МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

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

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2025

Диссертация подготовлена на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Научный руководитель: **Чижов Иван Владимирович,**
кандидат физико-математических наук.

Официальные оппоненты: **Фомичёв Владимир Михайлович,**
доктор физико-математических наук, профессор, профессор кафедры теории вероятностей и кибербезопасности Российского университета дружбы народов имени Патриса Лумумбы.

Камловский Олег Витальевич,
доктор физико-математических наук, доцент, профессор кафедры 252 Института искусственного интеллекта МИРЭА-Российского технологического университета.

Таранников Юрий Валерьевич,
доктор физико-математических наук, профессор кафедры дискретной математики механико-математического факультета Московского государственного университета имени М.В. Ломоносова.

Защита состоится 12 ноября 2025 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.012.3 Московского государственного университета имени М.В. Ломоносова по адресу: 119234 Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М.В. Ломоносова механико-математический факультет, аудитория 1408.

Email: vasenin@msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на портале: https://dissovet.msu.ru/dissertation/3532

Автореферат разослан _____ 2025 года.

Ученый секретарь
диссертационного совета МГУ.012.3,
кандидат физико-математических
наук Галатенко А.В.

Общая характеристика работы

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[4], китайский стандарт SM4[5] 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[6]), аутентифицированное шифрование с дополнительными данными (режимы GCM[7], MGM[8]), алгоритм вычисления

[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] ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры // Москва: Стандартинформ. 2018.

[5] *Diffie, W., Ledin, G.* SMS4 Encryption Algorithm for Wireless Networks // IACR Cryptol. ePrint Arch. 2008. URL: https://api.semanticscholar.org/CorpusID:28508321.

[6] ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // Москва: Стандартинформ. 2018.

[7] *Dworkin, M.* NIST SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. 2007.

[8] Р 1323565.1.026-2019. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование // Москва: Стандартинформ. 2019.

аутентификационных векторов в сетях мобильной связи MILENAGE[9], основанный на шифрсистеме AES, и т.д.

Среди функций хэширования, построенных на основе XSL-схем, можно выделить российский стандарт Стрибог[10], международные стандарты организации ISO PHOTON[11] и Whirlpool[12]. Функции хэширования используются при вычислении контрольных сумм и имитовставок (HMAC[13]), при хранении и проверке паролей, при генерации и проверке электронных подписей, разработке постквантовых электронных подписей (финалист конкурса NIST алгоритм SPHINCS+[14]), вычислении аутентификационных векторов в сетях мобильной связи (алгоритм S3G[15], 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 $s \geq 8$ (см.[16]) . Данный показатель является оптимальным для защиты от разностного метода криптоанализа[17].
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 (см.[16]) . Данный показатель

[9] 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.

[10] ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования // Москва: Стандартинформ. 2018.

[11] *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`.

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

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

[14] 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`.

[15] 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.

[16] *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.

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

является важным для защиты от линейного метода криптоанализа[18].

3. Вопросы построения эффективно реализуемых линейных преобразований с высокими показателями рассеивания. В частности, не известны методы построения максимально рассеивающих циркулянтных матриц произвольной размерности[19]. 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[20].

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.

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.

---

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

[19] 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.

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

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.

Публикации. Основные результаты по теме диссертации изложены в 4 печатных изданиях общим объемом 3,4375 п.л. Из них 3, общим объемом 2,875 п.л., — в рецензируемых научных изданиях, определенных п. 2.3 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова.

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.

Краткое 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.

Введём основные обозначения, определения и сокращения, используемые в диссертации и автореферате.

$Q = \mathbb{F}_{q^s}$ 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 $\mathbb{F}_q$. Если результаты получаются независимо от многочлена $f(x)$, конкретный вид многочлена в формулировках не приводится. Единицу и ноль поля $\mathbb{F}_q$ будем обозначать как 1 и 0 соответственно.

$Q_{m,m}$ — кольцо квадратных матриц размера m над полем Q.

Линейные преобразования будем отождествлять 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.

ЛРП — линейная рекуррентная последовательность.

$Sym(Q)$ — симметрическая группа подстановок на множестве Q.

Результат применения произведения подстановок AB, $A, B \in Sym(Q)$ к элементу множества Q есть результат последовательного применения подстановок A, затем B к соответствующему элементу множества Q.

$A_1 \sqcup A_2$ — объединение непересекающихся множеств A_1, A_2.

Нумерацию координат векторов будем вести справа налево, а нумерацию строк матриц — снизу вверх. Все нумерации будем начинать с нуля.

Длину блока будем обозначать буквой n, количество s-битных S-блоков m, $n = ms$.

Под раундом XSL-схемы мы понимаем последовательность следующих трёх преобразований:

– покоординатное наложение ключа по модулю 2 (XOR);

– нелинейное преобразование $\overline{S}$ ($\overline{S} = (S_{m-1},...,S_0)$, слой S-блоков);
– применение линейного преобразования (L-слой).

