cdot A) = \varphi(\varphi^{-1}(a(x)\cdot \varphi(\overrightarrow{E}_i))) = a(x)x^i$ при любом i. Подставив $i = 0$, получим $a(x) = \varphi(\overrightarrow{A}_0)$.

Достаточность. Для произвольного $\overrightarrow{c} = (c_{m-1},...,c_0)$

$$(c_{m-1},...,c_0)A = \sum_{i=0}^{m-1} c_i\overrightarrow{A}_i = \varphi^{-1}(\sum_{i=0}^{m-1} c_i\varphi(\overrightarrow{A}_i)) =$$

$$\varphi^{-1}(\varphi(\overrightarrow{A}_0)\cdot \sum_{i=0}^{m-1} c_ix^i) = \varphi^{-1}(\varphi(\overrightarrow{A}_0)\cdot \varphi(\overrightarrow{c})).$$

Значит по определению $A = A_{a(x),f(x)}$, где $a(x) = \varphi(\overrightarrow{A}_0)$. □

В дальнейшем повествовании будем зачастую опускать действие изоморфизма φ, тем самым отождествляя векторы длины m над Q и многочлены из кольца R.

Матрица линейного преобразования $\widehat{a}_{f(x)}$ имеет вид

$$A_{a(x),f(x)} = \begin{pmatrix} \widehat{a}_{f(x)}(x^{m-1}) \\ \dots \\ \widehat{a}_{f(x)}(x^i) \\ \dots \\ \widehat{a}_{f(x)}(x) \\ \widehat{a}_{f(x)}(1) \end{pmatrix} = \begin{pmatrix} a(x) \cdot x^{m-1} \bmod f(x) \\ \dots \\ a(x) \cdot x^i \bmod f(x) \\ \dots \\ a(x) \cdot x \bmod f(x) \\ a(x) \end{pmatrix}. \tag{2.1}$$

Нетрудно видеть, что множество матриц $\{A_{a(x),f(x)}, a(x) \in R\}$ с операциями сложения и умножения матриц является кольцом, изоморфным кольцу многочленов R. Матрица $A_{a(x),f(x)}$ соответствует многочлену $a(x)$, гомоморфизм по операции умножения следует из утверждения 2.1, гомоморфизм по операции сложения очевиден.

Пусть далее поле $P = \mathbb{F}_2$. Рассмотрим следующие операции над битовыми строками длины n, которые реализованы на вычислителях как *команды процессора*.

1. *XOR*(α, β) — побитовое сложение строк по модулю 2. Аналог операции сложения векторов соответствующей длины над P.
2. *AND*(α, β) — побитовое «логическое И» строк. Аналог умножения на диагональную матрицу: $AND(\alpha, \beta) = \alpha \cdot diag_{n \times n}(\beta)$.
3. *OR*(α, β) — побитовое «логическое ИЛИ» строк.
4. *SHFT*(α) — нециклический сдвиг строки влево (вправо) на i позиций с заполнением нулями. Аналог умножения на матрицу с единицами на диагонали, находящейся ниже (выше) главной на i позиций, и с нулевыми остальными элементами.
5. *CLMUL*(α, β) — умножение двоичных строк длины n как многочленов степени $n-1$ над полем P. Результат — строка длины $2n$.

Линейное преобразование $\widehat{a}_{f(x)}$ можно также считать преобразованием векторов длины n.

Замечание 2.1. Для многочленов $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$ и $f(x) = x^n + f_{n-1}x^{n-1} + \dots + f_0$ вектор коэффициентов многочлена $a(x) \cdot x \bmod f(x)$ имеет вид

$$(a_{n-2} + a_{n-1}f_{n-1},\ \dots,\ a_{i-1} + a_{n-1}f_i,\ \dots,\ a_{n-1}f_0). \tag{2.2}$$

Покажем, что в некоторых случаях преобразование $\widehat{a}_{f(x)}$ можно представить с использованием небольшого числа *команд процессора.*

Утверждение 2.2. *Пусть* $f(x) = x^n + f_{n-1}x^{n-1} + ... + f_0 = x^n + \overline{f(x)}$ *— многочлен степени* n *над полем* P, $a(x)$ *— многочлен над* P *степени меньше* n. *Тогда для преобразования* $\widehat{a} = \widehat{a}_{f(x)}$ *справедливы следующие утверждения:*

1) *если* $deg\ \overline{f(x)} \leqslant n/2$, *то преобразование* $\widehat{a}$ *может быть реализовано пятью командами процессора:* $3\ CLMUL + 2\ XOR$;
2) *если* $deg\ \overline{f(x)} + deg\ a(x) \leqslant n$, *то преобразование* $\widehat{a}$ *может быть реализовано тремя командами процессора:* $2\ CLMUL + 1\ XOR$;
3) *если* $deg\ \overline{f(x)} = 0$, *то преобразование* $\widehat{a}$ *может быть реализовано двумя командами процессора:* $1\ CLMUL + 1\ XOR$;
4) *для реализации преобразования* $\widehat{a}$ *в памяти необходимо хранить многочлены* $a(x)$ *и* $\overline{f(x)}$ *в случаях 1-2 и только многочлен* $a(x)$ *в случае 3.*

Доказательство. П. 4 очевиден, обоснуем пп. 1-3. Выполним команду $CLMUL$ для многочленов $a(x)$ и $h(x)$ и запишем результат в виде $b(x) = b_1(x)x^n + b_0(x)$, где степени многочленов $b_i(x)$ меньше n. Для получения результата линейного преобразования необходимо многочлен $b(x)$ привести по модулю $f(x)$.

1. Если $deg\ \overline{f(x)} = 0$, то $f(x) = x^n + 1$ (п. 3) и $b(x) \bmod f(x) = b(x) + b_1(x)f(x) = b(x) + b_1(x)x^n + b_1(x) = b_1(x) + b_0(x)$. Таким образом, помимо команды $CLMUL$, один раз применена команда XOR.
2. Если $deg\ \overline{f(x)} > 0$, то приведение по модулю чуть сложнее. Тогда $b(x) \bmod f(x) = b(x) + b_1(x)x^n + b_1(x)\overline{f(x)} \bmod f(x) = b_1(x)\overline{f(x)} + b_0(x) \bmod f(x)$.
   Пусть $b_1(x)\overline{f(x)} = c(x) = c_1(x)x^n + c_0(x)$, где $deg\ c_0(x) < n$ и $deg\ c_1(x) < n$.
   – Если $deg\ \overline{f(x)} + deg\ a(x) \leqslant n$, то $deg\ c(x) = deg\ b_1(x) + deg\ \overline{f(x)} = deg\ a(x) + deg\ h(x) + deg\ \overline{f(x)} - n \leqslant deg\ h(x) < n$. А значит, $b(x) \bmod f(x) = b_0(x) + c_0(x)$, где $c_0(x) = b_1(x)\overline{f(x)}$ можно найти одной командой $CLMUL$, что означает справедливость п. 2 исходного утверждения.
   – Если $deg\ \overline{f(x)} \leqslant n/2$, то $deg\ c_1(x) = deg\ b_1(x) + deg\ \overline{f(x)} - n < n/2$ и $deg\ c_1(x) + deg\ \overline{f(x)} < n$. Тогда $b(x) \bmod f(x) = c_1(x)x^n + c_0(x) + b_0(x) \bmod f(x) = c_1(x)x^n + c_0(x) + b_0(x) + c_1(x)f(x) = c_0(x) + b_0(x) + c_1(x)\overline{f(x)}$. Результат $c_1(x)\overline{f(x)}$ можно получить одной командой

$CLMUL$. Итого, для выполнения линейного преобразования потребуется 3 команды $CLMUL$ и 2 XOR.

□

Замечание 2.2. Отметим, что времена выполнения команд процессора различны [55]. Поэтому количество команд, необходимых для реализации преобразования, вообще говоря, не определяет однозначно время реализации преобразования.

Наибольшая эффективность преобразования $\widehat{a}$ достигается в случае 3: для реализации требуется лишь 2 команды процессора, а в памяти необходимо хранить лишь многочлен $a(x)$. Рассмотрим другие свойства преобразования $\widehat{a}_{x^n+1}$.

Утверждение 2.3. *Пусть $f(x) = x^n + 1$ — многочлен над P, $\widehat{a} = \widehat{a}_{f(x)}$. Тогда:*

1. *матрица A линейного преобразования $\widehat{a}$ является матрицей-циркулянтом над полем P;*
2. *при любом s показатели рассеивания на s-подвекторах для матриц A и $A^\top$ совпадают;*
3. *если n чётно и преобразование $\widehat{a}$ инволютивно, то при любом $s \geqslant 1$ показатель рассевания $\widehat{a}$ на s-подвекторах не превышает 4.*

Доказательство. 1. Для проверки утверждения достаточно подставить многочлен $x^n + 1$ в формулы (2.1) и (2.2).

2. Покажем, что для матрицы-циркулянта A справедливо равенство $A^\top = TAT$ (матрица T определена в (1.3)). Будем считать, что $i \geqslant j$, противоположный случай рассматривается аналогично. Поскольку матрица $A^\top$ также является циркулянтом, справедливо равенство $a^\top_{i,j} = a_{j,i} = a_{0,i-j}$. Для матрицы TAT : $TAT_{i,j} = a_{m-1-i,m-1-j} = a_{0,m-1-j-(m-1-i)} = a_{0,i-j}$. Поскольку матрица T есть произведение блочно-диагональной матрицы на блочно-перестановочную, показатели рассеивания матриц A и $A^\top$ совпадают.

3. Пусть $\widehat{a}$ — инволюция, $n = 2k$. Тогда $a(x)^2 \equiv 1 \bmod (x^{2k} + 1)$. Это значит, что для некоторого многочлена $t(x)$ справедливо равенство $a(x)^2 = 1 + (x^{2k} + 1)t(x)$, то есть $(a(x) + 1)^2 = (x^{2k} + 1)t(x)$. Следовательно, $t(x)$ является квадратом, и для $t(x) = t_1(x)^2$ имеем $a(x) + 1 = (x^k + 1)t_1(x)$. Рассмотрим действие преобразования $\widehat{a}$ на многочлен $x^k + 1$: $(x^k + 1)a(x) = (x^k + 1)((x^k + 1)t_1(x) + 1) =$

$(x^k+1)(x^k+1)(t_1(x))+(x^k+1) \equiv (x^k+1) \bmod x^{2k}+1$. То есть многочлен x^k+1, соответствующий вектору веса 2, переходит в себя и показатель рассеивания преобразования $\widehat{a}$ не превышает 4.

□

Первый пункт утверждения 3 позволяет быстрее находить показатель рассеивания преобразования $\widehat{a}_{x^n+1}$ путем перебора подматриц [18]. Второй пункт означает, что для матриц-циркулянтов показатели рассеивания матриц A, A^{-1}, $A^\top$, $(A^\top)^{-1}$ совпадают, что важно для стойкости схемы по отношению к разностному и линейному методам криптоанализа [16], [22]. Третий пункт означает, что среди преобразований указанного вида нет инволютивных преобразований с высоким показателем рассеивания.

Перебором на вычислителях были найдены преобразования вида $A_{a(x),x^n+1}$ со следующими показателями рассеивания на s-подвекторах (см. таблицу 1). MP означает максимально рассеивающую матрицу.

Таблица 1 — Максимальный найденный показатель рассеивания двоичных циркулянтных матриц.

Размер матрицы \ Размер s-подвектора	4-bit	6-bit	8-bit
4×4	5 (MP)	5 (MP)	5 (MP)
6×6	6	6	6
8×8	7	-	8
16×16	12	-	-

2.2 Разложение матрицы в сумму матриц вида $A_{a(x),f(x)}$

Поскольку среди матриц вида $A_{a(x),f(x)}$ над $P = \mathbb{F}_2$ не удаётся найти максимально рассеивающие размерностей больших, чем 4, имеет смысл перейти к матрицам с более сложной реализацией.

Пусть $A \in P_{n\times n}$, $f(x)$ – многочлен над P степени n, свободный член $f(x)$ равен 1, $a_i(x)$ – многочлены над P степени меньше n, $i \in \overline{1,t}$.

Рассмотрим разложение

$$A = \sum_{i=1}^{t} D_i A_i, \tag{2.3}$$

где $D_i = diag_{n\times n}(d_{i,n-1},...,d_{i,0}), d_{i,j} \in \{0,1\}, A_i = A_{a_i(x),f(x)}$ – матрицы над P размера $n \times n$, определённые в (2.1). Отметим, что разложение (2.3) для матрицы A зависит от выбора многочлена $f(x)$.

Как указано в разделе 2.1, умножение на матрицы D_i реализуется командой AND, на матрицы A_i – в соответствии с утверждением 2.2. Сумма реализуется командой XOR. Для эффективной реализации матрицы A необходимо стремиться к уменьшению числа слагаемых в сумме (2.3). С учётом результатов утверждения 2.2 очевидно следующее

Утверждение 2.4. *Пусть для матрицы A и многочлена $x^n + 1$ справедливо разложение (2.3). Тогда умножение вектора на матрицу A может быть выполнено с использованием команд процессора: t команд AND, t команд $CLMUL$ и $2t - 1$ команд XOR.*

Определение 2.2. Определим преобразование $Rev_{f(x)} : P_{n,n} \to P_{n,n}$. Результатом его действия на матрицу A является матрица B, в которой каждая строка $\overrightarrow{B_i} = \overrightarrow{A_i} \cdot A^{-i}_{x,f(x)}$. Иными словами, каждая строка $\overrightarrow{B_i}$ есть i-я строка матрицы A, к которой i раз применили преобразование, обратное умножению соответствующего многочлена $\overrightarrow{A_i}(x)$ на многочлен x по модулю $f(x)$. Обратное преобразование всегда существует, поскольку свободный член $f(x)$ равен 1.

Теорема 2.1. *Минимальное число слагаемых t в сумме (2.3) совпадает с рангом матрицы $B = Rev_{f(x)}(A)$.*

Доказательство. Поскольку преобразование $\overrightarrow{a} \to \overrightarrow{a} \cdot A^{-1}_{x,f(x)}$ является дистрибутивным относительно операции XOR и перестановочным с операцией AND, следующая цепочка равенств равносильна равенству (2.3):

$$Rev_{f(x)}(A) = Rev_{f(x)}(\sum_{i=1}^{t} D_i A_i) = \sum_{i=1}^{t} Rev_{f(x)}(D_i A_i) = \sum_{i=1}^{t} D_i Rev_{f(x)}(A_i) \tag{2.4}$$

Поскольку A_i – матрицы вида (2.1), в матрице $Rev_{f(x)}(A_i)$ все строки равны между собой и равны нулевой строке матрицы A_i. Следовательно, равенство (2.4) равносильно совокупности равенств:

$$\overrightarrow{B}_j = \sum_{i=1}^{t} d_{i,j} \overrightarrow{A}_{i,0}, \quad j \in \overline{1,n}.$$

Значит, равенство (2.4) равносильно тому, что каждая строка матрицы $B = Rev_{f(x)}(A)$ линейно выражается через совокупность строк $\overrightarrow{A}_{i,0}$, $i \in \overline{1,t}$ и число t совпадает с рангом матрицы B. □

Теорема 2.1 при заданном многочлене $f(x)$ позволяет легко найти минимальное число слагаемых t в разложении (2.3). Для $f(x) = x^n + 1$ и небольших t соответствующее линейное преобразование может быть эффективно реализовано с использованием утверждения 2.4.

2.3 Разложение матриц-циркулянтов над полем $\mathbb{F}_{2^s}$

Обозначим поля $P = \mathbb{F}_2$, $Q = (P[x]/g(x), +, \cdot)$, $g(x)$ – некоторый неприводимый многочлен степени s над полем P, $Q \cong \mathbb{F}_{2^s}$, $f(x) = x^n + 1$.

