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

Актуальность темы диссертации.

Тема диссертационного исследования С.А. Давыдова «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах» представляется высокоактуальной и значимой для современной криптографии. Её актуальность детерминирована комплексом фундаментальных и прикладных вызовов, стоящих перед областью защиты информации.

Архитектура XSL (XOR-Substitution-Linear) является де-факто стандартом для построения блочных шифров и хэш-функций. На её основе созданы такие критически важные алгоритмы, как американский стандарт AES, российские стандарты «Кузнечик» и «Стрибог», китайский SM4, а также многие международные хэш-функции (Whirlpool, PHOTON). Устойчивость и эффективность этих алгоритмов, используемых для обеспечения конфиденциальности и целостности данных в финансовом секторе, телекоммуникациях и государственном управлении, напрямую зависят от криптографической стойкости их компонентов – нелинейных S-блоков и линейного слоя L. Следовательно, любое углубление понимания их свойств и совершенствование методов их построения имеет стратегическое значение для всей инфраструктуры информационной безопасности.

Исследование направлено на преодоление ряда сложных и открытых проблем в синтезе криптографических примитивов, длительное время остающихся в фокусе внимания мирового криптографического сообщества.

Вопрос о существовании совершенных нелинейных (APN) подстановок в бинарных векторных пространствах чётной размерности $s \geq 8$ остается одной

из самых известных нерешённых задач в теории криптографии. В этом контексте разработка новых конструктивных методов синтеза дифференциально 4-равномерных подстановок (являющихся наилучшими из известных для чётных s), обладающих одновременно высокой нелинейностью, удовлетворительной алгебраической степенью и графовой алгебраической иммунностью, представляет собой высокоактуальную научную задачу.

Актуальной является задача построения линейных преобразований с оптимальными свойствами. Не существует универсальных аналитических методов построения максимально рассеивающих матриц (MDS-матриц) произвольной размерности для таких важных классов, как циркулянты. Актуальным является как поиск новых методов синтеза таких матриц, так и разработка эффективных, в том числе низкоресурсных, реализаций уже существующих линейных преобразований, используемых в стандартизированных алгоритмах.

Постоянное развитие методов криптоанализа, таких как метод инвариантных подпространств и его нелинейных обобщений, требует проведения превентивного анализа устойчивости широко используемых криптографических стандартов. Исследование инвариантных подпространств для ключевых классов линейных преобразований (циркулянтов и рекурсивных матриц) является насущной необходимостью для верификации и обоснования их стойкости.

Таким образом, тема диссертации, посвященной обеспечению стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности актуальна как в теоретическом, так и в прикладном смысле.

Основное содержание работы.

Первая глава диссертации посвящена решению одной из ключевых задач криптографии — синтезу нелинейных преобразований (S-блоков) с

высокими криптографическими характеристиками. Основное внимание уделено построению дифференциально 4-равномерных подстановок для пространств четной размерности, что является оптимальным известным показателем для защиты от дифференциального криптоанализа в случае, когда существование идеальных APN-подстановок остается открытой проблемой.

В основе главы лежит разработанная автором «Конструкция 1», которая является развитием и обобщением подхода, предложенного в более ранних работах. Суть метода заключается в получении подстановки в пространстве размерности s путем ограничения APN-преобразования (дифференциально 2-равномерного), заданного в пространстве большей размерности $s+1$, на специально выбранное подмножество. В отличие от предыдущих методов, использовавших только квадратичные APN-подстановки, новая конструкция допускает использование преобразований любой алгебраической степени. Для этого вводится понятие «подмножества, порождающего простое разбиение», которое обобщает идею гиперплоскости, используемую в прототипах.

Теоретической основой главы являются строгие математические доказательства свойств предлагаемой конструкции. Теорема 1.2 устанавливает, что результирующее преобразование действительно является дифференциально 4-равномерной подстановкой. Теорема 1.4 дает эквивалентные условия применимости конструкции, а Теорема 1.5 полностью описывает класс степенных APN-подстановок, к которым эта конструкция может быть применена. Важным результатом является Теорема 1.6, которая демонстрирует возможность использования конструкции не только для подстановок, но и для некоторых классов почти бент-преобразований, не являющихся биекциями.

Практическим выходом исследований является построение конкретных примеров S-блоков с улучшенными свойствами. В частности, для

размерности s=8 была построена подстановка с дифференциальной равномерностью 4, алгебраической степенью 3, нелинейностью 112 и графовой алгебраической иммунностью 2. Эти показатели соответствуют лучшим известным образцам, что подтверждает эффективность предложенного метода. Таким образом, первая глава содержит целостную теорию синтеза нелинейных преобразований, подкрепленную строгими доказательствами и практическими результатами, направленную на усиление стойкости S-блоков в XSL-схемах.