Определение 1.1. [19] *Показателем рассеивания матрицы* $A \in Q_{m,m}$ будем называть следующее число:

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

где $\omega(\overrightarrow{a})$ — вес Хэмминга вектора $\overrightarrow{a}$. Если $\tau(A) = m+1$, матрицу A будем называть *максимально рассеивающей матрицей.*

Определение 1.2. [16] 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.*

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 1.3. [16] *Алгебраической степенью* $deg(S)$ преобразования S называется максимальная из степеней многочленов Жегалкина булевых функций $S_{s-1},...,S_0$.

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 1.4. [16] Для любого $v \in V_s \backslash 0$ булева функция $\langle v,S \rangle = v_{s-1}S_{s-1}(x) + ... + v_0S_0(x)$ называется *компонентной функцией преобразования* S.

Определение 1.5. [21] *Степенью нелинейности* $nldeg(S)$ преобразования S называется минимальная из степеней многочленов Жегалкина среди всех компонентных функций преобразования S.

[21] *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.

Определение 1.6. [16] *Нелинейностью* $nl(S)$ преобразования S называется минимальное из расстояний Хемминга между всеми компонентными функциями преобразования S и аффинными булевыми функциями от s переменных.

Определение 1.7. Пусть $M \subseteq V_n$. *Булевой функцией-индикатором* множества M называется функция $f(x) : V_n \to V_1$, равная 1 тогда и только тогда, когда аргумент $x \in M$.

Определение 1.8. [21] *Графовой алгебраической иммунностью* $AI(S)$ преобразования S называется алгебраическая иммунность булевой функции-индикатора множества $\Gamma_S = \{(x,S(x))|x \in V_s\} \subseteq V_{2s}$.

Глава 1 посвящена построению дифференциально 4-равномерных подстановок с использованием *Конструкции 1*, являющейся обобщением метода построения подстановок, предложенного в теореме 2 работы[22]. Метод заключается в ограничении значений известных APN-преобразований пространства V_{s+1} на некоторую гиперплоскость, представимую как пространство V_s.

Определение 1.9. Подмножество K пространства V_{s+1} будем называть подмножеством, порождающим простое разбиение, если существует такой вектор $\gamma \in V_{s+1}$, что справедливо равенство

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

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

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). 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.*

[22] *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`.

По аналогии с работой[22], в случае использования в *Конструкции 1* почти бент[23] (максимально нелинейных) преобразований нечётной размерности $2k+1$ нелинейность полученной подстановки будет максимальной из всех известных значений нелинейности для подстановок в V_{2k}.

Авторы работы[22] для построения использовали обратные квадратичным APN-подстановки. Среди степенных APN-подстановок *Конструкция 1* применима только к таким подстановкам, что показано в следующей теореме.

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

Тем не менее, *Конструкция 1* допускает использование APN-преобразований (не обязательно подстановок) любой алгебраической степени. Соответствующие примеры получены теоретически и экспериментально, приведём их далее.

Пример 1.1. Рассмотрим единственную (с точностью до эквивалентности) известную на данный момент APN-подстановку от чётного числа переменных $s = 6$ Дж. Диллона и др.[24], 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*.

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

В работе[25] были построены следующие кубические почти бент преобразования для четных $s = 2k \geq 2$:

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

где $x \in V_{s+1}$, $gcd(s+1, j) = 1, \mathrm{tr}_2^{s+1}$ — функция след из поля $\mathbb{F}_{2^{s+1}}$ в поле $\mathbb{F}_2$.

Преобразование (2) не является подстановкой на пространстве V_{s+1}. Рассмотрим гиперплоскость $H_0 = \{u \in V_{s+1} | \mathrm{tr}_2^{s+1}(u) = 0\} \subset V_{s+1}$.

---

[23] *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.

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

[25] *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`.

Теорема 1.6. *Преобразование (2) инъективно на* H_0, *и* $\alpha + \beta \neq 1$ *для любых* $\alpha,\beta \in G(H_0)$.

Теорема 1.6 показывает возможность применения *Конструкции 1* к классу кубических APN-преобразований (2), не являющихся подстановками. Построенные дифференциально 4-равномерные подстановки обладают максимально известной нелинейностью среди подстановок на множестве $V_s, s = 2k$. 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.

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[26]. Для получения результата линейного преобразования остаётся выполнить приведение по модулю, сложность которого зависит от многочлена модуля.

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:

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

Пусть далее поле $P = \mathbb{F}_2$, свободный член многочлена $f(x)$ равен 1. 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, на диагонали которой стоят элементы вектора β.
3. *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.

[26] *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`.

4. *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 соответствующих многочленам векторов длины n.