Утверждение 2.5. *Пусть $C_{m\times m}$ – матрица-циркулянт над полем Q, $n = ms$, $A_{n\times n} = A(C, g(x))$ – двоичная матрица, реализующая соответствующее C преобразование на двоичных векторах длины n. Тогда.*

1. *Для матрицы A и многочлена $x^n + 1$ существует разложение вида (2.3), содержащее не более s слагаемых.*
2. *Если при этом двоичное представление каждого элемента матрицы C содержит ненулевые элементы лишь во младших k разрядах, существует разложение вида (2.3), содержащее не более k слагаемых.*

Доказательство. Пусть

$$A_{n\times n} = \begin{pmatrix} \overrightarrow{A}_{n-1} \\ \dots \\ \overrightarrow{A}_1 \\ \overrightarrow{A}_0 \end{pmatrix}, C_{m\times m} = \begin{pmatrix} c_0 & c_{m-1} & \dots & c_2 & c_1 \\ c_1 & c_0 & \dots & c_3 & c_2 \\ \dots & \dots & \dots & \dots & \dots \\ c_{m-2} & c_{m-3} & \dots & c_0 & c_{m-1} \\ c_{m-1} & c_{m-2} & \dots & c_1 & c_0 \end{pmatrix} = \begin{pmatrix} \overrightarrow{C}_{m-1} \\ \dots \\ \overrightarrow{C}_1 \\ \overrightarrow{C}_0 \end{pmatrix}.$$

Для получения матрицы A необходимо элементы c_i матрицы C заменить матрицами над полем P, реализующими соответствующее преобразование

(умножение на элемент поля). Такие матрицы имеют вид (2.1) и размер $s \times s$. Значит, каждая строка $\overrightarrow{C}_i$ представляется строками $\overrightarrow{A}_{is}$, $\overrightarrow{A}_{is+1}$,..., $\overrightarrow{A}_{is+s-1}$. Поскольку каждая строка $\overrightarrow{C}_i$ есть циклический сдвиг влево строки $\overrightarrow{C}_{i-1}$, при любых $i \in \overline{1,n-1}$, $k \in \overline{0,s-1}$ строка $\overrightarrow{A}_{is+k}$ есть циклический сдвиг строки $\overrightarrow{A}_{(i-1)s+k}$ на s разрядов влево.

Положим A_k, $k \in \overline{0,s-1}$ – матрица-циркулянт размера $n \times n$ над P, заданная строкой $\overrightarrow{A}_k$ матрицы A. Из сказанного выше следует, что строки с номерами $is+k, i \in \overline{0,n-1}$ в матрицах A и A_k совпадают. Положим в качестве D_k диагональную матрицу размера $n \times n$ над $\mathbb{F}_2$, в которой единицы стоят лишь на позициях с номерами $is+k, i \in \overline{0,n-1}$. Из построения матриц A_k и D_k следует искомое равенство:

$$A = \sum_{i=0}^{s-1} D_i A_i \tag{2.5}$$

Для доказательства пункта 2 достаточно заметить, что в соответствии с формулами построения матриц $A_{c_i(x),g(x)}$ (2.1) по элементам матрицы C каждая строка построенной матрицы с номером $j \in \overline{1,s-k}$ есть свдиг влево строки с номером $j-1$. Приведение по модулю $g(x)$ в этом случае не происходит, поскольку старший бит каждой строки с номером, меньшим j, нулевой. Это значит, что матрицы $A_0, ..., A_{s-k}$ совпадают и что, просуммировав матрицы D_0,...,D_{s-k}, можно заменить слагаемые $D_0A_0 + ... + D_{s-k}A_{s-k}$ одним. В сумме остаётся k слагаемых. □

Приведём несколько примеров применения утверждения 2.5. Обозначим $Diag(0x\boldsymbol{\alpha})$ — диагональная матрица над $\mathbb{F}_2$ подходящего размера, построенная по одинаковым байтам $\boldsymbol{\alpha}$. Так, в примере 2.1 $Diag(0x20) = diag(0x20, 0x20, 0x20, 0x20, 0x20, 0x20, 0x20, 0x20) \in P_{64,64}$. Приведённые разложения позволяют с использованием утверждения 2.4 предложить альтернативные реализации рассматриваемых линейных преобразований.

Пример 2.1. Рассмотрим матрицу $A(W,g(x))$, используемую в линейном преобразовании хэш-функции Whirlpool, где матрица $W = Circ_{2^8}(0x01, 0x04, 0x01, 0x08, 0x05, 0x02, 0x09, 0x01)$ – матрица-циркулянт над полем $\mathbb{F}_{2^8}$ размера 8×8 и $g(x) = x^8 + x^4 + x^3 + x^2 + 1$. Заметим, что двоичное представление каждого элемента W (совпадает с двоичным представлением соответствующего числа) содержит лишь 4 активных разряда — 4 младших

разряда. Значит, по утверждению 2.5, для матрицы $A(W,g(x))$ существует разложение вида (2.3) из 4-х слагаемых. Приведём его:

$$A(W,g(x)) = Circ_2(0x01, 0x04, 0x01, 0x08, 0x05, 0x02, 0x09, 0x01)+$$
$$+ Diag(0x20)Circ_2(0x00, 0x00, 0x00, 0x08, 0xe8, 0x00, 0x08, 0xe8)+$$
$$+ Diag(0x40)Circ_2(0x00, 0x04, 0x74, 0x08, 0xec, 0x74, 0x08, 0xe8)+$$
$$+ Diag(0x80)Circ_2(0x00, 0x04, 0x74, 0x08, 0xec, 0x76, 0x32, 0xe8).$$

Пример 2.2. Рассмотрим максимально рассеивающую матрицу $V = Circ_{2^8}(0x01, 0x02, 0x03, 0x05, 0x04, 0x03, 0x07, 0x07)$ с параметрами, аналогичными параметрам матрицы Whirlpool. По утверждению 2.5, для матрицы $A(V,g(x))$, где $g(x) = x^8 + x^4 + x^3 + x^2 + 1$, существует разложение вида (2.3) из 3-х слагаемых. Приведём его:

$$A(V,g(x)) = Circ_2(0x01, 0x02, 0x03, 0x05, 0x04, 0x03, 0x07, 0x07)+$$
$$+ Diag(0x40)Circ_2(0x74, 0x00, 0x00, 0x04, 0x70, 0x74, 0x04, 0x70)+$$
$$+ Diag(0x80)Circ_2(0x4e, 0x02, 0x38, 0x3e, 0x70, 0x76, 0x3c, 0x48).$$

Пример 2.3. Рассмотрим матрицу $A(L,g(x))$, используемую в линейном преобразовании шифрсистемы AES, где матрица $L = Circ_{2^8}(0x03, 0x01, 0x01, 0x02)$ – матрица-циркулянт над полем $\mathbb{F}_{2^8}$ размера 4×4 и $g(x) = x^8 + x^4 + x^3 + x + 1$. По утверждению 2.5, для матрицы $A(L,g(x))$ существует разложение вида (2.3) из 2-х слагаемых. Приведём его:

$$A(L,g(x)) = Circ_2(0x03, 0x01, 0x01, 0x02)+$$
$$+ Diag(0x80)Circ_2(0x34, 0x36, 0x00, 0x02).$$

Выводы по главе. В главе 2 были рассмотрены эксплуатационные характеристики линейных преобразований, заданных умножением на элемент кольца. Такие преобразования допускают эффективную программную реализацию, особенно в случае когда кольцом является кольцо матриц-циркулянтов над полем $\mathbb{F}_2$. Максимально рассеивающая на s-подвекторах матрица-циркулянт над $\mathbb{F}_2$ используется в шифрсистеме SM4. Её программная реализация может быть выполнена за две команды процессора CLMUL и XOR.

Недостатком класса двоичных матриц-циркулянтов является отсутствие теоретических методов построения максимально рассеивающих матриц больших размерностей (максимум 32×32 — матрица SM4). Поисковые методы

также не приводят к результатам. В связи с этим предлагается исследовать разложения произвольной матрицы в сумму произведений диагональных матриц и матриц-циркулянтов. В данной главе получены оценки на число слагаемых в указанном разложении. Небольшое число слагаемых удаётся получить в случае разложения матриц-циркулянтов, построенных над полем $\mathbb{F}_{2^s}$. Соответствующие разложения представлены для матриц, используемых в линейных преобразованиях шифрсистемы AES и хэш-функции Whirlpool.

Глава 3. Разложение рекурсивных матриц

В главе 2 рассматривались программные реализации линейных преобразований, заданных циркулянтными матрицами. В данной главе будет рассмотрен ещё один важный класс линейных преобразований — рекурсивные матрицы. Для матриц из данного класса существуют способы построения максимально рассеивающих матриц больших размерностей с использованием рекурсивных МДР-кодов [62]. Таким образом была получена матрица линейного преобразования шифрсистемы Кузнечик. Используются также поисковые методы построения рекурсивных матриц путём перебора коэффициентов характеристического многочлена, таким образом получены матрицы линейного преобразования, используемые в семействе хэш-функций PHOTON [10].

Помимо стандартной реализации XSL-схемы с использованием LUT-таблиц [52] рекурсивные матрицы могут быть реализованы через вычисление элементов линейной рекуррентной последовательности (реализации описаны в разделе 3.4). В данной главе будут получены другие варианты реализации рекурсивных линейных преобразований. Реализация через разложение рекурсивной матрицы по скорости шифрования лишь немногим уступает реализации с использованием предвычисленных LUT-таблиц, при этом требует кратно меньше памяти и может быть полезна для малоресурсных устройств с программной реализацией шифрования.

Для получения соответствующих разложений были найдены все решения уравнения подобия сопровождающей матрицы многочлена над конечным полем $S(f(x))$ и матрицы $S(f(x))^\top$. Теоретические результаты главы представлены в общем виде, над произвольным конечным полем $\mathbb{F}_{q^s}$. В разделе 3.1 показано, что как и матрица-циркулянт, транспонированная рекурсивная матрица также задаётся через умножение на элемент кольца.

В заключительном разделе главы 3 представлено сравнение различных программных реализаций шифрсистемы Кузнечик.

Результаты главы опубликованы в работах [71; 72].

3.1 Линейные преобразования, заданные через умножение на элемент кольца

В главе 2 введено определение линейных преобразований, заданных через умножение на элемент кольца и показано, что матрицы-циркулянты над полем $\mathbb{F}_2$ являются такими преобразованиями. Приведём примеры соответствующих преобразований над полем $Q = \mathbb{F}_{q^s}$.

Пример 3.1. *Матрица-циркулянт.* Матрица-циркулянт реализует умножение в кольце $R = Q[x]/(x^m - 1)$. Аналогично двоичному случаю (см. утверждение 2.2), для того чтобы умножить $a(x)$ на $b(x)$ в R достаточно выполнить умножение $a(x) \cdot b(x) = c(x)$ в кольце $Q[x]$ и затем сложить младшую и старшую координатные половины результата $(c_{2m-1},...,c_m) + (c_{m-1},...,c_0)$.

Пример 3.2. *Транспонирование сопровождающей матрицы.* Пусть $S = S(f(x))$ — сопровождающая матрица многочлена $f(x)$, тогда матрица $S^\top$ имеет вид:

$$S^\top = \begin{pmatrix} f_{m-1} & f_{m-2} & \dots & f_1 & f_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Матрица $S^\top$ реализует умножение на элемент x в кольце $R = Q[x]/f(x)$. Матрица $(S^m)^\top = (S^\top)^m$ реализует умножение на элемент x^m в том же кольце. В случае неприводимости многочлена $f(x)$ кольцо R является полем.

Поскольку матрицы S^m и $(S^m)^\top$ являются подобными, рекурсивное преобразование S^m также является умножением на элемент кольца x^m, но в другом базисе. Это означает, что выполнить рекурсивное преобразование S^m можно в три этапа:

1. перейти в базис, в котором матрица преобразования имеет вид $(S^\top)^m$;
2. выполнить умножение на элемент кольца x^m;
3. вернуться в исходный базис.

Найдем всевозможные матрицы C, которые выполняют переход между вышеуказанными базисами.

Теорема 3.1. *Для сопровождающей матрицы $S = S(f(x))$ выполняется равенство $S = C^{-1}S^{\top}C$ тогда и только тогда, когда C обратимая матрица вида:*

$$C = \begin{pmatrix} c_{2m-2} & c_{2m-3} & \dots & c_m & c_{m-1} \\ c_{2m-3} & c_{2m-4} & \dots & c_{m-1} & c_{m-2} \\ \dots & \dots & \dots & \dots & \dots \\ c_m & c_{m-1} & \dots & c_2 & c_1 \\ c_{m-1} & c_{m-2} & \dots & c_1 & c_0 \end{pmatrix}, \tag{3.1}$$

где $(c_{2m-2},\dots,c_0)$ - последовательные элементы ЛРП с характеристическим многочленом $f(x)$. Матрица вида (3.1) является Ганкелевой матрицей.

Доказательство. Для обратимой матрицы C равенство $S = C^{-1}S^{\top}C$ равносильно равенству $CS = S^{\top}C$ или

$$\begin{pmatrix} \overrightarrow{C}_{m-1}f^{\downarrow} & C^{\downarrow}_{m-1} & \dots & C^{\downarrow}_{1} \\ \overrightarrow{C}_{m-2}f^{\downarrow} & \dots & \dots & \dots \\ \overrightarrow{C}_{m-3}f^{\downarrow} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \overrightarrow{C}_{0}f^{\downarrow} & \dots & \dots & \dots \end{pmatrix} = \begin{pmatrix} \overrightarrow{f}C^{\downarrow}_{m-1} & \overrightarrow{f}C^{\downarrow}_{m-2} & \dots & \overrightarrow{f}C^{\downarrow}_{0} \\ \overrightarrow{C}_{m-1} & \dots & \dots & \dots \\ \overrightarrow{C}_{m-2} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \overrightarrow{C}_{1} & \dots & \dots & \dots \end{pmatrix},$$

где $\overrightarrow{f} = (f_{m-1},\dots,f_0)$ — вектор соответствующих коэффициентов многочлена $f(x)$.

Рассмотрим подматрицы указанных выше матриц с номерами строк и столбцов от 0 до $m-2$:

$$\begin{pmatrix} c_{m-2,m-1} & c_{m-2,m-2} & \dots & c_{m-2,1} \\ c_{m-3,m-1} & c_{m-3,m-2} & \dots & c_{m-3,1} \\ \dots & \dots & \dots & \dots \\ c_{0,m-1} & c_{0,m-2} & \dots & c_{0,1} \end{pmatrix} = \begin{pmatrix} c_{m-1,m-2} & c_{m-1,m-3} & \dots & c_{m-1,0} \\ c_{m-2,m-2} & c_{m-3,m-3} & \dots & c_{m-2,0} \\ \dots & \dots & \dots & \dots \\ c_{1,m-2} & c_{1,m-3} & \dots & c_{1,0} \end{pmatrix}.$$

Равенство указанных подматриц равносильно тому, что матрица C имеет вид (3.1). В силу симметричности матрицы C равенство $(m-1)$-х строк матриц CS и $S^{\top}C$ равносильно равенству $(m-1)$-х столбцов тех же матриц. Равенство $(m-1)$-х строк указанных матриц равносильно системе уравнений:

$$\begin{cases} c_{m-1,m-1} = \overrightarrow{f} C_{m-2}^{\downarrow} \\ c_{m-1,m-2} = \overrightarrow{f} C_{m-3}^{\downarrow} \\ \ldots \\ c_{m-1,1} = \overrightarrow{f} C_{0}^{\downarrow} \end{cases}$$

или, с учетом элементов матрицы (3.1):

$$\begin{cases} c_{2m-2} = \overrightarrow{f} C_{m-2}^{\downarrow} \\ c_{2m-3} = \overrightarrow{f} C_{m-3}^{\downarrow} \\ \ldots \\ c_{m} = \overrightarrow{f} C_{0}^{\downarrow} \end{cases} \tag{3.2}$$

Условие (3.2) равносильно тому, что элементы $(c_{2m-2},\ldots,c_0)$ есть последовательные элементы ЛРП с характеристическим многочленом $f(x)$. □

3.2 Выбор матрицы перехода C в уравнении подобия рекурсивной матрицы

Для эффективности реализации линейного преобразования рекурсивной матрицы в качестве матрицы подобия можно выбирать матрицы с наибольшим числом нулей. Поскольку элементы матрицы подобия C лежат на ЛРП с характеристическим многочленом степени m, для однозначного задания матрицы C достаточно выбрать m последовательных элементов в последовательности $(c_{2m-2},\ldots,c_0)$. Если выбрать m нулевых элементов, все элементы ЛРП будут равны нулю и матрица C будет нулевой. В данном разделе рассматриваются два варианта выбора последовательных элементов ЛРП, среди которых $m-1$ нулевой и один единичный.

Предварительно докажем вспомогательное утверждение.

Утверждение 3.1. *Пусть* $f(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0$ *— многочлен над полем* Q, $k \leqslant m$ *и матрицы* $C \in Q_{k,k}$ *и* $C' \in Q_{k,k}$ *имеют вид:*

$$C = \begin{pmatrix} c_{k-1} & c_{k-2} & ... & c_1 & c_0 \\ c_{k-2} & c_{k-3} & ... & c_0 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & c_0 & ... & 0 & 0 \\ c_0 & 0 & ... & 0 & 0 \end{pmatrix}, C' = \begin{pmatrix} 0 & 0 & ... & 0 & c_0 \\ 0 & 0 & ... & c_0 & c_1 \\ ... & ... & ... & ... & ... \\ 0 & c_0 & ... & c_{k-3} & c_{k-2} \\ c_0 & c_1 & ... & c_{k-2} & c_{k-1} \end{pmatrix},$$

где (c_{k-1},...,c_0,0,...,0) $-$ $m+k-1$ *последовательных элемента ЛРП с характеристическим многочленом* $f(x)$. *Тогда обратными матрицами к матрицам* C *и* C' *соответственно будут следующие матрицы:*

$$C^{-1} = c_0^{-1} \cdot \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_{m-k+3} & -f_{m-k+2} \\ 1 & -f_{m-1} & ... & -f_{m-k+2} & -f_{m-k+1} \end{pmatrix},$$

$$(C')^{-1} = c_0^{-1} \cdot \begin{pmatrix} -f_{m-k+1} & -f_{m-k+2} & ... & -f_{m-1} & 1 \\ -f_{m-k+2} & -f_{m-k+3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ -f_{m-1} & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

Доказательство. Обозначим первую из указанных выше матриц (C^{-1}) как F и покажем, что $FC = E$. Заметим, что в i-й строке матрицы F последние i элементов нулевые, а в j-м столбце матрицы C первые $m-1-j$ элементов нулевые. Посчитаем элемент

$$(fc)_{ij} = \overrightarrow{F}_i C_j^{\downarrow} \tag{3.3}$$

в 3 случаях.

1. i $>$ j. Тогда $i+m-1-j \geqslant m$ и в произведении (3.3) нет ненулевых слагаемых, поэтому произведение равно нулю.
2. i $=$ j. Тогда $i+m-1-j = m-1$ и единственное ненулевое слагаемое в произведении (3.3) есть $f_{i,i}c_{i,i} = c_0^{-1} \cdot c_0 = 1$.
3. i $<$ j. Тогда (3.3) без учета нулевых слагаемых будет равно

$$c_0^{-1}[(1 \cdot c_{j-i} - f_{m-1}c_{j-i-1} - ... - f_{m-(j-i)} \cdot c_0) = \\ (1 \cdot c_{j-i} - ... - f_{m-(j-i)} \cdot c_0 - f_{m-(j-i)-1} \cdot 0 - ... - f_0 \cdot 0)].$$

Поскольку вектор $(c_{j-i}, c_{j-i-1},...,c_1,c_0,0,...,0)$ состоит из последовательных элементов ЛРП с характеристическим многочленом $f(x)$, последнее выражение равно нулю.

Таким образом, $(fc)_{ij} = 0$ при $i \neq j$ и $(fc)_{ij} = 1$ при $i = j$, значит матрица FC есть единичная матрица.

Заметим, что $C' = TCT$ (см. свойства матрицы T в (1.3)). Тогда $(C')^{-1} = TC^{-1}T$. □

Перейдём к выбору матрицы подобия C.

Утверждение 3.2. *Пусть в условиях теоремы 3.1* $m = 2k$ *и* $c_k = ... = c_{3k-2} = 0, c_{3k-1} = 1$, *тогда матрицы* C *и* C^{-1} *в разложении*

$$C^{-1}(S^\top)^m C = S^m \tag{3.4}$$

состоят из двух блоков размера $k \times k$ *и имеют следующий вид:*

$$C = diag\left(\begin{pmatrix} c_{2m-2} & c_{2m-3} & ... & c_{2m-k} & 1 \\ c_{2m-3} & c_{2m-4} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_{2m-k} & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & ... & 0 & c_{k-1} \\ 0 & 0 & ... & c_{k-1} & c_{k-2} \\ ... & ... & ... & ... & ... \\ 0 & c_{k-1} & ... & c_2 & c_1 \\ c_{k-1} & c_{k-2} & ... & c_1 & c_0 \end{pmatrix}\right) \tag{3.5}$$

$$C^{-1} = diag\left(\begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_{m-k+3} & -f_{m-k+2} \\ 1 & -f_{m-1} & ... & -f_{m-k+2} & -f_{m-k+1} \end{pmatrix}, \begin{pmatrix} f_{k-1} & f_{k-2} & ... & f_1 & f_0 \\ f_{k-2} & f_{k-3} & ... & f_0 & 0 \\ ... & ... & ... & ... & ... \\ f_1 & f_0 & ... & 0 & 0 \\ f_0 & 0 & ... & 0 & 0 \end{pmatrix}\right) \tag{3.6}$$

где $(c_{2m-1},c_{2m-2},...,c_{2m-k+1},1,0,...,0)$ $-$ $m+k-1$ *последовательных элементов ЛРП с характеристическим многочленом* $f(x)$, $(c_0,c_1,...,c_{k-1},0,...,0)$ $-$ $m+k-1$ *последовательных элементов ЛРП с характеристическим многочленом* $f^*(x)$ *(см. (1.2)).*

Доказательство. Поскольку в матрице (3.1) элементы c_k,...,c_{3k-2} равны нулю, матрица C является блочно-диагональной с двумя блоками размера $k \times k$, причем блоки будут иметь вид, как в матрице (3.5). Поскольку в матрице (3.1) элементы (c_{2m-2},...,c_0) образуют ЛРП с характеристическим многочленом $f(x)$, для того, чтобы найти элементы (c_{2m-2},c_{2m-3},...,c_{m+1},1,0,...,0) и (c_0,c_1,...,c_{k-1},0,...,0) в матрице (3.5) достаточно рассчитать элементы ЛРП с начального состояния $c_k = ... = c_{3k-2} = 0$, $c_{3k-1} = 1$ в прямом направлении на $k-1$ тактов и обратном направлении на k тактов. В прямом направлении вычисление элементов происходит по закону рекурсии, задаваемому многочленом $f(x)$, в обратном — многочленом $f^*(x)$.

Обратная матрица C^{-1} будет состоять из двух блоков размера $k \times k$, каждый из которых является обратной матрицей к соответствующему блоку матрицы C. В соответствии с утверждением 3.1 верхний блок матрицы (3.6) будет обратной матрицей к верхнему блоку матрицы (3.5). Нижний блок матрицы (3.5) составлен из последовательных элементов ЛРП с начальным вектором ($c_{k-1} = f_0^{-1}$,0,...,0) и характеристическим многочленом $f^*(x) = x^m + f_0^{-1}(f_1 x^{m-1} + ... + f_{m-1}x - 1)$. Значит, в соответствии с утверждением 3.1, нижний блок матрицы (3.6) будет обратной матрицей к нижнему блоку матрицы (3.5). □

Утверждение 3.3. *Пусть в условиях теоремы 3.1* $c_0 = ... = c_{m-2} = 0, c_{m-1} = 1$, *тогда матрицы* C *и* C^{-1} *соответственно имеют вид:*

$$C = \begin{pmatrix} c_{2m-2} & c_{2m-3} & ... & c_m & 1 \\ c_{2m-3} & c_{2m-4} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_m & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}, C^{-1} = \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_3 & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix}, \quad (3.7)$$

где (c_{2m-2},c_{2m-3},...,c_m,1,0,...,0) - *последовательные элементы ЛРП длины* $2m-1$ *с характеристическим многочленом* $f(x) = x^m - f_{m-1}x^{m-1} - ... - f_1 x - f_0$.

Доказательство. Утверждение 3.3 напрямую следует из теоремы 3.1 и утверждения 3.1. □

3.3 Разложение рекурсивных матриц

Теорема 3.2. *Пусть* $f(x) = x^m - f_{m-1}x^{m-1} - ... - f_0$ *— многочлен над полем* $Q = \mathbb{F}_{q^s}$, $S = S(f)$ *— его сопровождающая матрица,* $A = S^m$ *— рекурсивная матрица. Пусть* $\overrightarrow{E}_{m-1} \cdot S^{m-1} = (c_{m-1},...,c_1,1)$. *Тогда справедливо следующее разложение матрицы* A *в произведение матриц* $F \cdot C$*:*

$$A = \begin{pmatrix} f_{m-1} & f_{m-2} & ... & f_1 & f_0 \\ f_{m-2} & f_{m-3} & ... & f_0 & 0 \\ ... & ... & ... & ... & ... \\ f_1 & f_0 & ... & 0 & 0 \\ f_0 & 0 & ... & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_{m-1} & c_{m-2} & ... & c_1 & 1 \\ c_{m-2} & c_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix} \quad (3.8)$$

Доказательство. В условиях утверждения 3.3 с перенумерованием индексов элементов c_i разложение матрицы S^m имеет вид $S^m = C^{-1}(S^\top)^m C =$

$$\begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & -f_3 & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix} (S^\top)^m \begin{pmatrix} c_{m-1} & c_{m-2} & ... & c_1 & 1 \\ c_{m-2} & c_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

Матрица $(S^\top)^m$ реализует умножение на элемент кольца x^m. При умножении матрицы C^{-1} на матрицу $(S^\top)^m$ каждая строка матрицы C^{-1} умножается на матрицу $(S^\top)^m$, то есть каждый элемент $\overrightarrow{C}_i^{-1}$ кольца $Q[x]/f(x)$ умножается на x^m.

$$\overrightarrow{C}_i^{-1} \cdot x^{i+1} \ mod \ f(x) = (x^m - f_{m-1}x^{m-1} - ... - f_{i+1}x^{i+1}) - \\ - (x^m - f_{m-1}x^{m-1} - ... - f_1 x - f_0) = f_i x^i + ... + f_1 x + f_0.$$

Значит $\overrightarrow{C}_i^{-1} \cdot x^m \ mod \ f(x) = f_i x^{m-1} + ... + f_0 x^{m-1-i}$ и $\overrightarrow{C}_i^{-1} \cdot x^m \ mod \ f(x)$ $= (f_i,...,f_0,0,...,0)$. □

Следствие 3.1. *Пусть выполнены условия теоремы 3.2,* $g(x) = f^*(x)$ *и* $f_0^{-1}\overrightarrow{E}_{m-1}S(g)^{m-1} = (d_{m-1},...,d_1,d_0)$, $d_0 = f_0^{-1}$. *Тогда обратной матрицей к матрице* $A = S(f)^m$ *будет следующая матрица:*

$$A^{-1} = \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & -f_{m-1} \\ ... & ... & ... & ... & ... \\ 0 & 1 & ... & ... & -f_2 \\ 1 & -f_{m-1} & ... & -f_2 & -f_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & ... & 0 & d_0 \\ 0 & 0 & ... & d_0 & d_1 \\ ... & ... & ... & ... & ... \\ 0 & d_0 & ... & ... & d_{m-2} \\ d_0 & d_1 & ... & d_{m-2} & d_{m-1} \end{pmatrix} \quad (3.9)$$

Доказательство. Заметим, что первую матрицу в произведении (3.8) можно представить, как:

$$f_0 \cdot \begin{pmatrix} f_0^{-1}f_{m-1} & f_0^{-1}f_{m-2} & ... & f_0^{-1}f_1 & 1 \\ f_0^{-1}f_{m-2} & f_0^{-1}f_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ f_0^{-1}f_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix}$$

Тогда, в соответствии с утверждением 3.1, первая и вторая матрицы в произведении (3.9) являются обратными матрицами ко второй и первой матрицам соответственно в произведении (3.8). □

3.4 Реализации рекурсивных матриц

3.4.1 Известные реализации

Далее в данной главе $q = 2$. Автору известны следующие варианты программной реализации линейных преобразований, задаваемых рекурсивными матрицами.

1. Реализация линейного регистра сдвига (вычисление элементов ЛРП на m тактов вперёд).
2. Реализация линейного регистра сдвига с предвычисленной таблицей умножения в поле $\mathbb{F}_{2^s}$. Данная реализация отличается от реализации 1 лишь тем, что вместо умножения в поле выполняется обращение в соответствующую область памяти. Поскольку при вычислении элементов ЛРП умножение выполняется только на коэффициенты многочлена f,

в памяти необходимо хранить лишь m строк таблицы умножения ($m \cdot 2^s$ элементов поля).

3. Использование предвычисленных LUT-таблиц из $m^2 \cdot 2^s$ элементов поля $\mathbb{F}_{2^s}$ [52].

Первый вариант достаточно медленный ввиду очень большого числа выполняемых операций. Второй вариант существенно быстрее первого, но требует хранения небольшой таблицы в памяти. Третий вариант применим к любой XSL-схеме (не обязательно с рекурсивным линейным преобразованием) и является самым быстрым на современных процессорах с достаточным объёмом кэш-памяти. Однако в случае когда шифрование реализуется на вычислителе с небольшими ресурсами, третий вариант может не удовлетворять ограничениям по используемой памяти.

Разложения рекурсивной матрицы вида (3.4) и (3.8) позволяют предложить новые варианты выполнения SL-преобразования, являющиеся компромиссными по количеству операций и объёму используемой памяти.

3.4.2 Реализация через разложение рекурсивной матрицы

Результат умножения вектора $\overrightarrow{a} = (a_{m-1},...,a_0)$ на матрицу A можно вычислить, посчитав линейную комбинацию строк матрицы A : $\overrightarrow{a}A = a_{m-1}\overrightarrow{A}_{m-1} + ... + a_0\overrightarrow{A}_0$. Для матриц F и C из (3.8) строки с номером i, умноженные на произвольный элемент поля $a_i \in Q$, могут быть получены сдвигом строки с номером $m-1$, умноженной на тот же элемент поля a_i на $m-1-i$ позиций влево. Если заранее вычислить произведение строки $\overrightarrow{F}_{m-1} = (f_{m-1},...,f_0)$ на все элементы поля Q, то при зашифровании вычислять $a_i\overrightarrow{F}_i$ можно путем обращения в соответсвующую область памяти и сдвигом на $(m-1-i)$ элементов влево. Аналогичный результат справедлив для матрицы C.

Для выполнения L-преобразования умножим поступивший вектор последовательно на матрицы F и C указанным выше способом. Для совмещения преобразований S и L в одно достаточно в предвычисленной таблице матрицы F по адресу $a \in Q$ хранить результат умножения $S(a) \cdot \overrightarrow{F}_{m-1}$.

Указанные таблицы для матриц F и C требуют хранения $2m \cdot 2^s$ элементов поля Q, что в $m/2$ раз меньше, чем в третьм варианте реализации и в 2

раза больше, чем во втором варианте реализации. При расшифровании можно использовать разложеине (3.9).

3.4.3 Реализация через умножение на элемент кольца (поля)

В указанной реализации необходимо последовательно выполнить умножение поступающего на вход L-преобразования вектора на 3 матрицы из равенства (3.4). Матрица $(S^\top)^m$ реализует умножение в кольце R на элемент x^m. Матрицы C^{-1} и C реализуют переход в соответствующий базис и возврат в исходный базис.

Выполнять умножение на матрицы C^{-1} и C можно способом, указанным в предыдущем пункте. Для этого потребуется хранить $m \cdot 2^s$ элементов поля для каждой матрицы (в случае некоторых шифрсистем, например шифрсистемы Кузнечик, оценка может быть меньше).

Выполнять умножение на x^m в кольце R можно путем m-кратного умножения на x. Для умножения на x в кольце R необходимо сдвинуть элементы вектора $(a_{m-1},...,a_0)$ влево на одну позицию и привести результат по модулю $f(x)$. Для приведения по модулю, к результату сдвига необходимо добавить $f(x)$, умноженный на a_{m-1}. Поскольку старший коэффициент всегда сокращается, результат умножения на x равен $\varphi[(a_{m-2},...,a_0,0) + (a_{m-1}f_{m-1},...,a_{m-1}f_0)]$.

Если заранее вычислить результаты умножения вектора $\overrightarrow{f} = (f_{m-1},...,f_0)$ на все элементы поля Q, то результат умножения на x можно вычислять за один нециклический сдвиг, одно обращение в память и одно сложение по модулю 2. Указанный способ умножения требует хранения $m \cdot 2^s$ элементов поля. Итого, реализация через умножение на элемент кольца требует хранения $3m \cdot 2^s$ элементов поля в общем случае. Объединение преобразований S и L выполняется аналогично предыдущему пункту.

3.4.4 Новые максимально рассеивающие преобразования

В предыдущем пункте была рассмотрена реализация рекурсивной матрицы $S^m = C^{-1}(S^\top)^m C$ как последовательная реализация матриц C^{-1}, $(S^\top)^m$ и C. Заметим, что сама по себе матрица $(S^\top)^m$ также является максимально рассеивающей матрицей и может быть использована в качестве линейного преобразования. Как было отмечено в предыдущем пункте, реализация такой матрицы требует хранения $m \cdot 2^s$ элементов поля, что в 3 раза меньше, чем в случае (3.4.3) и в 2 раза меньше, чем в случае (3.4.2). Число выполняемых при этом операций также сократится. Недостатком указанного подхода является невозможность объединения преобразований S и L в одно преобразование.

3.5 Сравнение реализаций шифрсистемы Кузнечик

В данном разделе сравниваются 5 различных реализаций шифрсистемы Кузнечик. Все реализации выполнены на языке программирования C++. Автор не ставил перед собой цель добиться максимально быстрого шифрования в каждой из реализаций и не использовал каких-либо средств оптимизации, выходящих за рамки разумного написания кода программы. Цель автора состояла именно в сравнении (приблизительном сравнении) указанных реализаций.

Реализации 1-3 совпадают с реализациями из пункта 3.4.1. Реализация 4 есть реализация через разложение рекурсивной матрицы (см. 3.4.2), реализация 5 есть реализация через умножение на элемент кольца с переходом в соответствующий базис (см. 3.4.3).

Шифрсистема Кузнечик использует следующие параметры $s = 8$ (т. е. нелинейное преобразование S выполняется над 8-битными векторами) и $m = 16$ (т. е. линейное преобразование реализуется матрицей размера 16×16, состоящей из элементов поля $\mathbb{F}_{2^8}$).

Размер S-блока составляет $2^8 \cdot 8$ бит или 256 байт. S-блок необходимо хранить в реализациях 1-2. В реализациях 3-5 преобразования S и L объединены и хранение S-блока не требуется. Поскольку у многочлена f всего 8 различных коэффициентов и один из них равен единице, размер таблицы умножения

для реализации 2 равен $7 \cdot 2^8 \cdot 8$ бит или 1,75 Кбайт. Размер предвычисленных таблиц для реализации 3 равен $16 \cdot 16 \cdot 2^8 \cdot 8$ бит или 64 Кбайта. Размер предвычисленных таблиц для реализации 4 равен $2 \cdot 16 \cdot 2^8 \cdot 8$ бит или 8 Кбайт. Для реализации 5 предвычисленные таблицы $\{a\overrightarrow{f},\ a \in Q\}$ занимают 4 Кбайта. Эти же таблицы заменяют таблицы для матрицы C. В силу условия $f^*(x) = f(x)$ вектор $(c_{15},...,c_8)$ совпадает с вектором $(c_0,...,c_7)$ и для матрицы C^{-1} таблицы занимают 2 Кбайта. Общий объем памяти для реализации 5 равен 6 Кбайт.

Программы выполнялись на одном ядре процессора Intel Core i5-8265U с тактовой частотой 3.9 GHz в режиме Turbo Boost и размерами кэш-памяти первого, второго и третьего уровня соответственно 32 Кбайта, 256 Кбайт и 6 Мбайт(общий для 4 ядер). Для обобщения результатов рассчитана величина cycles per byte (cbp), равная отношению тактовой частоты процессора к скорости шифровашия.

Введем следующие обозначения для операций: XOR — покоординатное сложение по модулю 2, SHFT — сдвиг, MEM — обращение в память, MUL — умножение элементов в поле $\mathbb{F}_{2^8}$. В таблице приведено количество операций за один раунд шифрования для процессора с 64-битной разрядностью (например, наложение раундового ключа длины 128 бит требует одного обращения в память и двух операций XOR).

В объёме памяти учитываются предвычисленные таблицы и S-блок и не учитываются вспомогательные переменные, указатели и пр. Выполнение развертывания ключа, считывание шифруемых данных в оперативную память и запись зашифрованных данных в файл не учитываются при замерах скорости зашифрования. Скорость зашифрования рассчитывалась как $1024/t$ (Мб/сек), где 1024 Мб = 1 Гб — размер подаваемого на шифрование случайного файла, а t — время его зашифрования в режиме CBC в секундах.

Выводы по главе. В главе 3 были рассмотрены линейные преобразования, заданные рекурсивными матрицами. Для сопровождающей матрицы полностью описаны решения уравнения подобия матрицы и транспонированной матрицы, на их основе получены разложения произвольной рекурсивной матрицы в произведение двух матриц определённого вида. На основе разложений предложены новые способы реализации рекурсивных матриц, требующие сравнительно небольшого объёма памяти при сохранении высокой скорости шифрования.

Таблица 2 — Сравнение различных реализаций шифрсистемы Кузнечик.

Реализация линейного преобразования	XOR / SHFT / MEM	Объем памяти	Скорость шифрования	cpb
1. Вычисление ЛРП без таблицы умножения	242/32/17 + 208 MUL	256 байт	1,7 Мб/с	2188
2. Вычисление ЛРП с таблицей умножения	242/32/225	2 Кб	9,7 Мб/с	384
3. Использование предвычисленных LUT-таблиц	34/0/17	64 Кб	113,8 Мб/с	33
4. Разложение рекурсивной матрицы (новая)	50/42/33	8 Кб	87,1 Мб/с	43
5. Умножение на элемент кольца (новая)	66/76/49	6 Кб	27,9 Мб/с	133

Глава 4. Инвариантные подпространства матриц-циркулянтов и рекурсивных матриц

В предыдущих главах изучались S и L преобразования XSL-схем. В данной главе будет рассмотрен метод инвариантных подпространств применительно к XSL-схеме в целом. Поскольку для S преобразований наиболее распространён случай параллельного применения одинаковых S-блоков, в главе будет рассмотрен именно этот случай. Такое ограничение сразу порождает класс инвариантных подпространств преобразования (S,...,S) независимо от S-блока S, данные подпространства описаны в разделе 4.2 и названы подпространствами *вида 1*. Если некоторые из таких подпространств сохраняются преобразованием L, сразу получается инвариантное подпространство раундовой функции. В таком случае оценка применимости метода инвариантных подпространств сводится к алгоритму развёртывания ключа. Если все раундовые ключи (при некотором исходном ключе шифрования) также попадают в указанное подпространство, схема обладает слабыми ключами и является нестойкой.

В разделах 4.4 и 4.5 изучаются инвариантные подпространства циркулянтных и рекурсивных матриц соответственно. Данные матрицы уже изучались в главах 2, 3 с точки зрения эффективной программной реализации. Для матриц-циркулянтов уже известна цепочка вложенных инвариантных подпространств *вида 1* из работы [46]. В данной главе будет показано, что других инвариантных подпространств у максимально рассеивающих матриц-циркулянтов размерности $2^r \times 2^r$ нет. Условие максимального рассеивания является существенным, при отказе от него (вернее, при отказе от условия теоремы 4.2 $c_1 + c_3 + c_5 + ... + c_{2^r-1} \neq 0$), другие инвариантные подпространства точно будут. Условие на размеры матрицы-циркулянта в степень двойки также является существенным.

Для рекурсивных матриц показано отсутствие инвариантных подпространств *вида 1* при условии на корни характеристического многочлена сопровождающей матрицы. При построении рекурсивной максимально рассеивающей матрицы через БЧХ-коды данное условие будет выполнено. В частности, результат справедлив для матрицы линейного преобразования шифрсистемы Кузнечик. Результат показывает неприменимость к шифрсистеме метода инвариантных подпространств с использованием подпространств

вида 1. Отметим, что в работе [50] для шифрсистемы Кузнечик показана неприменимость метода с использованием собственных инвариантных подпространств S-блока, а в работе [49] показана невозможность использовать нелинейные инварианты определённого вида.

Результаты главы представлены в работе [71].

4.1 Основные определения и обозначения

В данной главе используются обозначения $P = \mathbb{F}_2, Q = \mathbb{F}_{2^s}$.
$Sym(X)$ — симметрическая группа подстановок на множестве X.
$\otimes$ — тензорное (кронекерово) произведение матриц.
$N_2(A)$ — вторая нормальная форма матрицы A [57].
Нелинейное преобразование XSL-схемы обозначается $\overline{S}$.
Линейное преобразование XSL-схемы обозначается $\overline{L}$.

Определение 4.1. [58] Пусть на элементах произвольного множества M задано отношение порядка «$\leqslant$». На векторах из M^n определим отношение частичного порядка «$\preceq$: » $(a_{n-1},...,a_0) \preceq (b_{n-1},...,b_0)$ тогда и только тогда, когда для всех $i \in \overline{0,n-1}$ $a_i \leqslant b_i$.

Через $\langle \overrightarrow{\alpha}_0,..., \overrightarrow{\alpha}_{n-1} \rangle$ будем обозначать линейное пространство, порождённое векторами $\overrightarrow{\alpha}_0,..., \overrightarrow{\alpha}_{n-1}$.

Определение 4.2. [57] Пусть W — векторное пространство с базисом $\overrightarrow{\alpha}_0,..., \overrightarrow{\alpha}_{n-1}$ и вектор $\overrightarrow{\beta}$ имеет следующее разложение : $\overrightarrow{\beta} = \overrightarrow{\alpha}_0 b_0 + ... + \overrightarrow{\alpha}_{n-1} b_{n-1}$. Проекцией вектора $\overrightarrow{\beta}$ на подпространство $\langle \overrightarrow{\alpha}_{i_1},..., \overrightarrow{\alpha}_{i_r} \rangle$ называется вектор $PR_{\langle \overrightarrow{\alpha}_{i_1},..., \overrightarrow{\alpha}_{i_r} \rangle}(\overrightarrow{\beta}) = \overrightarrow{\alpha}_{i_1} b_{i_1} + ... + \overrightarrow{\alpha}_{i_r} b_{i_r}$.

Определение 4.3. [57] Пусть $F\colon W \to M$ — произвольное отображение множества W в M, $U \subset W$. Ограничением F на множество U называется отображение $F|_U\colon U \to M$, $F|_U(a) = F(a)$ для любого $a \in U$.

Определение 4.4. [57] Пусть задан вектор $\overrightarrow{\gamma} \in Q^m$ и φ — линейное преобразование Q^m. Минимальным многочленом $m_{\overrightarrow{\gamma},\varphi}(x)$ вектора $\overrightarrow{\gamma}$ относительно линейного преобразования φ называется унитарный многочлен $m(x)$ минимальной степени d, для которого спаведливо $m(\varphi)(\overrightarrow{\gamma}) = \overrightarrow{0}$.

В условиях определения $L^{\varphi}(\overrightarrow{\gamma}) = \langle \overrightarrow{\gamma}, \varphi(\overrightarrow{\gamma}), ..., \varphi^{d-1}(\overrightarrow{\gamma}) \rangle$ — циклическое подпространство, порождённое вектором $\overrightarrow{\gamma}$.

Докажем утверждение, которое пригодится нам в дальнейшей работе.

Утверждение 4.1. *Пусть характеристический многочлен линейного преобразования $\varphi\colon Q^m \to Q^m$ имеет каноническое разложение $\chi_{\varphi}(x) = g_1(x)^{k_1} \ldots g_r(x)^{k_r}$. Тогда для любого собственного инвариантного подпространства W преобразования φ существуют такие $i \in \overline{1,r}$ и $\overrightarrow{\gamma} \in Q^m$, что $m_{\overrightarrow{\gamma},\varphi}(x) = g_i(x)$ и $L^{\varphi}(\overrightarrow{\gamma}) < W$.*

Доказательство. Возьмём произвольное собственное инвариантное подпространство $W = \langle \overrightarrow{\alpha}_k, ..., \overrightarrow{\alpha}_0 \rangle$. Дополним базис W до базиса всего пространства $\langle \overrightarrow{\alpha}_{m-1}, ..., \overrightarrow{\alpha}_{k+1}, \overrightarrow{\alpha}_k, ..., \overrightarrow{\alpha}_0 \rangle$. Матрица линейного преобразования φ в указанном базисе будет иметь полураспавшийся вид $\begin{pmatrix} A_2 & A_1 \\ 0 & A_0 \end{pmatrix}$ и $\chi_{\varphi}(x) = \chi_{A_0}(x)\chi_{A_2}(x)$, значит $\chi_{A_0}(x)$ делит $\chi_{\varphi}(x)$ и существует такое $i \in \overline{1,r}$, что $g_i(x) | \chi_{A_0}(x)$. Тогда по следствию 1 стр. 75 [57] $g_i(x) | m_{A_0}(x)$. По теореме 11 стр. 69 [57] существует такой вектор $\overrightarrow{\gamma} \in W$, что $m_{\overrightarrow{\gamma},\varphi}(x) = g_i(x)$, и по утверждению 22 (в) стр. 72 [57] циклическое подпространство $L^{\varphi}(\overrightarrow{\gamma})$ лежит в W. □

Следствие 4.1. *Задача 12, стр. 81 в [57]. Если характеристический многочлен линейного преобразования раскладывается на линейные множители, то любое собственное инвариантное подпространство данного линейного преобразования содержит собственный вектор.*

Один раунд XSL-схемы $F_{\overrightarrow{k}}\colon V_n \to V_n$ состоит из наложения ключа $\overrightarrow{k}$ (XOR-преобразование), а также нелинейного преобразования $\overline{S}$ и линейного преобразования $\overline{L}$. Нелинейное преобразование состоит из совокупности m параллельных преобразований S_i над блоками небольшой длины s ($n = ms$), $\overline{S} = (S_{m-1}, ..., S_0)$, линейное преобразование $\overline{L}$ строится на основе преобразования с высоким показателем рассеивания [18]. В шифрсистеме AES $\overline{L}$ есть композиция из сдвига строк (ShiftRows) и параллельного умножения столбцов на максимально рассеивающую матрицу-циркулянт размера 4×4 над полем $\mathbb{F}_{2^8}$, а в шифрсистеме Кузнечик $\overline{L}$ — рекурсивная матрица размера 16×16 над полем $\mathbb{F}_{2^8}$.

Следующий подход к методу инвариантных подпространств предложен в [19]. Пусть $F_{\overrightarrow{k}}(\overrightarrow{u}) = F(\overrightarrow{u} + \overrightarrow{k})$ — раундовая функция XSL-схемы, где F

есть последовательное применение $\overline{S}$ и $\overline{L}$ преобразований к блоку текста из V_n. Если для некоторого подпространства $W < V_n$ существуют такие векторы $\overrightarrow{c}, \overrightarrow{d} \in V_n$, что $F(W + \overrightarrow{c}) = W + \overrightarrow{d}$, то любой раундовый ключ $\overrightarrow{k} \in W + \overrightarrow{c} + \overrightarrow{d}$ является «слабым», поскольку $F_{\overrightarrow{k}}(W + \overrightarrow{d}) = F(W + \overrightarrow{c}) = W + \overrightarrow{d}$.

Если соотношение $F_{\overrightarrow{k}}(W + \overrightarrow{d}) = F(W + \overrightarrow{c}) = W + \overrightarrow{d}$ удаётся сохранить на протяжении всех (почти всех) раундов XSL-схемы, можно построить алгоритм различения слабых и неслабых ключей шифрсистемы, что было продемонстрировано в работе [19]. Слабостью шифра PRINT является отсутствие какого-либо усложнения в алгоритме генерирования раундовых ключей, их биты просто копируют биты исходного ключа. Поэтому, выбрав единожды ключ из нужного смежного класса, авторы [19] смогли распространить атаку на все раунды шифрсистемы.

Введём определение инвариантного подпространства для нелинейного биективного преобразования.

Определение 4.5. Векторное пространство $W < V_n$ будем называть инвариантным подпространством преобразования $F\colon V_n \to V_n$, если существуют такие векторы $\overrightarrow{c}, \overrightarrow{d} \in V_n$, что $F(W + \overrightarrow{c}) = W + \overrightarrow{d}$.

Замечание 4.1. Для линейного биективного преобразования L приведённое выше определение инвариантного подпространства совпадает с классическим (см. [57]), поскольку существование таких векторов $\overrightarrow{c}, \overrightarrow{d}$ равносильно равенству $L(W) = W$.

4.2 Подпространства, инвариантные относительно нелинейных преобразований $\overline{S}$

В общем случае инвариантные подпространства следует искать для преобразования $\overline{S}\,\overline{L}$ (метод нелинейных инвариантов, см. [47], [49]). Частным случаем являются подпространства, инвариантные одновременно для преобразований $\overline{S}$ и $\overline{L}$ (метод инвариантных подпространств, см. [45]). В данном разделе изучаются $\overline{S}$. В [59] приведено описание подгрупп, инвариантных относительно

преобразования $\overline{S}$ с произвольными фиксированными S-блоками. В [60] приведено описание смежных классов, образ которых относительно преобразования $\overline{S}$ с произвольными фиксированными S-блоками является смежным классом.

Рассмотрим преобразования $\overline{S}$, состоящие в применении одинаковых S-блоков S к векторам небольшого размера s. Такой случай наиболее распространён, и можно выделить подпространства в V_{ms}, являющиеся инвариантными относительно $\overline{S}$ независимо от преобразования S. Сначала покажем, что каждое подпространство $W < V_{ms}$ над полем P с указанным свойством является векторным пространством над полем Q (в общем случае данный факт, очевидно, не справедлив).

Лемма 4.1. *Пусть $P = \mathbb{F}_2, Q = \mathbb{F}_{2^s}$, W — подпространство в V_{ms} над полем P. Если W является инвариантным относительно любого преобразования $\overline{S}$ = (S,S,...,S), где $S \in Sym(Q)$, то W является подпространством над Q^m.*

Доказательство. В случае линейной подстановки S условие инвариантности W относительно $\overline{S}$ равносильно тому, что $\overline{S}(\overrightarrow{w}) \in W$ для любого вектора $\overrightarrow{w} \in W$. Поскольку умножение на произвольный элемент $\alpha \in Q^*$ является линейной подстановкой на множестве элементов поля Q, в силу инвариантности W для произвольного $\overrightarrow{w} \in W$, $\alpha\overrightarrow{w} \in W$, что и требовалось доказать. □

Таким образом, искать инвариантные подпространства относительно любых преобразований $\overline{S} = (S,S,...,S)$, $S \in Sym(Q)$, достаточно лишь среди подпространств над полем Q. Полное описание подпространств с указанным свойством даёт следующее утверждение. Предварительно введём определение редуцированного подпространства.