Вторая глава диссертации посвящена исследованию эксплуатационных характеристик линейных преобразований, заданных через умножение на элемент кольца многочленов. Основное внимание уделено матрицам-циркулянтам над полем $\mathbf{F}_2$, которые находят широкое применение в таких стандартах, как AES, SM4 и Whirlpool. Центральной задачей главы является поиск эффективных программных реализаций этих преобразований, что особенно актуально в условиях ограниченных вычислительных ресурсов.

Ключевым результатом главы является разработка метода разложения произвольной матрицы A в сумму вида $\sum_{i=1}^{t} D_i A_i$, где D_i – диагональные матрицы, а A_i – матрицы, реализуемые через умножение на элемент кольца. Теорема 2.1 устанавливает, что минимальное количество слагаемых t в таком разложении совпадает с рангом матрицы $B=\mathrm{Rev}_{f(x)}(A)$, что позволяет эффективно оценивать сложность реализации. Для циркулянтных матриц доказано (Утверждение 2.5), что число слагаемых не превосходит s, где s – размерность S-блока, а в частных случаях может быть существенно меньше.

Практическая значимость результатов продемонстрирована на примерах разложений матриц из стандартов AES (2 слагаемых) и Whirlpool (4 слагаемых). Особое внимание уделено эффективной реализации с использованием процессорной команды CLMUL, позволяющей выполнять умножение многочленов за одну операцию. Показано, что для циркулянтных

матриц с модулем $f(x)=x^n+1$ преобразование может быть реализовано всего за две команды процессора (CLMUL и XOR), что существенно повышает производительность криптографических алгоритмов. Таким образом, вторая глава предлагает комплексный подход к оптимизации линейных преобразований, сочетающий теоретические оценки с практическими методами эффективной реализации.

Третья глава диссертации посвящена глубокому исследованию рекурсивных матриц — важного класса линейных преобразований, используемых в таких криптографических примитивах, как отечественный стандарт «Кузнечик» и семейство хэш-функций PHOTON. Основной фокус главы направлен на разработку эффективных методов реализации этих преобразований, что особенно актуально для систем с ограниченными вычислительными ресурсами. В отличие от циркулянтных матриц, рекурсивные матрицы позволяют строить максимально рассеивающие преобразования больших размерностей, однако их программная реализация традиционно требует значительных ресурсов памяти.

Теоретической основой главы являются результаты о разложении рекурсивных матриц. Ключевым достижением является Теорема 3.1, в которой найдены все решения уравнения подобия для сопровождающей матрицы многочлена, что позволило установить взаимно-однозначное соответствие между матрицами подобия и линейными рекуррентными последовательностями. На этой основе в Теореме 3.2 получено разложение произвольной рекурсивной матрицы $A=S^m$ в произведение $A=F\cdot C$ двух эффективно реализуемых матриц специального вида. Это разложение, в частности, обобщает известные результаты для шифросистемы «Кузнечик».

Практическая значимость результатов подтверждена разработкой и сравнительным анализом новых способов реализации. Предложены два принципиально новых метода: реализация через разложение рекурсивной

матрицы (п. 3.4.2) и реализация через умножение на элемент кольца с переходом в соответствующий базис (п. 3.4.3). Проведенное экспериментальное исследование для шифросистемы «Кузнечик» показало, что новая реализация на основе разложения (Реализация 4) демонстрирует наилучший баланс между скоростью работы (87.1 Мб/с) и объемом используемой памяти (8 Кб), что делает её предпочтительной для устройств с ограниченной быстродоступной памятью. Таким образом, третья глава предлагает комплексный подход к оптимизации рекурсивных преобразований, сочетающий фундаментальные математические результаты с практическими решениями для эффективной программной реализации.

Четвертая глава диссертации посвящена критически важному аспекту криптоанализа — исследованию инвариантных подпространств линейных преобразований, используемых в XSL-схемах. Основной фокус направлен на изучение матриц-циркулянтов и рекурсивных матриц, которые применяются в таких алгоритмах, как AES, «Кузнечик», Whirlpool и PHOTON. Целью данной главы является систематический анализ уязвимостей, которые могут возникнуть при наличии у линейного слоя инвариантных подпространств, согласованных со структурой нелинейного слоя.

В главе вводится и детально исследуется класс подпространств «вида 1», которые остаются инвариантными относительно нелинейного преобразования $S=(S,S,...,S)$ при любом выборе S-блока S. Ключевым результатом является Теорема 4.2, в которой установлено, что для максимально рассеивающих матриц-циркулянтов размерности $2^r \times 2^r$ не существует других инвариантных подпространств, кроме цепочки вложенных подпространств, описанной в утверждении 4.3. Это доказано путем приведения матрицы-циркулянта к верхнетреугольному виду Тёплица (Теорема 4.1) и использования условий невырожденности подматриц MDS-матриц.