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* $deg\ \overline{f(x)} \leq n/2$, *то преобразование* $\widehat{a}$ *может быть реализовано пятью командами процессора:* 3 $CLMUL$ + 2 XOR;
2) *если* $deg\ \overline{f(x)} + deg\ a(x) \leq n$, *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.*

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.

Теоретических методов построения максимально рассеивающих матриц-циркулянтов произвольной размерности 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 размера, чем 32×32.

В связи с этим в диссертации 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 (3)).

Рассмотрим разложение

$$A = \sum_{i=1}^{t} D_i A_i, \tag{3}$$

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 $n \times n$, реализующие умножение на многочлен $a_i(x)$ по модулю многочлена $f(x)$.

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 (3).

Утверждение 2.4. *Пусть для матрицы A и многочлена $x^n + 1$ справедливо разложение (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 (3) совпадает с рангом матрицы $B = Rev_{f(x)}(A)$.*

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.

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 (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 (3), содержащее не более k слагаемых.*

Разложения вида (3) для матриц, используемых в шифрсистеме AES и хэш-функции Whirlpool состоят из двух и четырёх слагаемых соответственно.

Отметим, что скорость выполнения команд процессора разная, 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.

В **главе 3** изучаются рекурсивные матрицы над полем $\mathbb{F}_{q^s}$.

Определение 3.1. Пусть $k > 1$, $f(x)$ — многочлен над полем $Q = \mathbb{F}_{q^s}$, $S(f(x))$ — сопровождающая матрица многочлена $f(x)$. Матрицу $S(f(x))^k$ будем называть *рекурсивной матрицей*.

В начале главы показано, что транспонированная сопровождающая матрица $S^\top = S(f(x))^\top$ задаётся через умножение на элемент x кольца $Q[x]/f(x)$. 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.

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:*

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

где $(c_{2m-2},\dots,c_0)$ — последовательные элементы ЛРП с характеристическим многочленом $f(x)$. Матрица вида (4) является Ганкелевой матрицей.

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 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 диссертации приведены два способа выбора отрезков ЛРП, позволяющих получать эффективно реализуемые матрицы перехода C и C^{-1}. На основе одного из способов предлагается разложение рекурсивной матрицы в

произведение двух эффективно реализуемых матриц F и C. Частный случай соответствующего разложения для рекурсивной матрицы линейного преобразования шифрсистемы Кузнечик был получен в работе[27].

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* $(1,0,...,0)\cdot S^{m-1} = (c_{m-1},...,c_1,1)$. *Тогда справедливо следующее разложение матрицы* A *в произведение матриц* $F \cdot C$*:*

$$A = \begin{pmatrix} f_{m-1} & f_{m-2} & ... & f_1 & f_0 \\ f_{m-2} & f_{m-3} & ... & f_0 & 0 \\ ... & ... & ... & ... & ... \\ f_1 & f_0 & ... & 0 & 0 \\ f_0 & 0 & ... & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c_{m-1} & c_{m-2} & ... & c_1 & 1 \\ c_{m-2} & c_{m-3} & ... & 1 & 0 \\ ... & ... & ... & ... & ... \\ c_1 & 1 & ... & 0 & 0 \\ 1 & 0 & ... & 0 & 0 \end{pmatrix} \quad (5)$$

В заключительной части главы приведены известные и предложены новые реализации рекурсивных матриц. В таблице 1 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.

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.

Известная реализация с использованием предвычисленных LUT-таблиц[28] 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, полученные в диссертации, позволяют предложить реализации 4 и 5 соответственно. Реализация 4 (на основе разложения из теоремы 3.2) позволяет сократить

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

[28] *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).

Таблица 1 — Сравнение различных реализаций шифрсистемы Кузнечик.

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

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.

Результаты скорости шифрования во многом согласуются с полученными теоретическими оценками и позволяют предположить, что на вычислителях с небольшим объёмом быстродоступной памяти реализация 4 будет наиболее эффективной.

В **главе 4** изучаются инвариантные подпространства матриц-циркулянтов и рекурсивных матриц. Для XSL-схем наиболее распространён случай использования нелинейного преобразования $\overline{S}$, как параллельного применения одинаковых S-блоков S. В таком случае можно выделить класс подпространств, инвариантных относительно преобразования $\overline{S}$ независимо от выбора S-блока.

Определение 4.1. 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 4.1. *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 $\widetilde{W} = Q^d$.*

Определение 4.2. Подпространство W пространства Q^m, для которого $\widetilde{W}$ является пространством Q^d при некотором d, будем называть подпространством *вида 1*.

Если подпространство *вида 1* инвариантно относительно линейного преобразования, оно является инвариантным относительно преобразования SL и необходимым условием стойкости шифрсистемы к методу

инвариантных подпространств является использование раундовых ключей X, не лежащих в соответствующем подпространстве[20]. 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.