Определение 4.6. Пусть $W < Q^m$. Для подпространства W:

назовём координату i нулевой, если $w_i = 0$ для всех $\overrightarrow{w} \in W$;

назовём координаты i,j совпадающими, если $w_i = w_j$ для всех $\overrightarrow{w} \in W$.

Отношение «быть совпадающими координатами» рефлексивно, симметрично и транзитивно, множество координат разбивается на классы эквивалентности.

Редуцированным подпространством $\widetilde{W}$ назовём подпространство, полученное из W удалением из всех его векторов всех нулевых координат и всех совпадающих координат, кроме единственного представителя (с наименьшим номером координаты) в каждом классе эквивалентности.

Пример 4.1. Пусть $W = \{(0,0,0,0), (0,0,1,1), (0,1,1,1), (0,1,0,0)\} < V_4$. Координата 3 нулевая, координаты 0 и 1 совпадающие. $\widetilde{W}$ содержит координаты 0 и 2, $\widetilde{W} = \{(0,0), (0,1), (1,1), (1,0)\} < V_2$.

Редуцированное пространство $\widetilde{W}$ определяется однозначно. Длина его векторов может быть меньше m, при этом его размерность всегда совпадает с размерностью пространства W.

Утверждение 4.2. *Пусть $Q = \mathbb{F}_{2^s}, s > 2$ и W — подпространство в Q^m размерности d. Тогда W является инвариантным относительно любого преобразования $\overline{S} = (S,S,...,S)$, $S \in Sym(Q)$, тогда и только тогда, когда $\widetilde{W} = Q^d$.*

Доказательство. **Достаточность.** Покажем справедливость соотношения $\overline{S}(W + \overrightarrow{a}) = W + \overrightarrow{b}$ при $\overrightarrow{a} = (0,0,...,0)$, $\overrightarrow{b} = (S(0),S(0),...,S(0)) \in Q^m$. Не ограничивая общности, будем считать, что координаты с номерами $\{0,...,d-1\}$ в W образуют подпространство Q^d. Выберем произвольные $\overrightarrow{w} = (w_{m-1},...,w_0) \in W$ и номер координаты $j \in \{d,...,m-1\}$. Пусть $\overrightarrow{w'} = (w'_{m-1},...,w'_0) = \overline{S}(\overrightarrow{w} + \overrightarrow{a}) + \overrightarrow{b}$. По условию, либо $w_j = 0$, тогда $w'_j = S(0) + S(0) = 0$, либо $w_j = w_i$ при некотором $i \in \{0,...,d-1\}$, тогда $w'_j = S(w_i) + S(0) = w'_i$. Таким образом, $\overrightarrow{w'} = \overline{S}(\overrightarrow{w} + \overrightarrow{a}) + \overrightarrow{b} \in W$ при любом $\overrightarrow{w} \in W$, что и требовалось доказать.

Необходимость. Покажем необходимость условий теоремы на примере подстановки инверсии элементов поля $S(x) = x^{-1}$ с доопределением $0^{-1} = 0$.

Для подстановки инверсии справедливы следующие свойства [34; 64]. Пусть задано уравнение

$$S(cx) + S(x + a) = b, \tag{4.1}$$

тогда:

- если $c = 1$ и $a \neq 0$, то уравнение (4.1) имеет не более четырёх решений $x \in Q$;
- если $c \neq 0$, $c \neq 1$ и $a \neq 0$, то уравнение (4.1) имеет не более трёх решений $x \in Q$;
- если $c = 0$ или ($a = 0$ и $c \neq 1$), то уравнение (4.1), очевидно, имеет единственное решение $x \in Q$;
- если $c = 1$ и $a = 0$, то при $b = 0$ решением уравнения (4.1) является любой элемент $x \in Q$.

По утверждению 15, стр. 28 в [57] W можно задать как решение системы однородных линейных уравнений $\overrightarrow{x}C = \overrightarrow{0}$, где $C_{m\times(m-d)}$ — матрица ранга $m-d$.

Будем считать, что матрица C имеет специальный ступенчатый вид [56].

$$C^\top = S(i_{m-d-1},\ldots,i_0) = \begin{pmatrix} * & 1 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & & & & & & & & & \\ * & 0 & \ldots & * & 1 & \ldots & 0 & 0 & \ldots & 0 \\ * & 0 & \ldots & * & 0 & \ldots & * & 1 & \ldots & 0 \end{pmatrix} \tag{4.2}$$

Векторы $\overrightarrow{w}$, являющиеся решением системы уравнений $\overrightarrow{w}C = \overrightarrow{0}$ можно строить следующим образом. Координаты с номерами $\overline{0,m-1} \setminus \{i_{m-d-1},\ldots,i_0\}$ задаём произвольными значениями, оставшиеся координаты $\{i_{m-d-1},\ldots,i_0\}$ определяются однозначно.

Рассмотрим варианты строк матрицы $C^\top$.

1. Если строка матрицы $C^\top$ содержит единственный ненулевой элемент (единицу на месте ступени), то соответствующая координата равна нулю во всех векторах попространства W.
2. Если строка матрицы $C^\top$ содержит две единицы и остальные нули, это означает что соответствующие две координаты равны во всех векторах попространства W.
3. Существует строка матрицы $C^\top$, содержащая два ненулевых элемента, один из которых отличен от единицы.
4. Существует строка матрицы $C^\top$, содержащая три (либо более) ненулевых элемента.

Методом от противного покажем, что случаи 3 и 4 невозможны.

Случай 3. соответствующая строка имеет два ненулевых элемента 1 и c_1 на позициях $j_0 < j_1$. Каждый вектор $\overrightarrow{w} \in W$ удовлетворяет линейному соотношению $w_{j_0} + c_1 w_{j_1} = 0$. Поскольку номер j_1 не является номером ступени, для любого $w_{j_1} \in Q$ существует вектор $\overrightarrow{w} \in W$ с соответствующим значением w_{j_1}, то есть для каждой пары (c_1x, x), $x \in Q$, существует вектор $\overrightarrow{w} \in W$ с координатами j_0, j_1, равными значениям (c_1x, x) соответственно.

Поскольку $\overline{S}(\overrightarrow{w} + \overrightarrow{a}) + \overrightarrow{b} \in W$, существуют такие a_0,a_1,b_0,b_1, что $S(c_1x + a_0) + c_1S(x + a_1) = b_1 + b_2$ при каждом $x \in Q$. Преобразуем последнее равенство к виду

$$S(c_1^2x) + S(x + a) = b,\ a,b \in Q. \tag{4.3}$$

По условию инвариантности W относительно $\overline{S}$ равенство (4.3) справедливо при любом $x \in Q$. С другой стороны, поскольку $c^2 \neq 0$ и $c^2 \neq 1$ равенство (4.3) справедливо не более чем для трёх $x \in Q$, а при $a = 0$ соответствующее значение x единственное. Получаем противоречие инвариантности W относительно $\overline{S}$.

Случай 4. соответствующая строка имеет не менее трёх ненулевых элементов. Данная строка задаёт линейное соотношение $w_{j_0} + c_1 w_{j_1} + ... + c_t w_{j_t} = 0$, где $t > 1$, $c_i \neq 0$, $0 \leqslant j_0 < ... < j_t \leqslant m$. Каждый вектор из W удовлетворяет данному соотношению, кроме того, поскольку номером координаты ступени является лишь j_0, существуют векторы $\overrightarrow{w} \in W$, у которых координаты с номерами j_3,...,j_t нулевые, а координаты с номерами j_0,j_1,j_2 равны $c_1x + c_2y$,x,y соответственно, где x,y — произвольные элементы поля Q.

Поскольку $\overline{S}(\overrightarrow{w} + \overrightarrow{a}) + \overrightarrow{b} \in W$, существуют такие a_0,a_1,a_2,b, что $S(c_1x + c_2y + a_0) + c_1S(x + a_1) + c_2S(y + a_2) = b$ при всех x,$y \in Q$. Подставив $x = 0$, с использованием свойств уравнения (4.1) получим $c_2 = 1$ и $a_0 = a_2$. Подставив $y = 0$, получим $c_1 = 1$ и $a_0 = a_1 = a$, то есть

$$S(x + y + a) + S(x + a) + S(y + a) = b$$

Далее, подставим $x = y+1$ и получим $S(x+a)+S(x+a+1) = b'$ при любом $x \in Q$, что невозможно в силу свойств уравнения (4.1). Таким образом, для строк матрицы $C^\top$ возможны лишь случаи 1 и 2, что и требовалось доказать. □

Замечание 4.2. При доказательстве необходимости в утверждении 4.2 была использована лишь подстановкой инверсии $S(x) = x^{-1}$. Это было возможно благодоря результату леммы 4.1, позволяющему перейти к полю Q. При рассмотрении подстановки инверсии и векторного пространства V_{ms} над полем P, инвариантными подпространствами будут также подмножества $Q_{m-1} \times ... \times Q_0$, где Q_i — произвольное подполе поля Q [61]. Более подробно параллельное действие подстановки инверсии на подгруппах и смежных классах изучено в [59] и [60].

В соответствии с доказанным утверждением введём следующее определение.

Определение 4.7. Подпространство W пространства Q^m, для которого $\widetilde{W}$ является пространством Q^d при некотором d, будем называть подпространством *вида 1.*

Замечание 4.3. Для любого подпространства W, не являющегося подпространством *вида 1*, существует S-блок S, при котором W не является инвариантным подпространством преобразования $\overline{S}$.

Изучение подпространств *вида 1*, инвариантных относительно преобразования $\overline{L}$, может проводиться независимо от преобразования $\overline{S}$. В случае существования такого подпространства гарантированно получается подпространство, инвариантное относительно преобразований $\overline{S}$ и $\overline{L}$. В [45] инвариантные подпространства *вида 1* построены для линейного преобразования, заданного матрицей Адамара, что позволило предложить атаку на 6 раундов шифрсистемы Khazad.

4.3 Приведение матрицы-циркулянта к верхнетреугольному виду

Следующее утверждение сформулировано в [46].

Утверждение 4.3. *[46] Пусть* $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ_{2^s}(c_{2^r-1},...,c_0) \in Q_{2^r,2^r}$, *тогда характеристический многочлен матрицы* C *равен* $\chi_C(x) = (x+t)^{2^r}$, *где* $t = \sum_{i=0}^{2^r-1} c_i$. *Матрица* C *подобна верхнетреугольной матрице и матрица подобия* B *имеет вид:*

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes r} \in Q_{2^r,2^r}. \tag{4.4}$$

Таким образом, строки матрицы B задают систему вложенных инвариантных подпространств преобразования, заданного матрицей C. Данные подпространства имеют вид $\langle \overrightarrow{B}_0 \rangle, \langle \overrightarrow{B}_0, \overrightarrow{B}_1 \rangle, \langle \overrightarrow{B}_0, \overrightarrow{B}_1, \overrightarrow{B}_2 \rangle,..., \langle \overrightarrow{B}_0, \overrightarrow{B}_1, \overrightarrow{B}_2, \overrightarrow{B}_3,..., \overrightarrow{B}_{2^r-1} \rangle$.

Пример 4.2. Приведём матрицу B при $r = 3$:

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Для дальнейшего исследования инвариантных подпространств матриц-циркулянтов докажем более подробную версию предыдущего утверждения.

Теорема 4.1. *Пусть* $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ_{2^s}(c_{2^r-1},...,c_0) \in Q_{2^r,2^r}$ *и*

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes r} \in Q_{2^r,2^r}. \tag{4.5}$$

Тогда $B^{-1}CB = T$, *где* $T \in Q_{2^r,2^r}$ — *верхнетреугольная матрица Тёплица вида:*

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & ... & t_{2^r-1} \\ 0 & t_0 & t_1 & ... & t_{2^r-2} \\ ... & & & & \\ 0 & 0 & ... & t_0 & t_1 \\ 0 & 0 & 0 & ... & t_0 \end{pmatrix}, \qquad t_i = \sum_{j \preceq (2^r-1-i)} c_{(j+1 \mod 2^r)}. \tag{4.6}$$

Напомним, что отношение «$\preceq$» определено в разделе 4.1 и не является классическим отношением «меньше либо равно».

Умножение строки значений булевой функции f на матрицу B позволяет получить строку коэффициентов многочлена Жегалкина функции f (см. стр. 212 в [58]). Докажем вспомогательную лемму о матрице B.

Лемма 4.2. *Матрица*

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes r} \in Q_{2^r,2^r}. \tag{4.7}$$

совпадает с обратной матрицей $B = B^{-1}$ *и для произвольной матрицы* $C \in Q_{2^r,2^r}$ *справедливо:* $B^{-1}CB = A = (a_{i,j})_{2^r \times 2^r}$, $a_{i,j} = \sum_{u \succeq i, v \preceq j} c_{u,v}$.

Доказательство. Пусть $\mathbf{x} = (x_{r-1},...,x_0), \overline{\mathbf{x}} = (\overline{x}_{r-1},...,\overline{x}_0), x_i$ — булевы переменные, $i = i_{r-1}2^{r-1} + ... + i_1 r + i_0$ — двоичное представление числа $i \in \overline{0,2^r-1}$.

Обозначим за $\mathbf{x}^i$ булеву функцию, равную $x_0^{i_0} \cdot ... \cdot x_{r-1}^{i_{r-1}}$. Нетрудно видеть, что строка $\overrightarrow{B_i}$ матрицы B есть строка значений булевой функции $\mathbf{x}^i$, а столбец $B_i^{\downarrow}$ есть столбец значений булевой функции $\overline{\mathbf{x}}^{2^r-1-i}$. Иными словами, произвольный элемент матрицы $b_{i,j}$ равен значению функции $\mathbf{x}^i$ на векторе, соответствующем двоичному представлению числа j, а также равен значению функции $\overline{\mathbf{x}}^{2^r-1-j}$ на векторе, соответствующем двоичному представлению числа i.

Пусть $B_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, тогда $B = B_1^{\otimes r}$ и, с использованием свойств тензорного произведения матриц, $B^2 = (B_1^{\otimes r})^2 = (B_1^2)^{\otimes r} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{\otimes r} = E_{2^r,2^r}$, где E — единичная матрица соответствующих размеров. Таким образом, $B = B^{-1}$.

Пусть теперь $BCB = A$, $a_{i,j} = \overrightarrow{B_i} C B_j^{\downarrow}$, тогда

$$\overrightarrow{B_i} C = \sum_{u:b_{i,u}=1} \overrightarrow{C_u} = \sum_{u \succeq i} \overrightarrow{C_u} = \overrightarrow{D},$$

$$\overrightarrow{D} B_j^{\downarrow} = \sum_{v:b_{v,j}=1} d_v = \sum_{v \preceq j} d_v.$$

Таким образом,

$$a_{i,j} = \overrightarrow{B_i} C B_j^{\downarrow} = \sum_{u \succeq i, v \preceq j} c_{u,v}.$$

□

Перейдём к доказательству теоремы 4.1.

Доказательство. В соответствии с леммой 4.2 элементы матрицы $T = B^{-1}CB$ равны $t_{i,j} = \sum_{u \succeq i, v \preceq j} c_{u,v}$. Поскольку C — матрица-циркулянт, справедливо $c_{u,v} = c_{(u-v \mod 2^r),0}$. Пусть номера нулевых разрядов числа i есть a_0,...,a_s, номера единичных разрядов числа j есть b_0,...,b_k. Тогда при $u \succeq i$ $u = i + u_{a_0}2^{a_0} + ... + u_{a_s}2^{a_s}$ при некоторых $u_w \in \{0,1\}$, и при $v \preceq j$ $v = j - v_{b_0}2^{b_0} - ... - v_{b_k}2^{b_k}$ при некоторых $v_q \in \{0,1\}$. Тогда

$$t_{i,j} = \sum_{u_{a_0},...,u_{a_s},v_{b_0},...,v_{b_k} \in \{0,1\}} c_{(i-j+u_{a_0}2^{a_0}+...+u_{a_s}2^{a_s}+v_{b_0}2^{b_0}+...+v_{b_k}2^{b_k} \mod 2^r),0}. \qquad (4.8)$$

Обозначим мультимножество $M_{i,j} = \{a_0,...,a_s,b_0,...,b_k\}$, $m = \sum_{l \in M_{i,j}} 2^l$. Сумма (4.8) может быть записана в виде

$$t_{i,j} = \sum_{M \subseteq M_{i,j}} c_{(i-j+\sum_{l \in M} 2^l \mod 2^r),0}. \qquad (4.9)$$

Далее докажем лемму о «склеивании» слагаемых в сумме (4.8).

Лемма 4.3. *Пусть* $\{c_i\}_{i\geqslant 0}$ *— последовательность элементов над полем характеристики 2, тогда для произвольных* $i, r, l, w \in \mathbb{N}_0$ *с условием* $l < w, i < 2^r$ *справедливо:*

$$\sum_{v_l,u_l,\ldots,u_{w-1}\in\{0,1\}} c_{(i+v_l2^l+u_l2^l+u_{l+1}2^{l+1}+\ldots+u_{w-1}2^{w-1} \mod 2^r)} = c_i + c_{(i+2^w \mod 2^r)}. \quad (4.10)$$

Доказательство. Рассмотрим сумму (4.10) при произвольной фиксации всех коэффициентов, кроме u_l и v_l. Сумма примет вид $\sum_{u_l,v_l\in\{0,1\}} c_{(i'+v_l2^l+u_l2^l \mod 2^r)}$. При $u_l \neq v_l$ соответствующие слагаемые равны и сокращаются. Оставшиеся два слагаемых можно записать как $\sum_{u'_{l+1}\in\{0,1\}} c_{(i'+u'_{l+1}2^{l+1} \mod 2^r)}$. В полученной новой сумме могут быть «склеены» слагаемые за счёт коэффициентов u_{l+1}, u'_{l+1}. Проделав аналогичную операцию «склеивания» слагаемых до разряда с номером w, получим утверждение леммы. □

Вернёмся к доказательству теоремы. Рассмотрим следующие случаи.

1. Пусть $i < j$, тогда $m > 2^r - 1$ и существуют такие l, w, что $a_l = b_w$. Выберем соответствующий l с наибольшим номером a_l. Так как $m > 2^r - 1$, для разрядов $\{a_l + 1,\ldots,r-1\}$ мультимножество $M_{i,j}$ содержит в точности один элемент, равный номеру соответствующего разряда. Разобьём элементы $M_{i,j}$ на два мультимножества $M_1 = \{b_w, a_l, a_l + 1,\ldots,r-1\}$, $M_2 = M_{i,j} \setminus M_1$. Для каждой произвольной фиксации индексов в сумме (4.8), соответствующих элементам мультимножества M_2, применим лемму 4.3 для «склеивания» коэффициентов $v_{b_w}, u_{a_l}, u_{a_l+1}, \ldots, u_{r-1}$ и получим сумму из двух слагаемых: $c_{i',0} + c_{(i'+2^r \mod 2^r),0} = 0$. Следовательно, вся сумма (4.8) также равна 0 при любых $i < j$.
2. Пусть $i = j$, тогда множества $\{a_0,\ldots,a_s\}$ и $\{b_0,\ldots,b_k\}$ не пересекаются, а их объединение в точности есть множество $\{0,\ldots,r-1\}$. Тогда сумма (4.8) есть $\sum_{t=0}^{2^r-1} c_{t,0}$ — сумма всех элементов нулевого (вообще говоря, любого) столбца или любой строки матрицы-циркулянта C.
3. Пусть $i > j$. Покажем, что элементы $t_{i,j}$ при равных $i - j$ равны между собой. По определению в мультимножество $M_{i,j}$ входят номера нулевых разрядов числа i и единичных разрядов числа j. Значит, если разряд с каким-либо номером l совпадает в i и j ($i_l = j_l$), он войдёт в $M_{i,j}$

в точности один раз. Таким образом, можно считать что i и j не имеют совпадающих единичных разрядов, в противном случае занулим данные разряды одновременно в i и j, не изменив разность $i-j$ и мультимножество $M_{i,j}$, а значит и сумму (4.8), равную $t_{i,j}$.

Далее, возьмём максимальный номер b_w, такой что $j_{b_w}=1$. Поскольку $i>j$, найдётся такой разряд q, что $q>b_w, i_q=1$ и $q\notin M_{i,j}$ (строгость неравенства $q>b_w$ обусловлена отсутствием совпадающих единичных разрядов в i и j). Пусть q — минимальный номер разряда с указанными свойствами, следовательно $i_z=0$ для всех $z\in\overline{b_w,q-1}$. Так как $i_{b_w}=0$, существует такой номер l, что $a_l=b_w$ и $a_l, a_l+1,...,q-1\in M_{i,j}$.

Заметим, что $M_{i-2^{b_w},j-2^{b_w}}=(M_{i,j}\setminus\{b_w,a_l,a_{l+1},...,q-1\})\bigcup\{q\}$. Пусть $\widetilde{M}=M_{i,j}\bigcap M_{i-2^{b_w},j-2^{b_w}}$.

$$t_{i,j}+t_{i-2^{b_w},j-2^{b_w}}=$$
$$\sum_{M\subseteq M_{i-2^{b_w},j-2^{b_w}}} c_{(i-j+\sum_{l\in M}2^l \mod 2^r),0}+\sum_{M\subseteq M_{i,j}} c_{(i-j+\sum_{l\in M}2^l \mod 2^r),0}=$$
$$\sum_{M\subseteq\widetilde{M}} c_{(i-j+2^q+\sum_{l\in M}2^l \mod 2^r),0}+$$
$$+\sum_{M\subseteq\widetilde{M}}\sum_{M'\subseteq\{b_w,a_l,a_{l+1},...,q-1\}\setminus\{\varnothing\}} c_{(i-j+\sum_{l\in M}2^l+\sum_{l'\in M'}2^{l'} \mod 2^r),0}=$$
$$\sum_{M\subseteq\widetilde{M}}\left(c_{(i'+2^q \mod 2^r),0}+c_{(i' \mod 2^r),0}+\sum_{M'\subseteq\{b_w,a_l,a_{l+1},...,q-1\}} c_{(i'+\sum_{l'\in M'}2^{l'} \mod 2^r),0}\right),$$

где $i'=(i-j+\sum_{l\in M}2^l) \mod 2^r$.

По лемме 4.3 о «склеивании» коэффициентов $v_{b_w}, u_{a_l}, u_{a_l+1}, ..., u_{q-1}$ каждое слагаемое последней суммы внутри скобок равно нулю. Значит, вся сумма равна нулю, и $t_{i,j}=t_{i-2^{b_w},j-2^{b_w}}$.

Поскольку $j-2^{b_w}$ имеет на 1 ненулевой разряд меньше, чем j, можно выполнить аналогичный процесс для всех единичных разрядов числа j по убыванию. В результате установим, что сумма (4.8) одинакова для всех i,j с постоянным значением $i-j$ и может быть вычислена единожды, например для элемента матрицы $t_{i-j,0}$.

Вычислим соответствующую сумму при $i>0$.

$$t_{i,0}=\sum_{u\succeq i, v\preceq 0} c_{u,v}=\sum_{u\succeq i} c_{u,0}. \tag{4.11}$$

Поскольку $c_{u,0} = c_{0,2^r-u} = c_{2^r-u}$ и условие $u \succeq i$ равносильно условию $2^r - 1 - u \preceq 2^r - 1 - i$, сумма (4.11) равна $\sum_{j \preceq (2^r-1-i)} c_{(j+1 \mod 2^r)}$, где j мы получили заменой $j = 2^r - 1 - u$.

□

В теореме 4.1 показано, что произвольная матрица циркулянт $C_{2^r \times 2^r}$ подобна верхнетреугольной матрице Тёплица T, а также найдены элементы матрицы T.

4.4 Описание инвариантных подпространств одного класса матриц-циркулянтов

Теорема 4.1 позволяет полностью описать инвариантные подпространства матрицы-циркулянта при следующем условии.

Теорема 4.2. *Пусть* $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ(c_{2^r-1},...,c_0) \in Q_{2^r,2^r}$ *и выполнено условие* $c_1 + c_3 + c_5 + ... + c_{2^r-1} \neq 0$. *Тогда линейное преобразование, заданное матрицей* C, *не имеет инвариантных подпространств, кроме подпространств, указанных в утверждении 4.3.*

Для доказательства понадобится следующая лемма.

Лемма 4.4. *Пусть* Q *— поле характеристики 2,* $n \in \mathbb{N}$, *матрица* $A_{n\times n} \in Q_{n,n}$ *является верхнетреугольной,* $\chi_A(x) = (x+t)^n, t \in Q^*$ *и для любого* $i \in \overline{1,n-1}$ $a_{i,i-1} \neq 0$. *Тогда линейное преобразование, заданное матрицей* A, *имеет единственное инвариантное подпространство размерности 1.*

Доказательство. По теореме 7, стр. 57 в [57] размерность пространства собственных векторов линейного преобразования A, принадлежащих собственному значению t, равна размерности пространства решений системы линейных уравнений $\overrightarrow{x}(Et + A) = \overrightarrow{0}$, которое, в свою очередь, равно $n - rang(Et + A)$. В силу условия $\chi_A(x) = (x + t)^n$ матрица A имеет единственное собственное значение t и ранг матрицы $(Et + A)$ меньше n. С другой стороны, в силу условия $a_{i,i-1} \neq 0$, $i \in \overline{1,n-1}$, подматрица матрицы $Et + A$ после вычёркивания нулевой строки и $(n-1)$-го столбца является верхнетреугольной и невырожденной, а значит, $rang(Et + A) = n - 1$ и размерность пространства собственных

векторов, принадлежащих собственному значению t, равна 1. В силу единственности собственного значения t справедливо утверждение леммы. $\square$

Перейдём к доказательству теоремы.

Доказательство. Поскольку матрица C подобна верхнетреугольной матрице T из теоремы 4.1, матрица T является матрицей того же линейного преобразования в базисе $(\overrightarrow{B}_0, \overrightarrow{B}_1,..., \overrightarrow{B}_{2^r-1})$, матрица B определена в (4.7). Для данного линейного преобразования рассмотрим произвольное инвариантное подпространство W размерности d. Индукцией по $l < d$ покажем, что W содержит векторы $\overrightarrow{B}_0,..., \overrightarrow{B}_l$.

Пусть $l = 0$. В силу леммы 4.4 и условия (см. теорему 4.1) $c_1 + c_3 + ... + c_{2^r-1} = t_1 \neq 0$ любой собственный вектор преобразования T имеет вид $a\overrightarrow{B}_0, a \in Q$, а в соответствии со следствием 4.1 любое инвариантное подпространство преобразования T (в частности W) содержит собственный вектор. Значит, $\overrightarrow{B}_0 \in W$.

Пусть $l > 0$ и векторы $\overrightarrow{B}_0,...,\overrightarrow{B}_{l-1}$ лежат в W. Покажем, что $\overrightarrow{B}_l$ также лежит в W. Положим $B_{[0,l]} = \langle \overrightarrow{B}_0,..., \overrightarrow{B}_{l-1}\rangle$, $B_{[l,2^r]} = \langle \overrightarrow{B}_l,..., \overrightarrow{B}_{2^r-1}\rangle$. Напомним, что $B_{[0,l]}$ инвариантно относительно T.

Дополним систему векторов $(\overrightarrow{B}_0,...,\overrightarrow{B}_{l-1})$ до базиса подпространства W: $(\overrightarrow{B}_0,...,\overrightarrow{B}_{l-1},\overrightarrow{W}_l,...,\overrightarrow{W}_{d-1})$. Пусть $W' = \langle \overrightarrow{W}_l,..., \overrightarrow{W}_{d-1}\rangle$ и T' — проекция на W' ограничения преобразования T на W', то есть $T'\colon W' \to W'$ и $T'(\alpha) = PR_{W'}(T(\alpha))$ для любого $\overrightarrow{\alpha} \in W'$.

$\chi_{T'}(x)$ делит $\chi_T(x)$, значит $\chi_{T'}(x) = (x+t)^w$ при некотором w и, в соответствии со следствием 4.1, линейное преобразование T' имеет собственный вектор $\overrightarrow{W}_0 \in W'$, $T'(\overrightarrow{W}_0) = t\overrightarrow{W}_0$. Тогда

$$T(\overrightarrow{W}_0) = t\overrightarrow{W}_0 + \overrightarrow{\alpha}_0,\ \overrightarrow{\alpha}_0 \in B_{[0,l]}. \tag{4.12}$$

Разложим вектор $\overrightarrow{W}_0$ в базисе $(\overrightarrow{B}_0,...,\overrightarrow{B}_{2^r-1})$: $\overrightarrow{W}_0 = \overrightarrow{W}'_0 + \overrightarrow{W}''_0$, где $\overrightarrow{W}'_0 \in B_{[0,l]}, \overrightarrow{W}''_0 \in B_{[l,2^r]}$. Пусть T'' есть проекция на $B_{[l,2^r]}$ ограничения T на $B_{[l,2^r]}$. Тогда:

$$T''(\overrightarrow{W}''_0) = PR_{B_{[l,2^r]}}(T(\overrightarrow{W}''_0)), \tag{4.13}$$

$$T(\overrightarrow{W}''_0) = T(\overrightarrow{W}_0) + T(\overrightarrow{W}'_0) = t\overrightarrow{W}_0 + \overrightarrow{\alpha}_0 + \overrightarrow{\alpha}_1, \overrightarrow{\alpha}_i \in B_{[0,l]}, i \in \{0,1\}, \tag{4.14}$$

$$t\overrightarrow{W}_0 = t\overrightarrow{W}'_0 + t\overrightarrow{W}''_0 = t\overrightarrow{W}''_0 + \overrightarrow{\alpha}_2, \overrightarrow{\alpha}_2 \in B_{[0,l]}. \quad (4.15)$$

Подставив (4.14) и (4.15) в (4.13) и воспользовавшись тем, что $PR_{B_{[l,2^r]}}(\overrightarrow{\alpha}_i) = 0$ для каждого $\overrightarrow{\alpha}_i \in B_{[0,l]}$, получим $T''(\overrightarrow{W}''_0) = t\overrightarrow{W}''_0$. С другой стороны, матрица линейного преобразования T'' в базисе $B_{[l,2^r]}$ получается из матрицы T вычёркиванием строк и столбцов с номерами $\{0,...,l-1\}$ и имеет верхнетреугольный вид. Вектор $\overrightarrow{B}_l$ является собственным вектором преобразования T'' и, в соответствии с леммой 4.4, $\overrightarrow{W}''_0 = \overrightarrow{B}_l a, a \in Q^*$, и $\overrightarrow{W}_0 = \overrightarrow{W}'_0 + \overrightarrow{B}_l a$, а значит, $\overrightarrow{B}_l \in \langle \overrightarrow{B}_0,..., \overrightarrow{B}_{l-1}, \overrightarrow{W}_0 \rangle$, что и требовалось доказать в индукционном переходе. □

Следствие 4.2. *Пусть $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ(c_{2^r-1},...,c_0) \in Q_{2^r,2^r}$ и C является максимально рассеивающей матрицей. Тогда линейное преобразование, заданное матрицей C, не имеет инвариантных подпространств, кроме подпространств, указанных в утверждении 4.3.*

Доказательство. Известно (см., например, [18]), что все квадратные подматрицы максимально рассеивающей матрицы невырождены. Рассмотрим подматрицу M матрицы C с номерами строк 0,2,4,...,2^r-2 и с номерами столбцов 1,3,5,...,2^r-1 размера $2^{r-1} \times 2^{r-1}$. Нетрудно видеть, что каждая строка подматрицы M состоит в точности из элементов $c_1, c_3, c_5, ..., c_{2^r-1}$. Если $c_1 + c_3 + ... + c_{2^r-1} = 0$, то сумма столбцов матрицы M равна нулевому столбцу и M — вырожденная подматрица, что невозможно в случае максимально рассеивающей матрицы C. Таким образом, $c_1 + c_3 + ... + c_{2^r-1} \neq 0$, что и требовалось доказать.

□

Пример 4.3. В шифрсистеме AES и хэш-функции Whirlpool используются максимально рассеивающие матрицы-циркулянты. Инвариантные подпространства данных матриц есть подпространства, указанные в утверждении 4.3, и только они.

Следствие 4.3. *В условиях теоремы 4.2 вторая нормальная форма матрицы C состоит из единственной клетки и имеет вид:*

$$N_2(C) = S((x+t)^{2^r}) = \begin{pmatrix} 0 & 0 & ... & 0 & t^{2^r} \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}_{2^r \times 2^r}, \qquad t = \sum_{j=0}^{2^r-1} c_j.$$

Доказательство. Предположим, что матрица C подобна распавшейся матрице. Тогда характеристический многочлен каждой клетки раскладывается на линейные множители (для каждой клетки он равен $(x+t)^w$ при некотором $w \in \mathbb{N}$), а значит, в соответствии со следствием 4.1, подпространства, образованные базисными векторами каждой клетки, содержат собственный вектор преобразования C. В соответствии с доказанной теоремой любой собственный вектор преобразования C лежит в подпространстве $\langle \overrightarrow{B}_0 \rangle$, получаем противоречие. Таким образом, матрица C неразложима из чего следует вид второй нормальной формы. □

4.5 Инвариантные подпространства рекурсивных матриц

Пусть $Q = \mathbb{F}_{2^s}$, $f(x) = f_{m-1}x^{m-1} + f_{m-2}x^{m-2} + ... + f_1x + f_0 \in Q[x]$. Всюду далее полагаем $f_0 \neq 0$. $L_Q(f)$ — множество линейных рекуррентных последовательностей над полем Q с характеристическим многочленом $f(x)$. Для любого $i \geqslant 0$ и любой последовательности $u \in L_Q(f)$ справедливо равенство

$$(u_{i+m},u_{i+m-1},...,u_{i+1}) = (u_{i+m-1},u_{i+m-2},...,u_i)S(f) = ... = (u_{m-1},u_{m-2},...,u_0)S(f)^{i+1},$$

где $S(f)$ — сопровождающая матрица многочлена $f(x)$.

Положим $f(x)^{[t]} = f_{m-1}^t x^{m-1} + f_{m-2}^t x^{m-2} + ... + f_1^t x + f_0^t$. При $t = 2^r$ $f(x^t)^{[t]} = (f(x))^t$. Элемент α является корнем $f(x)$ тогда и только тогда, когда α^t является корнем $f(x)^{[t]}$. Пусть $O(f)$ — НОК мультипликативных порядков всех ненулевых корней $f(x)$ в поле его разложения (см. [57]). При $t = 2^r$ f и $f^{[t]}$ приводимы или неприводимы над Q одновременно и $O(f) = O(f^{[t]})$.

При $k \geqslant m$ векторное пространство над Q, состоящее из начальных отрезков длины k всех последовательностей $u \in L_Q(f)$, называется *линейным*

рекурсивным кодом [62] и обозначается $L_Q^{\overline{0,k-1}}(f)$. Один из способов построения линейных рекурсивных МДР-кодов [62; 63] заключается в выборе многочлена $f(x)$, корнями которого в его поле разложения являются элементы некоторой БЧХ-цепочки. В таком случае все корни многочлена $f(x)$ различны, и справедлива следующая теорема 4.3.

Замечание 4.4. Для того чтобы показать, что собственное подпространство $W < Q^m$ не является подпространством *вида 1* достаточно показать выполнимость следующих двух условий.

1. Для любого $i \in \overline{0,m-1}$ существует такой вектор $\overrightarrow{u} = (u_{m-1},...,u_0) \in W$, что $u_i \neq 0$.
2. Для любых $i < j$ существует такой вектор $\overrightarrow{u} = (u_{m-1},...,u_0) \in W$, что $u_i \neq u_j$.

Теорема 4.3. *Пусть $Q = \mathbb{F}_{2^s}$ и $m = 2^r$ при некотором $r \in \mathbb{N}$, $f(x) \in Q[x], \deg f(x) = m$, $f_0 \neq 0$ и $f(x)$ не имеет кратных корней в поле разложения. Тогда, если порядок любого корня многочлена $f(x)$ в его поле разложения больше $m-1$, то рекурсивная матрица $S(f)^m$ не имеет собственных инвариантных подпространств вида 1.*

Доказательство. Пусть $f(x)$ имеет каноническое разложение $f(x) = g_1(x)... \ g_t(x)$. Пространство ЛРП $L_Q(f)$ раскладывается в прямую сумму подпространств $L_Q(f) = L_Q(g_1) \dotplus ... \dotplus L_Q(g_t)$. Поскольку вектор длины m однозначно задаёт ЛРП из $L_Q(f)$, справедливо также разложение пространства $L_Q^{[0,m-1]}(f)$ в прямую сумму подпространств

$$L_Q^{[0,m-1]}(f) = L_Q^{[0,m-1]}(g_1) \dotplus ... \dotplus L_Q^{[0,m-1]}(g_t) \tag{4.16}$$

Вторая нормальная форма матрицы $S(f)$ имеет вид $N_2(S(f)) = Diag(S(g_1(x)),...,S(g_t(x)))$. Следовательно, матрица $S(f)^m$ подобна матрице $(N_2(S(f)))^m = Diag(S(g_1(x))^m,...,S(g_t(x))^m)$. Характеристический многочлен матрицы $(N_2(S(f)))^m$ равен произведению характеристических многочленов матриц $S(g_i(x))^m, i \in \overline{1,t}$. Заметим, что для каждого $i \in \overline{1,t}$ $g_i^{[m]}(S(g_i(x))^m) = (g_i(S(g_i(x)))^m = 0_{m\times m}$. Так как $g_i(x)$ неприводим над Q, $g_i^{[m]}(x)$ также неприводим над Q и является характеристическим многочленом преобразования $S(g_i(x))^m$. Обозначив за φ линейное преобразование, заданное матрицей $S(f(x))$, имеем $\chi_{\varphi^m}(x) = (g_1^{[m]}(x))... \ (g_t^{[m]}(x))$.

Дальнейшее доказательство проведём в два этапа. Сначала покажем, что произвольное инвариантное подпространство W преобразования φ^m содержит подпространство $L_Q^{[0,m-1]}(g_i)$ при некотором i. Затем, с использованием замечания 4.4, покажем, что подпространство $L_Q^{[0,m-1]}(g_i)$ не является подпространством *вида 1.*

Рассмотрим произвольное инвариантное подпространство W преобразования φ^m. По утверждению 4.1 существуют такие $i \in \overline{1,r}, \overrightarrow{\gamma} \in W$, что $m_{\overrightarrow{\gamma},\varphi^m}(x) = g_i^{[m]}(x)$ и $L^{\varphi^m}(\overrightarrow{\gamma}) < W$. Не ограничивая общности, положим $i = 1$. Обозначим $g_1(x) = g(x)$, тогда $g_1^{[m]}(x) = g^{[m]}(x)$. Пусть $\overrightarrow{\gamma} = \overrightarrow{\gamma_1} + ... + \overrightarrow{\gamma_t}$ — разложение вектора $\overrightarrow{\gamma}$ на компоненты из суммы (4.16). Справедливы равенства $\overrightarrow{0} = g^{[m]}(\varphi^m)(\overrightarrow{\gamma}) = (g(\varphi)^m)(\overrightarrow{\gamma_1}) + ... + (g(\varphi)^m)(\overrightarrow{\gamma_t})$. Поскольку сумма (4.16) является прямой, каждое слагаемое в последнем равенстве равно нулевому вектору.

Для любого $\overrightarrow{\gamma_1}$ $(g(\varphi)^m)(\overrightarrow{\gamma_1}) = \overrightarrow{0}$. При этом, поскольку $g(x)$ взаимно прост с любым $g_i(x)$ при $i > 1$, $g(\varphi)^m(\overrightarrow{\gamma_i}) = \overrightarrow{0}$ только при $\overrightarrow{\gamma_i} = \overrightarrow{0}$, то есть $\overrightarrow{\gamma} = \overrightarrow{\gamma_1} \in L_Q^{[0,m-1]}(g_1)$ и $L^{\varphi^m}(\overrightarrow{\gamma}) < L_Q^{[0,m-1]}(g_1)$. С другой стороны, размерности подпространств $L^{\varphi^m}(\overrightarrow{\gamma})$ и $L_Q^{[0,m-1]}(g_1)$ совпадают и равны $k = \deg g_1(x)$, а значит указанные подпространства также совпадают. Следовательно, $L_Q^{[0,m-1]}(g_1) < W$.

Используя условие теоремы о порядке корней $g_1(x)$, покажем, что в этом случае W не является подпространством *вида 1.* Поскольку произвольный набор из k подряд идущих элементов $(u_{i+k-1},...,u_{i+1},u_i)$, $i \geqslant 0$, задаёт ЛРП $u \in L_Q(g_1)$, в $L_Q^{[0,m-1]}(g_1)$ есть векторы с ненулевым элементом на произвольной позиции $i \in \overline{0,m-1}$. Методом от противного покажем, что для произвольных позиций $i > j$ существует вектор u, у которого $u_i \neq u_j$. Для произвольного u

$$(u_{i+k-1},u_{i+k-2},...,u_i) = (u_{j+k-1},u_{j+k-2},...,u_j)S(g_1)^{i-j}.$$

Обозначим $S(g_1)^{i-j} = S_{k\times k} = (s_{ij})_{k\times k}$. Тогда

$$u_i = u_{j+k-1}s_{k-1,0} + ... + u_j s_{0,0}. \tag{4.17}$$

Выбирая $u_{j+k-1} = u_{j+k-2} = ... = u_1 = 0$, получим равенство $u_i = u_j s_{0,0}$, то есть $s_{0,0} = 1$. Сокращая в (4.17) u_i и $u_j s_{0,0}$, получим равенство $0 = u_{j+k-1}s_{k-1,0} + ... + u_{j+1}s_{1,0}$. В силу произвольности u, $s_{k-1,0} = ... = s_{1,0} = 0$. Далее заметим, что для произвольного $l > 0$ также справедлив закон ЛРП $(u_{i+k-1+l},u_{i+k-2+l},...,u_{i+l}) = (u_{j+k-1+l},u_{j+k-2+l},...,u_{j+l})S(g_1)^{i-j}$. То есть период произвольной ЛРП u меньше либо равен, чем $i - j \leqslant m - 1$. По утверждениям 13, 14 стр. 327 [57] $T(u) =$

$T(m_{u,S(g_1)}(x)) = T(g_1(x)) = O(g_1)$, что противоречит условию теоремы $O(g_1) > m-1$. Таким образом, для произвольных позиций $i > j$ существует вектор $\overrightarrow{u} \in L_Q^{[0,m-1]}(g_1) < W$, у которого $u_i \neq u_j$. В соответствии с замечанием 4.4 W не является инвариантным подпространством *вида 1*. В силу произвольности в выборе W теорема доказана. □

Следствие 4.4. *Матрица линейного преобразования шифрсистемы Кузнечик не имеет собственных инвариантных подпространств вида 1 при* $s = 8$.

Доказательство. Характеристический многочлен $f(x)$ матрицы $S(f)$ раскладывается на линейные множители над полем $Q = \mathbb{F}_{2^8}$ и не имеет кратных корней. Корнями многочлена являются элементы θ^{120},θ^{121},...,θ^{135}, где θ — примитивный элемент поля $\mathbb{F}_{2^8}$. Непосредственной проверкой можно убедиться, что порядок каждого корня больше $m-1 = 15$ и справедливы условия теоремы 4.3. □

4.6 Инвариантные подпространства матриц, подобных рекурсивным

В предыдущем разделе показано, что в условиях теоремы 4.3 рекурсивная матрица не имеет собственных инвариантных подпространств *вида 1*. В разделе 3.4.4 было предложено использовать в качестве матриц линейных преобразований матрицы $(S(f)^\top)^m$, подобные рекурсивным. Такие матрицы являются максимально рассеивающими одновременно с матрицами $S(f)^m$ и потенциально имеют эффективную реализацию. Инвариантные подпространства подобных матриц имеют взаимно однозначное соответствие через умножение на матрицу подобия C, однако, свойство «быть подпространством *вида 1*» не сохраняется при таком домножении. Поэтому исследование инвариантных подпространств преобразований $(S(f)^\top)^m$ является отдельной задачей, которую, однако, в условиях теоремы 4.3 можно решить непосредственной проверкой.

Инвариантные подпространства рекурсивной матрицы в условиях теоремы 4.3 можно найти с использованием разложения (4.16). Каждое из слагаемых в отдельности не имеет собственных инвариантных подпространств в силу неприводимости многочленов $g_i^{[m]}(x)$. Любая комбинация слагаемых является

инвариантным подпространством, других инвариантным подпространств у преобразования S^m нет.

Пусть W — инвариантное подпространство S^m, тогда $WS^m = W$, где умножение подпространства на матрицу означает умножение каждого вектора на матрицу. Поскольку $S^m = C^{-1}(S^\top)^m C$, $W = WS^m = WC^{-1}(S^\top)^m C$ или $WC^{-1} = WC^{-1}(S^\top)^m$, то есть W — инвариантное подпространство S^m, тогда и только тогда, когда WC^{-1} — инвариантное подпространство $(S^\top)^m$. Для того, чтобы проверить наличие инвариантных подпространств *вида 1* преобразования $(S(f)^\top)^m$ при условии, что $f(x)$ не имеет кратных корней, достаточно.

1. Перебрать все подмножества слагаемых в разложении (4.16), всего $2^t - 2$ собственных подпространств $t \leqslant m$.
2. Для каждого подмножества вычислить соответствующее инвариантное подпространство W и пространство WC^{-1}, где C^{-1} — матрица из (3.7).
3. Проверить, является ли пространство WC^{-1} подпространством *вида 1*.

Выводы по главе. Результаты главы 4 показывают неприменимость метода инвариантных подпространств с подпространствами *вида 1* к XSL-схемам с одинаковыми S-блоками и циркулянтными, либо рекурсивными линейными преобразованиями. Для циркулянтных матриц дополнительно необходимо проверить, чтобы раундовые ключи (константы в случае хэш-функции) не лежали в цепочке подпространств из работы [46]. Для шифрсистемы AES и хэш-функции Whirlpool условие на непринадлежность ключей подпространствам из цепочки выполняется. Для шифрсистемы Кузнечик, использующей рекурсивную матрицу на основе БЧХ-кода, неприменимость метода с использованием подпространств *вида 1* также обоснована.

Заключение

В рамках достижения поставленной цели в диссертации получены следующие результаты, соответствующие задачам 1-4 во введении.

1. Предложена *Конструкция 1*, позволяющая строить дифференциально 4-равномерные подстановки размерности s из некоторых дифференциально 2-равномерных преобразований размерности $s+1$. Доказана теорема о дифференциальной 4-равномерности построенных подстановок. Приведены достаточные условия применимости *Конструкции 1* и полностью описаны степенные подстановки, к которым данная конструкция применима. Показан случай, в котором построенные подстановки обладают максимально известной нелинейнойстью. Для практически важной размерности $s = 8$ построенная подстановка приведена в Приложении А. Указанная подстановка обладает оптимальными из известных показателей дифференциальной равномерности (4) и нелинейности (112), а также степенью нелинейности и алгебраической степенью (5) и графовой алгебраической иммунностью (2).
2. Предложены подходы к эффективной программной реализации линейных преобразований, заданных умножением на элемент кольца. Указанный класс преобразований обобщает класс двоичных матриц-циркулянтов, а значит, указанная реализация применима к матрице линейного преобразования китайского стандарта шифрования SM4 [4]. Предложено разложение произвольной матрицы в сумму произведений диагональных матриц и матриц, реализуемых через умножение на элемент кольца. Получена нижняя оценка на число слагаемых в указанном разложении. Для матриц-циркулянтов над полем $\mathbb{F}_{2^s}$ также получена верхняя оценка на число слагаемых в разложении. В частности, результат получен для матриц, используемых в линейных преобразованиях шифрсистемы AES [3] и хэш-функции Whirlpool [11].
3. Найдены все решения уравнения подобия для сопровождающей матрицы многочлена над конечным полем и её транспонированной матрицы. На основе решений получены разложения для произвольной рекурсивной матрицы и предложены новые программные реализации шифр-

системы Кузнечик [2], использующие сравнительно небольшой объём памяти.

4. Показано, что любая матрица-циркулянт подобна верхнетреугольной матрице Тёплица. Полностью описаны инвариантные подпространства максимально рассеивающих матриц-циркулянтов, в частности матриц, используемых в линейных преобразованиях шифрсистемы AES и хэш-функции Whirlpool. Показано отсутствие инвариантных подпространств согласованного с размером S-блока *вида 1* для рекурсивных матриц, характеристический многочлен которых не имеет кратных корней в поле разложения. Результат справедлив для матрицы линейного преобразования шифрсистемы Кузнечик. Указанные результаты показывают неприменимость метода анализа на основе инвариантных подпространств с использованием подпространств *вида 1* к шифрсистемам AES и Кузнечик и хэш-функции Whirlpool.

Результаты диссертации могут применяться:

1. в синтезе линейных и нелинейных преобразований для использования в XSL-схемах;
2. в разработке низкоресурсных программных реализаций шифрсистем Кузнечик и SM4, хэш-функций PHOTON [10] и Whirlpool;
3. в обосновании стойкости к методу инвариантных подпространств шифрсистем Кузнечик, AES и хэш-функции Whirlpool.

Список литературы

1. Data Encryption Standard (DES) // Federal Information Processing Standards. — October 25, 1999. — Publication 46—3. — URL: https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf.
2. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры // Москва: Стандартинформ. — 2018.
3. Advanced Encryption Standard (AES) // Federal Information Processing Standards. — November 26, 2001. — Publication 197. — URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.
4. *Diffie, W., Ledin, G.* SMS4 Encryption Algorithm for Wireless Networks // IACR Cryptol. ePrint Arch. — 2008. — URL: https://api.semanticscholar.org/CorpusID:28508321.
5. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // Москва: Стандартинформ. — 2018.
6. *Dworkin, M.* NIST SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. — 2007.
7. Р 1323565.1.026-2019. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование // Москва: Стандартинформ. — 2019.
8. 3GPP TS 35.205. 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General. V 18.0.0. — 2024.
9. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования // Москва: Стандартинформ. — 2018.
10. *Guo, J., Peyrin, T., Poschmann, A. Y.* The PHOTON Family of Lightweight Hash Functions // IACR Cryptology ePrint Archive. — 2011. — URL: https://api.semanticscholar.org/CorpusID:1102361.

11. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash functions // ISO/IEC. — 2004. — № 10118—3. — URL: https://www.iso.org/standard/39876.html.

12. Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования // Москва: Стандартинформ. — 2016.

13. The SPHINCS+ Signature Framework / D. J. Bernstein [и др.] // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. — 2019. — URL: https://api.semanticscholar.org/CorpusID:204772152.

14. Р 1323565.1.003-2024. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи // Москва: Стандартинформ. — 2024.

15. *Carlet, C.* Vectorial Boolean Functions for Cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / под ред. Y. Crama, P. L. Hammer. — Cambridge University Press, 2010. — С. 398—470.

16. *Biham, E., Shamir, A.* Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. — 1990. — Vol. 4. — P. 3—72.

17. *Matsui, M.* Linear Cryptanalysis Method for DES Cipher // International Conference on the Theory and Application of Cryptographic Techniques. — 1994.

18. Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results / K. C. Gupta [и др.] // Adv. Math. Commun. — 2019. — Т. 13. — С. 779—843.

19. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack / G. Leander [и др.] // Annual International Cryptology Conference. — 2011. — URL: https://api.semanticscholar.org/CorpusID:1332575.

20. *Shannon, C. E.* Communication theory of secrecy systems // Bell Syst. Tech. J. — 1949. — Vol. 28. — P. 656—715.

21. *Liskov, M. D., Rivest, R. L., Wagner, D. A.* Tweakable Block Ciphers // Journal of Cryptology. — 2002. — Т. 24. — С. 588—613. — URL: https://api.semanticscholar.org/CorpusID:1559583.

22. *Malyshev F. M.* The duality of differential and linear methods in cryptography // Mathematical Aspects of Cryptography. — 2014. — Т. 5, вып. 3. — С. 35—47.

23. *Barreto, P., Rijmen, V.* The KHAZAD Legacy-Level Block Cipher // Computer Science. — 2001. — URL: https://api.semanticscholar.org/CorpusID:53742378.

24. PRESENT: An Ultra-Lightweight Block Cipher / A. Bogdanov [и др.] // Workshop on Cryptographic Hardware and Embedded Systems. — 2007. — URL: https://api.semanticscholar.org/CorpusID:5926793.

25. Midori: A Block Cipher for Low Energy / S. Banik [и др.] // International Conference on the Theory and Application of Cryptology and Information Security. — 2015. — URL: https://api.semanticscholar.org/CorpusID:6849787.

26. The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS / C. Beierle [и др.] // IACR Cryptol. ePrint Arch. — 2016. — URL: https://api.semanticscholar.org/CorpusID:1279633.

27. The QARMAv2 Family of Tweakable Block Ciphers / R. Avanzi [и др.] // IACR Transactions on Symmetric Cryptology. — 2023. — С. 25—73.

28. *Knudsen, L. R.* Truncated and Higher Order Differentials // Fast Software Encryption Workshop. — 1994. — URL: https://api.semanticscholar.org/CorpusID:18843747.

29. *Courtois, N. T., Pieprzyk, J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // IACR Cryptol. ePrint Arch. — 2002. — URL: https://api.semanticscholar.org/CorpusID:2760507.

30. An APN permutation in dimension six / K. A. Browning [и др.] // Finite Fields: theory and applications. — 2010. — Т. 518. — С. 33—42.

31. *А. В. Казимиров, В. Н. Казимирова, Р. В. Олейников.* Метод генерации сильно нелинейных S-блоков на основе градиентного спуска // Матем. вопр. криптогр. — 2014. — Т. 5, № 2. — С. 71—78.

32. *Edel, Y., Pott, A.* A new almost perfect nonlinear function which is not quadratic // IACR Cryptol. ePrint Arch. — 2008. — URL: https://api.semanticscholar.org/CorpusID:1000796.

33. Constructing Differentially 4-Uniform Permutations Over $\mathbb{F}_2^{2k}$ via the Switching Method / L. Qu [и др.] // IEEE Transactions on Information Theory. — 2013. — Т. 59. — С. 4675—4686. — URL: https://api.semanticscholar.org/CorpusID:8895395.

34. *Claude, C.* On Known and New Differentially Uniform Functions // Information Security and Privacy / под ред. U. Parampalli, P. Hawkes. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. — С. 1—15.

35. More constructions of differentially 4-uniform permutations on $\mathbb{F}_2^{2k}$ / L. Qu [и др.] // Designs, Codes and Cryptography. — 2013. — Т. 78. — С. 391—408. — URL: https://api.semanticscholar.org/CorpusID:195346106.

36. *Tang, D., Carlet, C., Tang, X.* Differentially 4-uniform bijections by permuting the inverse function // Designs, Codes and Cryptography. — 2014. — Т. 77.

37. *Li, Y., Wang, M.* Constructing differentially 4-uniform permutations over $\mathbb{F}_2^{2m}$ from quadratic APN permutations over $\mathbb{F}_2^{2m+1}$ // Designs, Codes and Cryptography. — 2014. — Т. 72. — С. 249—264. — URL: https://api.semanticscholar.org/CorpusID:8239899.

38. *Менячихин, А. В.* Адаптированный спектрально-разностный метод построения дифференциально 4-равномерных кусочно-линейных подстановок, ортоморфизмов, инволюций поля $\mathbb{F}_2^n$ // Дискретная математика. — 2023. — Т. 35, № 2. — С. 42—77.

39. *Буров, Д. А., Костарев, С. В.* Некоторые криптографические свойства кусочно-мономиальных преобразований поля $\mathbb{F}_{2^n}$ // XIII Симпозиум современные тенденции в криптографии (CTCrypt 2024). — 2024.

40. *Буров, Д. А., Костарев, С. В., Менячихин, А. В.* Класс кусочно-мономиальных подстановок: дифференциально 4-равномерные подстановки поля $\mathbb{F}_{2^8}$ с графовой алгебраической иммунностью 3 существуют // XII Симпозиум современные тенденции в криптографии (CTCrypt 2023). — 2023.

41. *Leander, G., Minaud, B., Rønjom, S.* A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro // IACR Cryptol. ePrint Arch. — 2015. — URL: https://api.semanticscholar.org/CorpusID:16751896.

42. LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations / V. Grosso [и др.] // Fast Software Encryption Workshop. — 2014. — URL: https://api.semanticscholar.org/CorpusID:1647275.

43. Block Ciphers That Are Easier to Mask: How Far Can We Go? / B. Gérard [и др.] // Cryptographic Hardware and Embedded Systems - CHES 2013 / под ред. G. Bertoni, J.-S. Coron. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. — С. 383—399.

44. Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs / J. Guo [и др.] // IACR Transactions on Symmetric Cryptology. — 2016. — С. 33—56.

45. *Burov, D. A., Pogorelov, B. A.* An attack on 6 rounds of Khazad // Математические вопросы криптографии. — 2016. — Т. 7, № 2. — С. 35—46.

46. *Волгин, А. В., Крючков, Г. В.* Характеризация линейных преобразований, задающихся матрицами Адамара над конечным полем и циркулянтными матрицами // Прикладная дискретная математика. Приложение. — 2017. — № 10. — С. 10—11.

47. *Todo, Y., Leander, G., Sasaki, Y.* Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64 // Journal of Cryptology. — 2016. — Т. 32. — С. 1383—1422. — URL: https://api.semanticscholar.org/CorpusID:2843496.

48. *Halevi, S., Coppersmith, D., Jutla, C. S.* Scream: A Software-Efficient Stream Cipher // IACR Cryptol. ePrint Arch. — 2002. — URL: https://api.semanticscholar.org/CorpusID:1499691.

49. *Буров, Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. — 2021. — Т. 33, № 2. — С. 31—45.

50. *Фомин, Д. Б.* On the Impossibility of an Invariant Attack on Kuznyechik // 10th Workshop on Current Trends in Cryptology (CTCrypt 2021). Preproceedings. — 2021. — С. 151—161.

51. *Kyureghyan, G. M.* Crooked maps in $\mathbb{F}_2^n$ // Finite Fields and Their Applications. — 2007. — Т. 13, № 3. — С. 713—726. — URL: https://www.sciencedirect.com/science/article/pii/S1071579706000207.

52. *Дорохин, С. В., Качков, С. С., Сидоренко, А. А.* Реализация блочного шифра "Кузнечик" с использованием векторных инструкций // Труды Московского физико-технического института. — 2018. — Т. 10, 4 (40).

53. *Tolba, M. F., Youssef, A.* Improved Meet-in-the-Middle Attacks on Reduced Round Kuznyechik // ICISC. — 2017.

54. *Diffie, W., Ledin, G.* SMS4 Encryption Algorithm for Wireless Networks // IACR Cryptol. ePrint Arch. — 2008. — URL: https://eprint.iacr.org/2008/329.pdf.

55. *Fog, A.* Instruction tables: Lists of instruction latencies, throughputs and micro-operation breakdowns for Intel, AMD and VIA CPUs. — 1996–2022. — URL: https://agner.org/optimize/instruction_tables.pdf ; https://agner.org/optimize/instruction_tables.pdf.

56. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Том I. — Москва : Гелиос АРВ, 2003.

57. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Том II. — Москва : Гелиос АРВ, 2003.

58. *Глухов М. М., Шишков А. Б.* Математическая логика. Дискретные функции. Теория алгоритмов. — Санкт-Петербург, Москва, Краснодар : Лань, 2012.

59. *Буров Д. А.* Подгруппы прямого произведения групп, инвариантные относительно действия подстановок на сомножителях // Дискрет. матем. — 2019. — Апр. — № 31. — С. 3—19.

60. *Буров Д. А.* О переходах смежных классов прямого произведения групп под действием биективных отображений групп на сомножителях // Дискрет. матем. — 2023. — Апр. — № 35. — С. 18—45.

61. *Kolomeec, N., Bykov, D.* On the image of an affine subspace under the inverse function within a finite field // Designs, Codes and Cryptography. — 2024. — Февр. — Т. 92. — С. 467—476.

62. Параметры рекурсивных МДР-кодов / Гонсалес С. [и др.] // Дискрет. матем. — 2000. — Апр. — № 12. — С. 3—24.

63. *Мак-Вильямс Ф. Дж., С. Н. Д. А.* Теория кодов, исправляющих ошибки. — Москва : Связь, Перевод с английского И. И. Грушко и В. А. Зиновьева, 1979.

64. C-Differentials, Multiplicative Uniformity, and (Almost) Perfect c-Nonlinearity / P. Ellingsen [и др.] // IEEE Transactions on Information Theory. — 2019. — Т. 66. — С. 5781—5789. — URL: https://api.semanticscholar.org/CorpusID:202538792.

65. Булевы функции в теории кодирования и криптологии / Логачев О. А. [и др.]. — Москва : ЛЕНАНД, 2015.

66. *Courtois, N. T., Bard, G. V.* Algebraic Cryptanalysis of the Data Encryption Standard // IACR Cryptol. ePrint Arch. — 2007. — Т. 2006. — С. 402. — URL: https://api.semanticscholar.org/CorpusID:8206418.

67. *Perrin, L.* Partitions in the S-Box of Streebog and Kuznyechik // IACR Trans. Symmetric Cryptol. — 2019. — Т. 2019. — С. 302—329. — URL: https://api.semanticscholar.org/CorpusID:60442929.

68. *Budaghyan, L., Carlet, C., Pott, A.* New classes of almost bent and almost perfect nonlinear polynomials // IEEE Transactions on Information Theory. — 2005. — Т. 52. — С. 1141—1152. — URL: https://api.semanticscholar.org/CorpusID:6488601.

Публикации автора по теме диссертации

69. *С. А. Давыдов, И. А. Круглов.* Метод синтеза дифференциально 4-равномерных подстановок пространства V_m для четных m // Дискрет. матем. — 2019. — Т. 31, № 2. — С. 69—76. — (0.5 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.220) // Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%.

70. *С. А. Давыдов*, *Ю. Д. Шкуратов*. Использование матриц-циркулянтов над $\mathbb{F}_2$ при построении эффективных линейных преобразований с высокими показателями рассеивания // Матем. вопр. криптогр. — 2024. — Т. 15, № 2. — С. 29—46. — (1.125 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.143) // Соавтору принадлежат лемма 1 и теорема 2. Остальные результаты получены Давыдовым С.А. – 86%.

71. *С. А. Давыдов*. Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц // Дискрет. матем. — 2024. — Т. 36, № 4. — С. 44—63. — (1.25 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.220) – 100%.

72. *С. А. Давыдов*, *В. А. Шишкин*. Способы разложения рекурсивных матриц и их применение к реализации линейных преобразований // International Journal of Open Information Technologies. — 2023. — Т. 11, № 7. — С. 30—38. — (0.5625 п.л., ВАК, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.492) // Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%.

Приложение А. Построенные дифференциально 4-равномерные подстановки

В данном приложении приведены построенные в главе 1 подстановки в поле V_8. Подстановки заданы нижней строкой.

$S = \{0, 4, 32, 60, 37, 114, 207, 128, 12, 162, 175, 19, 164, 125, 205, 6, 96, 34, 84, 13, 72, 89, 146, 152, 68, 191, 123, 145, 225, 109, 48, 173, 46, 177, 55, 176, 111, 163, 188, 104, 90, 67, 192, 203, 150, 248, 198, 186, 35, 249, 8, 201, 75, 194, 142, 28, 247, 184, 215, 137, 18, 42, 220, 245, 20, 2, 242, 246, 140, 238, 170, 218, 130, 197, 237, 178, 59, 44, 148, 155, 147, 211, 27, 74, 49, 5, 93, 120, 182, 180, 63, 38, 53, 103, 88, 17, 69, 228, 154, 41, 149, 64, 138, 77, 135, 91, 209, 21, 118, 250, 224, 116, 243, 7, 100, 129, 61, 189, 78, 223, 10, 144, 156, 29, 229, 47, 151, 70, 160, 101, 196, 16, 240, 66, 122, 217, 102, 193, 9, 181, 187, 79, 58, 213, 133, 22, 172, 45, 252, 24, 31, 233, 227, 1, 73, 179, 23, 166, 119, 222, 236, 158, 157, 254, 216, 221, 71, 83, 82, 110, 40, 15, 235, 132, 127, 11, 200, 239, 210, 231, 241, 161, 33, 99, 94, 36, 199, 165, 234, 195, 185, 136, 204, 43, 30, 226, 97, 214, 87, 251, 208, 174, 3, 108, 92, 86, 107, 112, 62, 159, 219, 98, 141, 124, 168, 65, 25, 50, 117, 76, 139, 212, 39, 106, 255, 131, 56, 95, 26, 54, 57, 14, 183, 126, 113, 169, 115, 206, 81, 253, 80, 105, 134, 167, 143, 230, 153, 232, 171, 52, 244, 121, 85, 190, 202, 51\}$.

$S^{-1} = \{0, 153, 65, 202, 1, 85, 15, 113, 50, 138, 120, 175, 8, 19, 231, 171, 131, 95, 60, 11, 64, 107, 145, 156, 149, 216, 228, 82, 55, 123, 194, 150, 2, 182, 17, 48, 185, 4, 91, 222, 170, 99, 61, 193, 77, 147, 32, 125, 30, 84, 217, 255, 249, 92, 229, 34, 226, 230, 142, 76, 3, 116, 208, 90, 101, 215, 133, 41, 24, 96, 127, 166, 20, 154, 83, 52, 219, 103, 118, 141, 240, 238, 168, 167, 18, 252, 205, 198, 94, 21, 40, 105, 204, 86, 184, 227, 16, 196, 211, 183, 114, 129, 136, 93, 39, 241, 223, 206, 203, 29, 169, 36, 207, 234, 5, 236, 111, 218, 108, 158, 87, 251, 134, 26, 213, 13, 233, 174, 7, 115, 72, 225, 173, 144, 242, 104, 191, 59, 102, 220, 68, 212, 54, 244, 121, 27, 22, 80, 78, 100, 44, 126, 23, 246, 98, 79, 122, 162, 161, 209, 128, 181, 9, 37, 12, 187, 157, 243, 214, 235, 70, 248, 146, 31, 201, 10, 35, 33, 75, 155, 89, 139, 88, 232, 57, 190, 47, 140, 38, 117, 253, 25, 42, 137, 53, 189, 130, 73, 46, 186, 176, 51, 254, 43, 192, 14, 237, 6, 200, 106, 178, 81, 221, 143, 197, 58, 164, 135, 71, 210, 62, 165, 159, 119, 110, 28, 195, 152, 97, 124, 245, 179, 247, 151, 188, 172, 160, 74, 69, 177, 132, 180, 66, 112, 250, 63, 67, 56, 45, 49, 109, 199, 148, 239, 163, 224\}$.