Для рекурсивных матриц в Теореме 4.3 получены достаточные условия отсутствия инвариантных подпространств вида 1. Показано, что если характеристический многочлен сопровождающей матрицы не имеет кратных корней, а порядок каждого корня превышает $m-1$, что выполняется для матриц, построенных на основе кодов БЧХ, то таких подпространств не существует. Следствие 4.4 констатирует, что линейное преобразование шифросистемы «Кузнечик» удовлетворяет этим условиям, что является весомым аргументом в пользу его стойкости к атакам на основе инвариантных подпространств. Таким образом, четвертая глава предоставляет мощный теоретический аппарат для анализа и обоснования стойкости широкого класса криптографических алгоритмов.

Новизна научных результатов.

Научные результаты, представленные в диссертации С.А. Давыдова, обладают высокой степенью научной новизны и вносят существенный вклад в развитие теории и практики криптографии. Новизна подтверждается следующими ключевыми результатами.

В диссертации предлагаются принципиально новые конструкции и методы. Разработана «Конструкция 1» для построения дифференциально 4-равномерных подстановок, являющаяся существенным развитием известных подходов. Её новизна заключается в обобщении метода ограничения на произвольные «подмножества, порождающие простое разбиение» (вместо только гиперплоскостей); возможности применения к APN-преобразованиям любой алгебраической степени, а не только к квадратичным, что значительно расширяет класс используемых функций, применимости к небиективным почти бент-преобразованиям, что позволило впервые построить подстановки с заданными свойствами из такого класса функций.

В диссертации получены фундаментальные теоретические результаты. Впервые получено полное описание всех решений уравнения

подобия $S=C^{-1}S^{T}C$ для сопровождающей матрицы многочлена над конечным полем (Теорема 3.1). Это позволило установить взаимно-однозначное соответствие между матрицами подобия и линейными рекуррентными последовательностями.

В диссертации впервые полностью описаны инвариантные подпространства максимально рассеивающих матриц-циркулянтов (Теорема 4.2). Показано, что при условии максимального рассеивания и размера, равного степени двойки, других инвариантных подпространств, кроме известной цепочки, не существует. Найдены и доказаны достаточные условия отсутствия инвариантных подпространств вида 1 у рекурсивных матриц (Теорема 4.3). Это новый теоретический результат, имеющий важное значение для криптоанализа.

Предложен новый метод разложения произвольной матрицы в сумму произведений диагональных матриц и матриц, реализуемых через умножение на элемент кольца, с оценкой минимального числа слагаемых (Теорема 2.1). Получены новые разложения рекурсивных матриц в произведение двух эффективно реализуемых матриц (Теорема 3.2), которые являются обобщением ранее известных частных решений. Разработаны и практически испытаны новые низкоресурсные реализации линейных преобразований для шифросистемы «Кузнечик», показавшие конкурентное соотношение «скорость/память» по сравнению с известными аналогами.

В диссертации решены конкретные научные проблемы. Впервые применена разработанная конструкция для построения дифференциально 4-равномерной подстановки из кубического небиективного почти бент-преобразования, что демонстрирует принципиальную новизну подхода. Впервые строго обоснована невозможность применения атак на основе инвариантных

подпространств вида 1 к линейным преобразованиям алгоритмов «Кузнечик» и AES в определенной конфигурации.

Таким образом, научная новизна работы носит комплексный и фундаментальный характер, проявляясь как в создании новых теоретических конструкций и доказательстве теорем, так и в разработке практических методов и алгоритмов, имеющих непосредственное приложение для повышения безопасности и эффективности современных криптографических стандартов.

Обоснованность и достоверность научных положений, выводов и рекомендаций, сформулированных в диссертации.

Научные положения, выводы и рекомендации, представленные в диссертационной работе С.А. Давыдова, характеризуются высокой степенью обоснованности и достоверности, что подтверждается следующими ключевыми аспектами:

Работа использует строгий математический аппарат. Все основные результаты работы — включая конструкцию дифференциально 4-равномерных подстановок, разложения циркулянтных и рекурсивных матриц, а также описание их инвариантных подпространств — сопровождаются полными и строгими доказательствами. В частности, теоремы 1.2, 1.4-1.6 в первой главе, теорема 2.1 во второй, теоремы 3.1-3.2 в третьей и теоремы 4.1-4.3 в четвертой главе содержат корректные математические выводы, основанные на методах современной алгебры, теории конечных полей и теории линейных рекуррентных последовательностей.