Пусть далее

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

где $\otimes r$ означает кронекерову степень матрицы.

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

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

В работе[29] найден класс вложенных инвариантных подпространств матриц-циркулянтов. Данные подпространства имеют вид:

$$\langle \overrightarrow{B}_0 \rangle, \langle \overrightarrow{B}_0, \overrightarrow{B}_1 \rangle, \langle \overrightarrow{B}_0, \overrightarrow{B}_1, \overrightarrow{B}_2 \rangle, ..., \langle \overrightarrow{B}_0, \overrightarrow{B}_1, \overrightarrow{B}_2, \overrightarrow{B}_3, ..., \overrightarrow{B}_{2^r-1} \rangle. \qquad (6)$$

Каждое подпространство указанного класса является подпространством *вида 1*.

Теорема 4.1. *Пусть* $Q = \mathbb{F}_{2^s}$, $r \in \mathbb{N}$, $C = Circ_{2^s}(c_{2^r-1},...,c_0) \in Q_{2^r,2^r}$ *Тогда* $B^{-1}CB = T$, *где* $T \in Q_{2^r,2^r}$ — *верхнетреугольная матрица Тёплица вида:*

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

Отношение «$\preceq$» определено для векторов, представляющих числа в двоичной системе счисления: $a = (a_{r-1}2^{r-1} + ... + a_1 2 + a_0)$, $a \preceq b$ тогда и только тогда, когда $a_i \leq b_i$ для всех разрядов i.

[29] *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.

Теорема 4.1 уточняет результат из работы[29]: 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 условии, представленном в теореме 4.2.

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 из цепочки (6).*

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 из цепочки (6).*

Пример 4.3. В шифрсистеме AES и хэш-функции Whirlpool используются максимально рассеивающие матрицы-циркулянты. Инвариантные подпространства данных матриц есть подпространства из цепочки (6), и только они.

Раундовые ключи шифрсистемы AES и константы хэш-функции Whirlpool не лежат в соответствующих подпространствах, что не позволяет провести атаку на основе инвариантных подпространств.

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.*

В теореме 4.3 представлены условия, при которых рекурсивная матрица не имеет инвариантных подпространств *вида 1.* Распространённым способом построения максимально рассеивающих рекурсивных матриц является использование порождающей матрицы БЧХ-кода. Таким образом построена матрица линейного преобразования шифрсистемы Кузнечик. Корни многочлена $f(x)$ есть элементы БЧХ-цепочки, которые обязательно различны, это позволяет использовать теорему 4.3.

Следствие 4.3. *Матрица линейного преобразования шифрсистемы Кузнечик не имеет собственных инвариантных подпространств вида 1.*

В **заключении** приведены основные результаты работы, которые состоят в следующем:

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 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. 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 и хэш-функции Whirlpool.
3. Найдены все решения уравнения подобия для сопровождающей матрицы многочлена над конечным полем и её транспонированной матрицы. На их основе получены разложения для произвольной рекурсивной матрицы и предложены новые программные реализации шифрсистемы Кузнечик, 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.

В **приложении** представлены два примера построенных дифференциально 4-равномерных подстановок.

Результаты диссертации могут быть интересны специалистам в области криптографии и линейной алгебры.

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.

Публикации автора по теме диссертации

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

1. С. А. Давыдов, И. А. Круглов. Метод синтеза дифференциально 4-равномерных подстановок пространства V_m для четных m // Дискретная математика — 2019. — Т. 31, № 2. — С. 69—76. 0,5 п.л., ВАК, RSCI. Импакт-фактор 0,220 (РИНЦ). Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%, 0,465 п.л., EDN: ZJDZIL.

2. С. А. Давыдов, Ю. Д. Шкуратов. Использование матриц-циркулянтов над $\mathbb{F}_2$ при построении эффективных линейных преобразований с высокими показателями рассеивания // Математические вопросы криптографии — 2024. — Т. 15, № 2. — С. 29—46. 1,125 п.л., ВАК, RSCI. Импакт-фактор 0,143 (РИНЦ). Соавтору принадлежат лемма 1 и теорема 2. Остальные результаты получены Давыдовым С.А. – 86%, 0,9675 п.л., EDN: WYZJQK.

3. С. А. Давыдов. Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц // Дискретная математика — 2024. — Т. 36, № 4. — С. 44—63. 1,25 п.л., ВАК, RSCI. Импакт-фактор 0,220 (РИНЦ). EDN: YWWKFP.

Другие публикации автора по теме диссертации.

4. 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. Импакт-фактор 0,492 (РИНЦ). Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%, 0,534 п.л., EDN: EVYWMG.

Давыдов Степан Андреевич

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

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Отдел полиграфии Научной библиотеки МГУ имени М.В. Ломоносова
119192, Москва, Ломоносовский проспект, 27.