Теоретические результаты подкреплены практическими исследованиями. Например, в разделе 1.2 представлены конкретные примеры построенных подстановок с вычисленными криптографическими параметрами. В главе 3 проведено комплексное сравнение различных реализаций шифросистемы

«Кузнечик» на языке C++, где замеры скорости и объема памяти объективно подтвердили эффективность предложенных автором новых методов реализации (реализации 4 и 5).

Основные результаты диссертации были представлены на ведущих международных и российских научно-практических конференциях по криптографии («РусКрипто», симпозиум «Современные тенденции в криптографии») и опубликованы в рецензируемых журналах, рекомендованных ВАК, включая «Дискретная математика» и «Математические вопросы криптографии». Факт публикации в этих изданиях, а также наличие библиографических ссылок на работы автора в других научных статьях, свидетельствует о признании и достоверности полученных результатов научным сообществом.

Полученные в диссертации результаты не противоречат установленным научным фактам и гармонично развивают существующие подходы. Так, конструкция построения S-блоков является обобщением и развитием методов, предложенных в работах [34], [37], а разложения рекурсивных матриц согласуются с частными результатами, известными для шифросистемы «Кузнечик» [53]. Выводы об инвариантных подпространствах циркулянтов дополняют и уточняют результаты, полученные в [46].

Представленные в работе алгоритмы, конструкции и разложения сформулированы достаточно четко и детально, чтобы другие исследователи могли их воспроизвести и проверить. Это касается как алгоритмических процедур (например, разложения матриц в главах 2 и 3), так и аналитических методов (описание инвариантных подпространств в главе 4).

Таким образом, комплексное использование строгих математических методов, практическая экспериментальная проверка, апробация в научном сообществе и соответствие фундаментальным научным принципам

обеспечивают высокую обоснованность, достоверность и научную ценность всех положений, выводов и рекомендаций, выносимых на защиту.

Замечания к диссертации.

В работе представлено сравнение реализаций для шифросистемы "Кузнечик", однако отсутствует развернутое сравнение предложенных S-блоков (Глава 1) и методов разложения матриц (Главы 2-3) с наиболее современными и известными аналогами из международных исследований. Например, не приведено сравнение предложенных дифференциально 4-равномерных подстановок с лучшими известными конструкциями других авторов по таким параметрам, как сопротивление алгебраическим атакам, эффективность аппаратной реализации.

Основной фокус работы сосредоточен на программных реализациях и математических моделях. Между многие криптографические алгоритмы, особенно для низкоресурсных устройств, предназначены для аппаратной реализации (ASIC, FPGA). В работе в недостаточной степени исследуется потенциал и возможные ограничения предложенных методов разложения матриц и новых линейных преобразований с точки зрения их аппаратной эффективности (площадь кристалла, энергопотребление, задержка).

Для новых S-блоков, построенных в Главе 1, приведены основные криптографические характеристики (дифференциальная равномерность, нелинейность, алгебраическая иммунность). Однако отсутствует анализ их стойкости к более специализированным атакам, таким как алгебраические атаки с использованием SAT-солверов, атаки на основе отказов (fault attacks) или анализ на устойчивость к атакам по побочным каналам (side-channel attacks).

В то время как практическая значимость разложений для "Кузнечика", AES и Whirlpool показана убедительно, практическая применимость результатов по инвариантным подпространствам (Глава 4) сформулирована в несколько общем виде. Не в полной мере раскрыто, как именно эти результаты должны повлиять на процесс разработки и анализа будущих стандартов, кроме констатации факта стойкости конкретных алгоритмов.

В библиографическом списке обнаружены опечатки в именах известных авторов. В пункте [34] французский исследователь Клод Карле (Claude Carlet) ошибочно указан как "Claude, C.", в то время как в других пунктах (например, [36]) его фамилия указана корректно: "Carlet, C.". В пункте [63] фамилия и инициалы основателя Энциклопедии целочисленных последовательностей (OEIS) Нила Слоэна (Neil J. A. Sloane) ошибочно указаны как "С. Н. Д. А.". Это сочетание букв не соответствует ни реальным инициалам автора (N. J. A.), ни стандартным правилам транслитерации.

Заключение по диссертации.

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

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

Официальный оппонент:
Доктор физико-математических наук,
профессор кафедры дискретной математики
механико-математического факультета
ФГБОУ ВО «Московский государственный
университет имени М. В. Ломоносова»

ТАРАННИКОВ Юрий Валерьевич

Контактные данные:

Специальность, по которой официальным оппонентом защищена диссертация:2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Адрес места работы:
119991, ГСП-1, Москва, Ленинские горы, МГУ, д.1,
главное здание МГУ, механико-математический факультет
Тел.: 7(495)9391244; e-mail: office@mech.math.msu.su

Подпись сотрудника кафедры дискретной математики
механико-математического факультета МГУ имени
М.В.Ломоносова Таранникова Ю.В. удостоверяю: