Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики»

На правах рукописи

Фомин Денис Бониславович

Построение нелинейных биективных преобразований для алгоритмов защиты конфиденциальности данных в недоверенных средах

РЕЗЮМЕ ДИССЕРТАЦИИ

на соискание учёной степени
кандидата наук по прикладной математике

Научный руководитель:
кандидат физико-математических наук, доцент
Нестеренко Алексей Юрьевич

Москва — 2023

Введение

Диссертационное исследование посвящено решению задачи повышения уровня безопасности алгоритмических методов защиты информации, при синтезе которых в том числе необходимо использовать нелинейные биективные преобразования (подстановки). Для невозможности применения известных методов анализа необходимо гарантировать значения их показателей нелинейности. При этом функционирование алгоритмов защиты конфиденциальности данных происходит в условиях недоверенной среды, а именно при возможности нарушителя получать информацию о времени выполнения операций, что налагает дополнительные требования на конструкции нелинейных биективных преобразований. Не теряя общности, в рамках данного диссертационного исследования рассматриваются только вопросы обеспечения конфиденциальности данных.

В настоящее время все больше развиваются облачные технологии, когда часть вычислительных задач (или целиком работа операционной системы) происходит на удаленном вычислительном устройстве, которое, как правило, принадлежит некоторому поставщику услуг. Степень доверия к облачной инфраструктуре зависит от используемых средств защиты, которые формируются на основе модели нарушителя, для исследования достаточности которой необходимо проведение всесторонних исследований. Ввиду наличия аппаратных вычислительных средств на стороне поставщика услуг, у нарушителя появляются дополнительные возможности, связанные с возможностью использования информации из побочных каналов утечки. Одним из наиболее распространенных таких каналов является время выполнения операций на вычислительном устройстве.

В диссертации проводится изучение возможностей нарушителя, приводящих к невозможности обеспечения свойства конфиденциальности данных при реализации алгоритмов их защиты в недоверенной среде на графических вычислителях. В частности показано, что используемые на момент проведения исследования программные средства, их реализующие, потенциально не являются безопасными, что приводит к необходимости использования иных способов их реализации.

Для эффективной реализации алгоритмов защиты конфиденциальности данных необходима возможность представления его нелинейных преобразований в виде «небольшого» количества логических операций. В то же время стойкость

алгоритма напрямую зависит от показателей нелинейности подстановок, используемых при его синтезе. В диссертационном исследовании рассматриваются вопросы построения эффективно реализуемых нелинейных биективных преобразований, имеющих «высокие» показатели нелинейности, что позволяет их использовать при синтезе перспективных алгоритмов защиты конфиденциальности данных. Также в диссертации предлагается новый метод анализа алгоритмов защиты конфиденциальности данных, основанный на особенностях используемых нелинейных преобразований. Для гарантирования невозможности применения разработанного метода предложен и обоснован подход, позволяющая оценить стойкость используемого алгоритма защиты конфиденциальности данных.

Актуальность. Увеличение количества вычислительных устройств приводит к необходимости обработки больших объемов данных. При этом постоянно происходят передача, обработка, хранение конфиденциальной информации, для защиты которой применяются различные программно-аппаратные и организационные меры. Обеспечение конфиденциальности информации на протяжении большого количества времени представляет собой сложную и актуальную задачу, решение которой связано с синтезом средств защиты информации.

Дополнительной сложностью обеспечения свойств безопасности данных при реализации алгоритмов их защиты является возможность получения нарушителем дополнительной информации из побочных каналов утечки. В 1995 году впервые опубликована статья, в которой была показана принципиальная возможность использования времени выполнения операций для восстановления неизвестной нарушителю информации при реализации различных алгоритмов обеспечения безопасности данных, [44]. В настоящее время, при реализации методов защиты информации необходимо учитывать такие возможности нарушителя, что находит свое отражение в нормативных документах [4; 5].

От правильного выбора модели нарушителя зависит как безопасность информационной системы в целом, так и сложность обеспечения ее корректного функционирования. Недостаточные требования могут привести к нарушению свойств безопасности информационной системы, завышенные же — к невозможности или высокой сложности ее использования.

Возможность реализации методов анализа, использующих информацию о времени выполнения операций на центральном процессоре ЭВМ хорошо известна, [44]. Более того, использование современных стандартизированных алгоритмов защиты конфиденциальности данных оказывается не безопасным

относительно таких методов анализа (см. напр. [8; 13]). Архитектура же графических сопроцессоров сильно отличается от архитектуры центрального процессора современной ЭВМ: они являются массивно-параллельными вычислительными устройствами, одновременно реализующими большое количество простых операций.

Таким образом, задача исследования возможности применения методов анализа с использованием информации из побочных каналов утечки в целом и, в частности, по времени выполнения операций при реализации алгоритмов защиты информации на графических вычислителях является актуальной. Более того, в работе [45] хоть и говорится о потенциальной возможности реализации таких методов анализа, однако предполагается что их применение будет не эффективным или может быть невозможным при минимальном изменении способа реализации алгоритма защиты конфиденциальности данных.

Один из способов защиты от методов анализа, использующих информацию о времени выполнения операций в вычислительном устройстве, является реализация преобразований без хранения специальных таблиц замен, позволяющих эффективно реализовать алгоритмы защиты данных [6; 27; 47; 68]. Для этого необходимо представить все преобразования с использованием логических операций, что без дополнительных оптимизаций приводит к высокому времени работы алгоритмов защиты данных.

В работе [9] был предложен новый подход к таким оптимизациям, заключающийся в том, что вместо выполнения операций над одним аргументом за счёт использования регистров вычислительного устройства возможно параллельное вычисление значений функции защиты конфиденциальности данных. При этом, чем больше длина регистра вычислительного устройства, тем выше производительность такой реализации. В литературе такой способ носит название bitslice-реализации и в настоящее время активно применяется для вычисления значений алгоритмов защиты конфиденциальности данных, [7; 65], что гарантирует невозможность применения методов анализа по времени выполнения как в случае использования в качестве вычислительного устройства как центрального процессора, так и графического вычислителя, [58].

Эффективность bitslice-реализации напрямую зависит от количества логических операций, необходимых для вычисления значения нелинейного преобразования. Таким образом, для возможности использования bitslice-реализаций алгоритмов обеспечения конфиденциальности данных, необходимо, чтобы нели-

нейные преобразования были «легко реализуемыми», что говорит о том, что к ним предъявляются требования аналогичные требованиям к низкоресурсным нелинейным преобразованиям, [53]. При этом, при синтезе подстановок для низкоресурсных устройств используются либо подстановки малой размерности (пространств $\mathbb{F}_2^4$, $\mathbb{F}_2^5$) априори легче реализуемые, чем подстановки больших размерностей, либо нелинейные биективные преобразования которые представляются композицией функций с аргументами меньшей размерности, [14; 17; 59]. В настоящее время существуют три основных универсальных подхода к построению реализаций нелинейных биективных преобразований в виде логических элементов: полный поиск с использованием обхода графа в глубину и использованием метода встречи посередине ([38; 74; 80]), эвристические методы ([35; 38; 67; 85]) и использование алгебраически задаваемых подстановок (в частности, подстановок обращения ненулевых элементов поля), [59].

В то же время при синтезе алгоритмов обеспечения конфиденциальности данных необходимо использовать нелинейные преобразования, позволяющие противостоять известным методам анализа. Эффективность применения линейного [34; 43; 55], разностного [10; 34] и некоторых типов алгебраических методов анализа [21; 37; 64; 72] напрямую зависит от показателей нелинейности используемых в алгоритме подстановок [18] и называемых криптографическими характеристиками подстановок:

– нелинейность;
– показатель дифференциальной δ-равномерности;
– алгебраические степени прямого и обратного преобразований;
– значение графовой алгебраической иммунности.

Значение показателей нелинейности подстановок малой размерности хорошо изучено, однако они далеки от аналогичных значений даже для случайных подстановок больших размерностей. Таким образом, их использование при синтезе перспективных алгоритмов защиты конфиденциальности данных, требует реализации большего количества подстановок при сохранении одинакового уровня безопасности.

Ввиду вышесказанного, имеется большое количество причин построения подстановок большей размерности с использованием функций, определенных над пространствами меньшей размерности:

– имеется возможность программной реализации с таблицами замен,

- возможна программная реализация преобразования с небольшим количеством логических преобразований,
- имеется возможность использования подстановок для реализации низкоресурсных алгоритмов,
- имеется возможность эффективного аппаратного маскирования [14; 48].

Известно большое количество способов построения таких нелинейных преобразований: на основе сети Фейстеля [17; 31; 51], с использованием конструкции типа Misty [17; 32; 54], SPN-сети [50; 66; 71] или других конструкций [70]. В тоже время для нелинейных биективных преобразований перечисленных выше, показатели нелинейности, как правило, не выше аналогичных, полученных случайным поиском.

Таким образом, актуальной задачей является построение нелинейных биективных преобразований, представимых с использованием функций от аргументов меньшей размерности, показатели нелинейности которых будут лучше аналогичных, полученных случайным поиском. Одним из таких способов основан на использовании конструкции типа «бабочка», которая была предложена в [63] в ходе исследования возможности декомпозиции известной 6-ти битовой дифференциально 2-равномерной подстановки [15] и способа построения декомпозиции для нелинейного преобразования Российских криптографических стандартов [11].

Конструктивные особенности подстановок, задаваемых конструкцией типа «бабочка» могут оказать влияние на безопасность алгоритма обеспечения конфиденциальности данных. Согласно п. 27 Доктрины информационной безопасности Российской Федерации [3] при синтезе алгоритмов защиты информации необходимо на этапе разработки гарантировать невозможность проведения различных методов анализа, что говорит об актуальности исследования влияния свойств предложенных нелинейных биективных преобразований на безопасность алгоритма в целом.

Целью данной работы является совершенствование алгоритмических методов защиты информации, при их функционировании в недоверенной среде, посредством разработки новых принципов построения нелинейных биективных преобразований.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Оценка уровня безопасности алгоритмов обеспечения конфиденциальности данных при их реализации на гетерогенных платформах, позволяющих нарушителю получать информацию о времени выполнения операций.
2. Разработка новых способов построения нелинейных биективных преобразований, использование которых уменьшает эффективность применения известных и представленных в данном диссертационном исследовании методов анализа. Оценка основных криптографических характеристик предложенных нелинейных биективных преобразований.
3. Разработка новых методов анализа, основанных на свойствах предлагаемых нелинейных биективных преобразований.

Научная новизна:

1. Предложен новый метод анализа алгоритмов обеспечения конфиденциальности данных, реализованных на графических сопроцессорах, с использованием информации о времени выполнения операций.
2. Предложены новые классы нелинейных биективных преобразований, а также разработаны алгоритмы их построения.
3. Предложен новый метод анализа XSL-сетей, основанный на поиске инвариантов их преобразования.

Теоретическая значимость данного диссертационного исследования заключается в развитии математических методов и моделей, используемых при синтезе и анализе алгоритмов обеспечения конфиденциальности данных, в том числе при их реализации в недоверенных средах.

Предложен метод анализа алгоритмов обеспечения конфиденциальности данных, реализованных на графических вычислителях, с использованием информации о времени выполнения операций. Показано, что не смотря на высокую сложность и отсутствие опубликованных данных об архитектурных особенностях платформы графических вычислителей, возможно предложить метод анализа, позволяющий последовательно восстановить неизвестные нарушителю параметры алгоритма обеспечения конфиденциальности данных специального вида.

С использованием аппарата дискретных функций, а также теории конечных полей предложенны новые семейства нелинейных биективных преобразований, а также алгоритмы их построения, получены оценки на показатели их нелинейно-

сти. Разработанный математический аппарат позволяет гарантировать свойства для достачтоно широкого семества нелинейных биективных преобразований.

Предложен новый подход к построению инвариантов преобразований алгоритмов обеспечения конфиденциальности данных, имеющих структуру XSL-сети, с использованием аппарата теории графов и линейной алгебры. С его использованием возможно получать оценки стойкости для современных и перспективных алгоритмов обеспечения конфиденциальности данных или гарантировать невозможность применения такого метода анализа.

Практическая значимость данного диссертационного исследования заключается в следующем:

1. Новый метод анализа показал низкую безопасность алгоритма AES при его реализации в недоверенной среде на графических вычислителях с использованием предвычисленных таблиц, что подтверждается независимыми исследованиями [19; 58]. Показано, что для стандартизированного в РФ алгоритма шифрования Кузнечик [2], применение указанного метода не эффективно.
2. Новые семейства нелинейных биективных преобразований, позволяют их использовать при синтезе перспективных алгоритмов защиты конфиденциальности данных.
3. Уровень безопасности стандартизованного в РФ алгоритма шифрования Кузнечик [2] не снижается относительно разработанного в диссертационном исследовании метода анализа, основанного на поиске инвариантов преобразований.
4. Полученные в диссертационном исследовании результаты могут использоваться в учебном процессе при подготовке учебных материалов и лекционных курсов.

В рамках диссертационного исследования применяются математический аппарат и подходы различных разделов математики, таких как дискретная математика, теория конечных полей, теория графов, теория алгоритмов, а также экспериментальные исследования предлагаемых примитивов и алгоритмов.

Основные результаты, выносимые на защиту:

1. Метод анализа алгоритмов обеспечения конфиденциальности данных специального вида, реализованного на графических вычислителях, по информации о времени выполнения операций.

2. Новые параметрические семейства подстановок и оценка их криптографических характеристик: нелинейность (nonlinearity), алгебраическая степень (algebraic degree), дифференциальная δ-равномерность (differential δ-uniformity).
3. Метод анализа, основанный на поиске инвариантов преобразований, используемых в алгоритмах обеспечения конфиденциальности данных, построенных на основе XSL-сети.

Достоверность полученных результатов подтверждается корректностью постановки задачи и применяемых методов исследования, обеспечивается строгими математическими доказательствами утверждений и подтверждается их согласованностью с результатами экспериментальных исследований. Помимо этого, результаты, полученные в рамках данного диссертационного исследования, находятся в соответствии с результатами, полученными другими авторами:

– В работах [19; 58] указывается, что предложенный в данном диссертационном исследовании метод анализа алгоритмов обеспечения конфиденциальности данных специального вида, реализованного на графических вычислителях, по информации о времени выполнения операций, применим при практической реализации облачных вычислений.
– Позже в работах зарубежных авторов также исследовался вопрос использования времени выполнения операций при реализации алгоритмов обеспечения конфиденциальности данных, однако с использованием иного подхода (см. напр. [29; 39—41]).
– Независимо автором [22; 23] были получены нелинейные биективные преобразования, аналогичные одному параметрическому семейству подстановок, представленному в диссертации, и имеющие такие же показатели нелинейности.
– Экспериментальные исследования предложенных автором нелинейных биективных преобразований независимо исследовались в работах [28; 77].
– В работе [76], в частности показано,что раундовые преобразования алгоритма Кузнечик не имеют нелинейных инвариантов специального вида, что не противоречит результатам, полученным автором.

Апробация работы. Основные результаты диссертационного исследования были представлены на следующих международных и всероссийских конференциях, а также на научно-исследовательских семинарах:

– 2023, XII симпозиум «Современные тенденции в криптографии» CTCrypt 2023 (Волгоград), 6-9 июня 2023 г., доклад: «Сложность вычисления некоторых подстановок, имеющих TU-представление».
– 2023, XII симпозиум «Современные тенденции в криптографии» CTCrypt 2023 (Волгоград), 6-9 июня 2023 г., доклад: «О способе построения подстановок, имеющих TU-представление».
– 2021, семинар Научного руководителя Московский институт электроники и математики им. А.М. Тихонова Национального исследовательского университета «Высшая школа экономики» (Москва), 16 декабря 2021 г., доклад: «Построение нелинейных биективных преобразований для построения алгоритмов защиты конфиденциальности данных в недоверенных средах».
– 2021, семинар «Криптография и криптоанализ» Криптографического Центра на базе Института Математики им. С.Л.Соболева, Международного математического Центра в Академгородке, Факультета информационных технологий и Новосибирского государственного университета, 14 сентября 2021 г., доклад: «Использование TU-представления для синтеза нелинейных биективных преобразований».
– 2021, XXIII научно-практическая конференция «РусКрипто'2021» (Солнечногорск), 23-26 марта 2021 г., доклад: «Стойкость алгоритма Кузнечик к обобщенной инвариантной атаке».
– 2021, X симпозиум «Современные тенденции в криптографии» CTCrypt 2021 (Московская область, Руза), 1-4 июня 2021 г., доклад: «On Differential Uniformity of Permutations Derived Using a Generalized Construction».
– 2021, X симпозиум «Современные тенденции в криптографии» CTCrypt 2021 (Московская область, Руза), 1-4 июня 2021 г., доклад: «On the Impossibility of an Invariant Attack on Kuznyechik».
– 2021, 20-я Международная конференция «Сибирская научная школа-семинар "Компьютерная безопасность и криптография"» — SIBECRYPT'21 имени Г.П. Агибалова (Новосибирск), 6-11 сентября 2021 г., доклад: «О способе построения дифференциально 2δ-равномерных подстановок на $F_{2^{2m}}$».
– 2021, 20-я Международная конференция «Сибирская научная школа-семинар "Компьютерная безопасность и криптография"» —

SIBECRYPT'21 имени Г.П. Агибалова (Новосибирск), 6-11 сентября 2021 г., доклад: «Об эвристическом подходе к построению биективных векторных булевых функций с заданными криптографическими характеристиками».

- 2020, IX симпозиум «Современные тенденции в криптографии» CTCrypt 2020 (Московская область, Руза), 15-17 сентября 2020 г., доклад: «A compact bit-sliced representation of Kuznechik S-box».
- 2019, VIII симпозиум «Современные тенденции в криптографии» CTCrypt 2019 (Светлогорск), 3-7 июня 2019 г., доклад: «On the Way of Constructing $2n$-Bit Permutations from n-Bit Ones».
- 2019, 18 всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» SIBECRYPT'19 (Томск), 9-14 сентября, доклад: «Об аппаратной реализации одного класса байтовых подстановок».
- 2018, VII симпозиум «Современные тенденции в криптографии» CTCrypt 2018 (Суздаль), 28-30 мая 2018 г., доклад: «New classes of 8-bit permutations based on a butterfly structure».
- 2018, XIX Всероссийский Симпозиум по прикладной и промышленной математике (осенняя сессия) (Сочи), 22-30 сентября 2018 г., доклад: «О подходах к построению низкоресурсных нелинейных преобразований».
- 2015, IV симпозиум «Современные тенденции в криптографии» CTCrypt 2015 (Казань), 3-5 июня 2015 г., доклад: «A timing attack on CUDA implementations of an AES-type block cipher».

Содержание работы. Результаты диссертационного исследования условно можно разделить на следующие разделы:

1. Оценка возможности использования информации о времени выполнения операций для нарушения свойств безопасности информации, алгоритмы защиты которых реализованы на графических вычислителях.
2. Выбор примитивов для построения нелинейного биективного преобразования, позволяющих гарантировать эффективность программной и аппаратной реализации.
3. Построение параметрических семейств подстановок и оценка их показателей нелинейности.

4. Оценка влияния конструктивных особенностей предлагаемых параметрических семейств подстановок на безопасность алгоритмов защиты конфиденциальности данных.

Изложим основные результаты диссертационного исследования. Для начала введем необходимые обозначения.

Полем из двух элементов будем называть множество $\mathbb{F}_2 = \{0,1\}$ с заданными естественным образом операциями сложения «$+$» и умножения «$\cdot$». Пусть $(\mathbb{F}_2^n, +) = \left\{(a_0, a_1, \ldots, a_{n-1}), a_i \in \mathbb{F}_2, i \in \overline{0,n-1}\right\}$ — арифметическое векторное пространство размерности n, $\theta = (0,0,\ldots,0)$ — ноль векторного пространства. Если рассмотреть аддитивную группу векторного пространства $(\mathbb{F}_2^n, \oplus)$ и задать специальным образом операцию умножения, то можно построить поле, которое будем обозначать $(\mathbb{F}_{2^n}, +, \cdot)$.

Первая глава диссертационного исследования посвящена изучению принципиальной возможности нарушителя по восстановлению неизвестных данных с использованием информации из побочных каналов утечки при реализации алгоритмов защиты данных на графических вычислителях.

Исторически первым опубликованным методом анализа, использующим информацию из побочных каналов утечки является восстановление ключевой информации алгоритмов защиты данных с открытым ключом [44] по времени их работы на центральном процессоре. С развитием науки появились новые методы анализа с использованием информации из разнообразных источников утечки информации: сигналы в канале питания, сигналы от электромагнитного излучения, информация о температуре или звуках, издаваемых устройством [46; 75].

До 2015 года не было известно методов анализа алгоритмов защиты информации, реализованных на графических вычислителях, по информации из побочных каналов утечки. На конференции CTCrypt'15 впервые был представлен такой метод анализа, где в качестве побочного канала утечки информации использовалась информация о времени выполнения алгоритма защиты конфиденциальности данных. Позже, в октябре 2015 года, на конференции ICCD'15, зарубежными авторами была представлена работа, [69], где предлагался метод анализа с использованием информации, получаемой из цепи питания графического вычислителя.

Первый раздел посвящен описанию представленного на CTCrypt'15 и позже опубликованного в [81] метода анализа. В качестве предмета исследования в пер-

вом разделе была выбрана реализация алгоритма защиты конфиденциальности данных, реализованного на графическом вычислителе с использованием наиболее эффективного подхода, основанного на использовании предвычисленных таблиц, [27; 36; 42]. В качестве объекта исследования — алгоритм обеспечения конфиденциальности данных, построенный на основе XSL-сети. В рамках данного раздела будем считать, что n — размер блока в битах, m — число нелинейных биективных преобразований (подстановок) на подвекторах длины n', $n = n' \cdot m$.

При реализации алгоритмов из предлагаемого семейства используются следующие преобразования:

- Наложение неизвестного нарушителю параметра, называемого раундовым ключом: $\mathrm{X}[K]\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, где $\mathrm{X}[K](a) = K \oplus a;\ a,K \in \mathbb{F}_2^n$.
- Нелинейное преобразование, представляющее собой параллельное применение подстановок пространства $\mathbb{F}_2^{n'}$: $\mathrm{S}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\mathrm{S}(a) = \mathrm{S}(a_1,\ldots,a_s) = (\pi(a_1),\ldots,\pi(a_m))$, $a_i \in \mathbb{F}_2^{n'}$, $\pi \in S\left(\mathbb{F}_2^{n'}\right)$, $i = 1,\ldots,m$.
- Линейное преобразование: $\mathrm{L}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\mathrm{L}(a) = a \cdot L'$, где $L' \in \mathrm{GL}_n$.

При реализации алгоритма обеспечения конфиденциальности данных происходит итеративное применение описанных выше операций, при этом каждая итерация называется раундом.

В случае, когда m является квадратом некоторого натурального числа $m = k^2$, можно считать, что преобразования алгоритмов из предлагаемого семейства выполняются над элементами $k \times k$ матрицы:

$$\begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,k-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,k-1} \\ \cdots & \cdots & \cdots & x_{k-1,k-1} \\ x_{k-1,0} & x_{k-1,1} & \cdots & x_{k-1,k-1} \end{pmatrix},$$

$x_{i,j} \in \mathbb{F}_2^{n'}$, $i,j = \{0,1,\ldots,k-1\}$. В этом случае линейное преобразование может задаваться композицией двух преобразований: умножение некоторой обратимой матрицы на каждый из столбцов матрицы и перестановкой элементов матрицы таким образом, что в каждой строке и в каждом столбце получившейся матрицы оказался элемент каждого из k столбцов исходной матрицы. Такие линейные преобразования будем называть преобразованиями A-типа. В алгоритме шифрования AES, [24] и функции хэширования ГОСТ 34.11-2018 [1] используются линейные преобразования A-типа. В рамках данного раздела промежуточное значение, получаемое после i-ой итерации рассматриваемого алгоритма шифрования, будем

обозначать

$$x^{(i)} = \begin{pmatrix} x^{(i)}_{0,0} & x^{(i)}_{0,1} & \cdots & x^{(i)}_{0,k-1} \\ x^{(i)}_{1,0} & x^{(i)}_{1,1} & \cdots & x^{(i)}_{1,k-1} \\ \cdots & \cdots & \cdots & x^{(i)}_{k-1,k-1} \\ x^{(i)}_{k-1,0} & x^{(i)}_{k-1,1} & \cdots & x^{(i)}_{k-1,k-1} \end{pmatrix},$$

$x^{(i)}_{i,j} \in \mathbb{F}_2^{n'}, i,j = \{0,1,\ldots,k-1\}$, а $x^{(0)}$ — открытый текст. Для удобства изложения будем использовать обозначение $x^{(i)}[j,k]$ для величины $x^{(i)}_{j,k}$, $j,k = \{0,1,\ldots,k-1\}$.

Верно следующее

Утверждение 1. *[81] Для алгоритма защиты конфиденциальности данных с линейным преобразованием A-типа произвольное значение $x^{(2)}_{i,j}$, $i,j \in \{1,\ldots,k-1\}$, после первого раунда определяется ровно k значениями на первом раунде преобразований и для того, чтобы фиксировать значение $x^{(2)}_{i,j}$ константой существует $2^{n' \cdot k-1}$ способов выбрать эти k значений после выполнения операции* X *на первом раунде алгоритма.*

Рассмотрим алгоритм AES, для которого $k = 4$. Обозначим значение, получаемое после наложения ключа в первом раунде матрицей:

$$\begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \\ x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} \end{pmatrix},$$

$x_{i,j} \in \mathbb{F}_2^8$, $i,j = \{0,1,\ldots,3\}$. Согласно утверждению 1 существует 2^{24} способов задания значения $x^{(2)}_{i,0}$ некоторой константой для произвольного $i \in \{0,\ldots,3\}$, задав значения $x_{0,0}, x_{1,1}, x_{2,2}, x_{3,3}$ специальным образом. Кроме этого:

возможно задать константой:	задав специальным образом:
$\left\{x^{(2)}_{i,0}, i = 0,\ldots,3\right\}$	$\{x_{0,0}, x_{1,1}, x_{2,2}, x_{3,3}\}$
$\left\{x^{(2)}_{i,1}, i = 0,\ldots,3\right\}$	$\{x_{0,1}, x_{1,2}, x_{2,3}, x_{3,0}\}$
$\left\{x^{(2)}_{i,2}, i = 0,\ldots,3\right\}$	$\{x_{0,2}, x_{1,3}, x_{2,0}, x_{3,1}\}$
$\left\{x^{(2)}_{i,3}, i = 0,\ldots,3\right\}$	$\{x_{0,3}, x_{1,0}, x_{2,1}, x_{3,2}\}$

и возможно это сделать 2^{24} способами.

Для восстановления ключа на первом раунде применяется следующее свойство разделяемой памяти, используемой для хранения таблиц замены: обращение в память происходит одновременно 32 потоками, все ячейки памяти разделены на

32 банка, скорость обращения к которым прямо пропорционально максимальному количеству обращений к одному и тому же банку памяти. При этом, скорость обращения в память будет минимальной, когда все потоки обращаются к одному и тому же участку памяти или ни одна пара потоков не обращаются к одному и тому же участку памяти, [60]. Используя это свойство можно восстановить все k значений ключа, имеющих длину $n' \cdot k$. Таким образом, $2^{n' \cdot k}$ различными способами выбирая материал, подаваемый на вход алгоритму защиты конфиденциальности данных можно определить момент, когда скорость реализации была минимальна, что позволяет восстанавливать ключ первого раунда. Аналогичным образом возможно восстановить и остальные раундовые ключи. В качестве иллюстрации опишем способ восстановления первого раундового ключа

$$K = \begin{pmatrix} k_{0,0}^{(1)} & k_{0,1}^{(1)} & k_{0,2}^{(1)} & k_{0,3}^{(1)} \\ k_{1,0}^{(1)} & k_{1,1}^{(1)} & k_{1,2}^{(1)} & k_{1,3}^{(1)} \\ k_{2,0}^{(1)} & k_{2,1}^{(1)} & k_{2,2}^{(1)} & k_{2,3}^{(1)} \\ k_{3,0}^{(1)} & k_{3,1}^{(1)} & k_{3,2}^{(1)} & k_{3,3}^{(1)} \end{pmatrix}$$

алгоритма AES (см. алгоритм 1). Реализацию x случайной величины, имеющей равномерное распределение на множестве D будем обозначать через: $x \xleftarrow{U} W$, функцию, вычисляющую время реализации процедуры шифрования алгоритмом E_K данных $D_1, D_2, \ldots, D_M$ будем обозначать через time $(E_K, \{D_1, D_2, \ldots, D_M\})$. При описании алгоритма также будет использоваться операция целочисленного деления «\».

Значения $k_{0,0}^1$,$k_{1,1}^1$,$k_{2,2}^1$,$k_{3,3}^1$ однозначно определяются по значению, выдаваемому алгоритмом 1. Аналогично восстанавливаются значение всего ключа первого раунда.

Таким образом, трудоемкость восстановления ключа рассматриваемого алгоритма равняется $2^{n'k}$ операций вычисления значений специального вида. Параметр M алгоритма 1 выбирается экспериментально. В работе [81] приведены данные и графики, показывающие практическую возможность применения предложенного метода анализа.

Таким образом показано, что использование предвычисленных таблиц замены для реализации алгоритмов конфиденциальности данных, потенциально позволяет нарушителю восстанавливать неизвестные ему параметры. Более того, для реализации методов анализа по побочным каналам утечки, зачастую иссле-

Алгоритм 1: Восстановление значений $k^1_{0,0}$,$k^1_{1,1}$,$k^1_{2,2}$,$k^1_{3,3}$ ключа алгоритма AES

Входные данные: Черный ящик E_K, реализующий алгоритм шифрования AES, M — параметр метода

цикл $i = 1$ **до** M **выполнять**

  цикл $j = 0$ **до** 3 **выполнять**

    цикл $k = 0$ **до** 3 **выполнять**

      $x_{j,k} \xleftarrow{U} \mathbb{F}_2^8$

  $$D_i \leftarrow \begin{pmatrix} 0 & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \\ x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} \end{pmatrix} \cdot L^{-1}$$

$T_0 = \text{time}\,(E_K, \{D_1, D_2, \ldots, D_M\})$

цикл $n = 1$ **до** $2^{32} - 1$ **выполнять**

  цикл $i = 1$ **до** M **выполнять**

    цикл $j = 0$ **до** 3 **выполнять**

      $D_i[j,j] \leftarrow D_i[j,j] \oplus \left(\left((n \oplus (n-1)) \setminus 2^{8 \cdot j}\right) \pmod{2^8}\right)$

  $T_n = \text{time}\,(E_K, \{D_1, D_2, \ldots, D_M\})$

Результат: $\underset{n \in \{0,1,\ldots,2^{32}-1\}}{\arg\min} \; T_n$

дуется операция обращения в память, так как она считается одной из самых информативных для нарушителя, [26; 29; 33; 52; 69].

Из вышесказанного следует, что для защиты от рассмотренного метода и ряда других методов анализа необходимо использовать реализацию преобразований, для которой отсутствует необходимость обращения в память, то есть с использованием только логических операций (напр. bitslice-реализацию). Однако это может привести к низкой скорости реализации алгоритмов защиты конфиденциальности данных. Таким образом, необходимо выбрать конструкцию нелинейного биективного преобразования с гарантированным наличием эффективной реализации.

Вторая глава диссертационного исследования посвящена выбору примитивов для построения нелинейного биективного преобразования, позволяющих гарантировать эффективность программной и аппаратной реализации.

В 2016 году группой авторов проводилось исследования возможностей представления некоторых подстановок, имеющие «хорошие» показатели

нелинейности с использованием функций, определенных над пространствами меньшей размерности. В результате исследования был предложен подход к построению подстановок на основе так называемого TU-представления [12; 62], которое в некотором смысле можно считать обобщением двухраундовой сети Фейстеля. Подстановки построенные по данному принципу далее будут называться F-конструкциями (Feistel-like constructions). Нелинейное биективное преобразование, используемое в отечественных стандартизированных алгоритмах, а также подстановка, CCZ-эквивалентная единственно известной дифференциально 2-равномерной подстановке пространств вида $\mathbb{F}_2^{2m}$, имеют TU-представление, [12; 62; 63].

В настоящее время наиболее перспективным с точки зрения реализации алгоритмов защиты конфиденциальности данных является использование преобразований из симметрической группы $S\left(\mathbb{F}_2^8\right)$, обладающих «хорошими» показателями нелинейности. Нелинейное биективное преобразование алгоритма Кузнечик представимо в виде композиции следующих функций (см. рис. 1): функции $\mathbb{F}_2^4 \to \mathbb{F}_2^4$, подстановок из симметрической группы $S\left(\mathbb{F}_2^4\right)$, умножения в поле $\mathbb{F}_{2^4}$, мультиплексора (условного оператора), линейных функций GL_8.

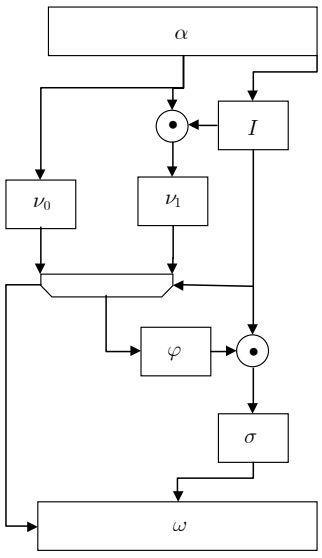

Рисунок 1 — Представление подстановки алгоритма Кузнечик [12]

Рассмотрим способ определения трудоемкости каждой из этих функций. В работе [74] проведен поиск и построены все подстановки пространства $\mathbb{F}_2^4$, реализуемые менее чем за 12 логических операций, а также операции копирования «MOV». Это составляет порядка 90% всех подстановок, найдены эффективно реализуемые представители для 271 из 302 классов аффинной эквивалентности. Была

построена 4-равномерная подстановка, которая может быть реализована только 9 операциями, имеет нелинейность, равную 4, и алгебраическую степень, равную 2. В работе [74] были построены не все 4-х битовые подстановки, и в настоящее время остается открытым вопрос о минимальном представлении достаточно широкого класса подстановок. Среди 16 классов аффинной эквивалентности, имеющих показатель дифференциальной равномерности и нелинейность равные 4, только для 7 классов были найдены эффективно реализуемые представители (от 9 до 13 операций «AND», «OR», «XOR», «NOT», «MOV»).

В работе [20] автором исследуется иной базис, состоящий только из операций «AND» и «XOR». Отказ от операции «MOV» был связан с тем, что авторы ориентируются в первую очередь на аппаратную реализацию, где операция копирования не требует наличия дополнительных ресурсов. Ограничение базисных операций до «AND» и «XOR» связан с тем, что использование только этих операций облегчает создание так называемой «пороговой» реализации подстановок, что позволяет противодействовать методам, использующим информацию из побочных каналов утечки. Отечественными специалистами в работе [80] представлены результаты исследования, посвященные поиску подстановок пространства $\mathbb{F}_2^4$, реализуемых в базисе «AND» и «XOR» более, чем за 11 инструкций. Для ряда подстановок, для которых в работе [74] не были найдены эффективно реализуемые представители, авторами [80] даются оценки числа используемых инструкций. Стоит отметить, что в целом, не совсем корректно сравнивать результаты работы [74] и [80] в виду различия в базисе. Для еще 7 классов из 16, имеющих показатель дифференциальной и нелинейность равные 4, были найдены эффективно реализуемые представители (но уже в базисе «AND» и «XOR»).

Отдельно стоит отметить, что мономиальные подстановки пространства $\mathbb{F}_2^4$ являются либо линейными (трудоемкость их реализации легко определить), либо являются линейно эквивалентными подстановке обращения ненулевых элементов, реализация которой хорошо исследовалась, [57; 61; 73].

В общем же случае, поиск эффективной реализации конкретной функции или подстановки $\mathbb{F}_2^4 \to \mathbb{F}_2^4$ является достаточно трудоемкой задачей, [16]. В связи с этим, зачастую при решении данной задачи используются различные эвристические алгоритмы. Наиболее известными алгоритмами являются ESPRESSO [67] и BOOM [35], которые внедрены в большое количество коммерческих пакетов. Оте-

чественные авторы представили свой аналог, который использовался при поиске минимального представления подстановки алгоритма Кузнечик в работе [85].

Умножение в поле очевидным образом является квадратичной формой и эффективно реализуется, [85]. Отдельно необходимо рассмотреть трудоемкость реализации мультиплексора. Согласно [12] происходят следующие вычисления: «Если $r = \theta$ тогда $l = \nu_0(l)$ иначе $l = \nu_1(l \cdot I(r))$», где ν_0, ν_1, I — нелинейные биективные функции пространства $\mathbb{F}_2^4$. Рассмотрим функцию индикатор, принимающую значение равное 1 в точке $r = \theta$ и нулевое значение во всех остальных точках:

$$\mathrm{Ind}_\theta(r) = \bar{r}_1 \cdot \bar{r}_2 \cdot \bar{r}_3 \cdot \bar{r}_4 = \overline{r_1 + r_2 + r_3 + r_4}.$$

Она реализуется за 4 логические операции, ее отрицание — за 3. Тогда вычисления значения l происходят по формуле:

$$l = \mathrm{Ind}_\theta(r) \cdot \nu_0(l) + \overline{\mathrm{Ind}_\theta(r)} \cdot \nu_1(l \cdot I(r)).$$

Вычисление данной функции можно упростить следующим образом:

$$l = \mathrm{Ind}_\theta(r) \cdot (\nu_0(l) \oplus \nu_1(\theta)) \oplus \nu_1(l \cdot I(r))$$

так как I является мономиальной подстановкой. Очевидно, что реализация тем эффективнее, чем меньше вес значения $\nu_1(\theta)$.

Таким образом, в качестве примитивов для построения подстановки пространства $\mathbb{F}_2^8$ будем выбирать подстановки пространства $\mathbb{F}_2^4$, а также операцию умножения в поле $\mathbb{F}_{2^4}$ и мультиплексор. При этом желательно, чтобы подстановки пространства $\mathbb{F}_2^4$ были либо мономиальные, либо имели неподвижную точку в нуле, или являлись линейными. Очевидно, что меньшее количество используемых нелинейных преобразований приводит в повышению эффективности реализации.

Подстановки, рассматриваемые далее при разных значениях параметров реализуются с использованием от 2 до 6 подстановок пространства $\mathbb{F}_2^4$. При этом, наиболее эффективно реализуемой подстановкой $F(x_1, x_2) = (y_1, y_2)$ (с точки зрения количества используемых нелинейных преобразований) является биективная функция, определяемая следующими формулами:

1. $x' = x^{-1}$
2. $y' = y^{-1}$
3. $x'' = x \cdot y'$
4. $y'' = x' \cdot y'$

5. если $x = \theta$ тогда $y_1 = y'$ иначе $y_1 = y''$
6. если $x = y$ тогда $y_2 = x'$ иначе $y_2 = x''$

Кроме этого, результаты работы [88] показывают эффективность реализации определяемых в диссертационном исследовании нелинейных биективных преобразований на аппаратных платформах.

Третья глава диссертационного исследования посвящена построению нелинейных биективных преобразований и оценке их показателей нелинейности. Опишем основные криптографические характеристики нелинейных биективных преобразований, используемые при анализе симметричных криптографических алгоритмов, [18].

Определение 1. *Векторной булевой функцией (или (n,m)-функцией) S называется отображение $\mathbb{F}_2^n \to \mathbb{F}_2^m$, $n,m \in \mathbb{N}$.*

Определение 2. *Значение преобразования Уолша-Адамара (WHT) $W_S(a,b)$ (n,m)-функции S для значений $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$ определяется следующим равенством:*

$$W_S^{a,b} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle a,x \rangle + \langle b,S(x) \rangle}.$$

Определение 3. *Нелинейность (n,m)-функции S обозначается N_S и определяется следующим образом:*

$$N_S = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n, \\ b \in \mathbb{F}_2^m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Линейность L_S (n,m)-функции S определяется следующим образом:

$$L_S = \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n, \\ b \in \mathbb{F}_2^m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Нелинейность (n,m)-функции характеризует ее удаленность от множества линейных функций той же размерности [18]. Использование в алгоритме обеспечения конфиденциальности данных функции с высокой нелинейностью увеличивает его стойкость к линейному методу анализа [34; 43; 55; 78; 79]. При этом существуют векторные булевы функции $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n,m \in \mathbb{N}$, $m \leqslant n/2$, которые максимально удалены от множества всех линейных функций и называются бент-функциями. Их нелинейность равна $2^{n-1} - 2^{n/2-1}$.

Определение 4. *Алгебраической степенью* $\deg(S)$ (n,m)*-функции* S *называется минимальная степень многочлена Жегалкина среди всевозможных линейных комбинаций ее координатных функций* $\langle a,S(x)\rangle$ *по всевозможным* $a \in \mathbb{F}_2^m \backslash \theta$*:*

$$\deg(S) = \min_{a \in \mathbb{F}_2^m \backslash \theta} \deg\left(\langle a,S(x)\rangle\right).$$

Использование в алгоритме обеспечения конфиденциальности данных функции с высокой алгебраической степенью увеличивает его стойкость к интерполяционному и алгебраическому методам анализа, [37; 64; 72]. Известно, что при $n \geqslant 3$ сбалансированная булева функция имеет алгебраическую степень, равную $n-1$, только если она существенно зависит от всех n переменных. Таким образом, алгебраическая степень подстановки не превышает значение $n-1$, [18].

Определение 5. *Для произвольных* $a \in \mathbb{F}_2^n \backslash \theta, b \in \mathbb{F}_2^m$ *положим*

$$\delta_S^{a,b} = \left|\{x \in \mathbb{F}_{2^n} | S(x+a) + S(x) = b\}\right|.$$

Будем говорить, что S *является дифференциально* δ_S*-равномерной функцией, если*

$$\delta_S = \max_{\substack{a \in \mathbb{F}_2^n \backslash \theta, \\ b \in \mathbb{F}_2^m}} \delta_S^{a,b},$$

а значение δ_S *будем называть показателем дифференциальной равномерности функции* S*.*

Использование в алгоритме обеспечения конфиденциальности данных функции с низкой дифференциальной равномерностью увеличивает его стойкость к разностному методу анализа [10; 34; 78; 79]. Наименьшим возможным значением является 2, однако с точностью до CCZ-эквивалентности известна только одна 2-равномерная подстановка пространства $\mathbb{F}_2^m$ в случае четного m, [63].

Произвольную (n,m)-функцию F возможно задать в виде ее координатных функций: $F\left(\overline{x}\right) = \left(f_1\left(\overline{x}\right), f_2\left(\overline{x}\right), \ldots, f_m\left(\overline{x}\right)\right)$, где $\overline{x} = (x_1, x_2 \ldots, x_n) \in \mathbb{F}_2^n$, $f_i\left(\overline{x}\right)$ — булевы функции, $i \in \overline{1,m}$.

Рассмотрим следующее множество $\mathcal{G}_k$ булевых функций от $n+m$ переменных $G(x_1, \ldots, x_n, y_1, \ldots, y_m)$, таких, что $\deg(G) \leqslant k$, $k \in \mathbb{N}$ и для каждого $\overline{x} \in \mathbb{F}_2^n$ при подстановке вместо каждой переменной y_i, $i \in \overline{1,m}$, значения соответствующей булевой функции $f_i\left(\overline{x}\right)$, значение функции $G(x_1, \ldots, x_n, f_1\left(\overline{x}\right), \ldots, f_m\left(\overline{x}\right))$ равно нулю:

$$\mathcal{G}_k = \{G(x_1, \ldots, x_n, y_1, \ldots, y_m) \colon G(x_1, \ldots, x_n, f_1\left(\overline{x}\right), \ldots, f_m\left(\overline{x}\right)) = 0 \; \forall \overline{x} \in \mathbb{F}_2^n\}.$$

Множество $\mathcal{G}_k$ образует подгруппу в кольце многочленов степени не выше k. Обозначим r_F^k — максимальное число линейно независимых элементов множества $\mathcal{G}_k$.

Определение 6. *Минимальное число k такое, что $r_F^k \neq 0$, называется графовой алгебраической иммунностью F и обозначается $AI_{gr}(F)$, [18].*

В работе [21] предлагается метод алгебраического анализа, использующий низкую графовую алгебраическую иммунность нелинейного преобразования. Таким образом, использование функций с высокой алгебраической иммунностью увеличивает стойкость алгоритма обеспечения конфиденциальности данных к алгебраическим методам анализа.

При синтезе алгоритмов обеспечения конфиденциальности данных необходимо использовать подстановки, позволяющие противостоять известным методам анализа. Эффективность применения линейного [34; 43; 55; 78], разностного [10; 34; 78] и некоторых типов алгебраических методов анализа [21; 37; 64; 72] напрямую зависит от криптографических характеристик используемых в алгоритме нелинейных преобразований. Такими характеристиками (при фиксированном значении n) являются следующие:

- нелинейность подстановки;
- дифференциальная δ-равномерность подстановки;
- алгебраические степени подстановки и обратной подстановки;
- алгебраическая иммунность подстановки.

Определение 7 ([92])**.** *Пусть F_1, $F_2 \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ — произвольные $(2m,m)$-функции. Определим преобразование $F(x_1, x_2) = (y_1, y_2)$, которое будем называть F-конструкцией (см. рис. 2), следующей системой:*

$$\begin{cases} y_1 = F_1(x_1, x_2) \\ y_2 = F_2(x_2, y_1) \end{cases}. \tag{1}$$

F-конструкция является базовой для построения нелинейных биективных преобразований в данном диссертационном исследовании.

Утверждение 2 ([12; 92])**.** *Пусть $F_1, F_2 \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ такие функции, для которых при фиксации произвольного z_2 функция $F_i(z_1,z_2)$, $i \in \overline{1,2}$ является биекцией по переменной z_1. Тогда*

1) преобразование F является подстановкой на множестве $\mathbb{F}_2^m \times \mathbb{F}_2^m$,

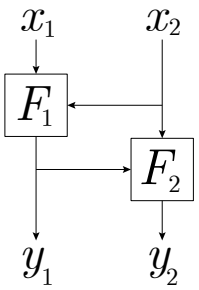

Рисунок 2 — F-конструкция

2) *общее количество подстановок* F*, которые определяются формулами* (1)*, равно* $\left(2^m!\right)^{2^{m+1}}$.

Таким образом, для задания нелинейных биективных преобразований, определяемых F-конструкцией, необходимо выбирать функции F_1, F_2, удовлетворяющие утверждению 2. Построение сбалансированных (n,m)-функций, имеющих нелинейность не ниже некоторой границы $\mathbf{N}$, является сложной задачей при больших значениях границы $\mathbf{N}$ и при $n \geqslant 8$ и $m \geqslant 4$. Одним из известных подходов является построение сбалансированных (n,m)-функций из несбалансированных (n,m)-функций, имеющих высокую нелинейность, (см. напр. [25]), который исследуется в диссертационном исследовании при выборе функций F_i, $i \in \overline{1,2}$ в формуле (1).

Пусть $s'(x,y)$ – функция $\mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ и для некоторого $\dot{y} \in \mathbb{F}_2^m$ функция $s'(x,\dot{y})$ не является подстановкой по переменной x. Тогда такую точку $\dot{y}$ будем называть выколотой точкой функции s'. Множество выколотых точек функции s' будем обозначать $\dot{Y} \subseteq \mathbb{F}_2^m$:

$$\dot{Y} = \{\dot{y}\colon\ |\{s'(x,\dot{y}), x \in \mathbb{F}_2^m\}| < 2^m\}\,.$$

В случае, когда $\dot{Y}$ не пусто, можно переопределить функцию в каждой выколотой точке $\dot{y} \in \dot{Y}$ и построить новую функцию $s(x,y)$ такую, что $s\colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ является подстановкой по переменной $x \in \mathbb{F}_2^m$ при фиксации произвольного значения $y \in \mathbb{F}_2^m$. Пусть $\widehat{\pi}_y(x)$, $y \in \dot{Y}$ — подстановки пространства $\mathbb{F}_2^m$, тогда зададим $(2m,m)$-функцию s следующим образом:

$$s(x,y) = \begin{cases} s'(x,y), & y \notin \dot{Y} \\ \widehat{\pi}_y(x), & y \in \dot{Y} \end{cases}. \tag{2}$$

Для оценки нелинейности функции $s(x,y)$ необходимо уметь вычислять коэффициенты Уолша-Адамара этой функции. Для функций $s'(x,\dot{y})$, $\dot{y} \in \dot{Y}$, как функций от одного переменного x введем обозначение $g_{\dot{y}}(x)$.

Утверждение 3 ([92]). *Пусть $s'(x,y)$ — $(2m,m)$-функция со множеством выколотых точек $\dot{Y}$, $\widehat{\pi}_{\dot{y}}$ — множество подстановок на $\mathbb{F}_2^m$, $\dot{y} \in \dot{Y}$. Определим $(2m,m)$-функцию $s(x,y)$, не имеющую выколотых точек по формуле* (2). *Пусть $\alpha, \beta, \gamma \in \mathbb{F}_2^m$, тогда коэффициенты Уолша-Адамара функции s вычисляются по следующей формуле:*

$$W_s^{\alpha\|\beta,\gamma} = \begin{cases} W_{s'}^{\alpha\|\beta,\gamma} + \sum\limits_{\dot{y}\in\dot{Y}} (-1)^{\langle\beta,\dot{y}\rangle} \left(W_{\widehat{\pi}_{\dot{y}}}^{\alpha,\gamma} - W_{g_{\dot{y}}}^{\alpha,\gamma} \right), & \alpha \neq \theta \\ W_{s'}^{\alpha\|\beta,\gamma} + \sum\limits_{\dot{y}\in\dot{Y}} (-1)^{\langle\beta,\dot{y}\rangle} \left(2 \cdot wt\left(\langle\gamma, g_{\dot{y}}(x)\rangle\right) - 2^m\right), & \alpha = \theta, \gamma \neq \theta \\ W_{s'}^{\alpha\|\beta,\gamma}, & \alpha = \theta, \gamma = \theta \end{cases}. \quad (3)$$

Можно получить следующую оценку на линейность функции s, построенной по формуле 2.

Следствие 1 ([92]). *В условиях утверждения 3 верна следующая оценка сверху на линейность L_s функции s:*

$$L_s \leqslant \max\left\{ L_{s'} + \sum_{\dot{y}\in\dot{Y}} \left(L_{\widehat{\pi}_{\dot{y}}} + L_{g_{\dot{y}}(x)}\right), L_{s'} + \sum_{\dot{y}\in\dot{Y}} \left| 2^m - 2 \cdot \min_{\gamma\in\mathbb{F}_2^m\setminus\theta} wt\left(\langle\gamma, g_{\dot{y}}(x)\rangle\right) \right| \right\}.$$

Пусть стоит задача построить функцию s с линейностью не выше некоторой границы $\mathbf{L}$. Тогда, можно искать такие функции s' и $\widehat{\pi}_y$, что верхняя граница, полученная в следствии 1, будет меньше $\mathbf{L}$. Так как каждое слагаемое в

$$\sum_{\dot{y}\in\dot{Y}} \left(L_{\widehat{\pi}_{\dot{y}}} + L_{g_{\dot{y}}(x)}\right) \text{ и } \sum_{\dot{y}\in\dot{Y}} \left|2^m - 2 \cdot wt\left(g_{\dot{y}}\left(x\right)\right)\right|$$

является неотрицательным целым числом (или даже положительным, так как для любой подстановки π ее линейность больше 0, $L_\pi > 0$), то при одном и том же значении линейности функции s' функция s, полученная по формуле (2), потенциально имеет тем большую линейность, чем больше выколотых точек у функции s'.

Действительно, пусть дана $(2m,m)$-функция s', имеющая ровно одну выколотую точку $\dot{y}$. Обозначим $g(x) = s\left(x, \dot{y}\right)$ и пусть $\widehat{\pi}$ — подстановка на $\mathbb{F}_2^m$. Определим $(2m,m)$-функцию s, не имеющую выколотых точек следующим образом:

$$s(x,y) = \begin{cases} s'(x,y), & y \neq \dot{y} \\ \widehat{\pi}(x), & y = \dot{y} \end{cases}. \quad (4)$$

Для таких функций можно получить потенциально меньшую оценку на линейность L_s.

Следствие 2 ([92]). *Пусть* s — $(2m,m)$*-функция заданая формулой* (4). *Тогда верна следующая верхняя оценка на линейность* L_s *функции* s*:*

$$L_s \leqslant \max\left\{L_{s'} + L_{\widehat{\pi}} + L_g, L_{s'} + \left|2^m - 2 \cdot \min_{\gamma \in \mathbb{F}_2^m \setminus \theta} wt\left(\langle \gamma, g(x)\rangle\right)\right|\right\}.$$

В связи со следствием 2 наибольший интерес представляют функции s', которые имеют только одну выколотую точку $\dot{y}$.

Покажем, что при дополнительных ограничениях на функцию g удается уточнить верхнюю оценку на линейность функции s. Например, когда произвольная невырожденная линейная комбинация координатных функций $g(x)$ тождественно равна 0 или 1, что эквивалентно тому, что функция $g(x)$ является константой.

Утверждение 4 ([92]). *Пусть* s' — $(2m,m)$*-функция, имеющая ровно одну выколотую точку* $\dot{y}$, $g(x) = s'(x, \dot{y})$, $\widehat{\pi}$ — *подстановка на* $\mathbb{F}_2^m$. *Определим* $(2m,m)$*-функцию* s *формулой* (4).

Тогда, если произвольная невырожденная линейная комбинация функции $g(x)$ *равна либо 0 либо 1, то коэффициенты Уолша-Адамара функции* $s(x,y)$ *для произвольных* $\alpha, \beta, \gamma \in \mathbb{F}_2^m$ *вычисляются по следующей формуле:*

$$W_s^{\alpha\|\beta,\gamma} = \begin{cases} W_{s'}^{\alpha\|\beta,\gamma} + (-1)^{\langle \beta, \dot{y}\rangle} \cdot W_{\widehat{\pi}}^{\alpha,\gamma}, & \alpha \neq \theta \\ 0, & \alpha = \theta, \gamma \neq \theta \\ W_{s'}^{\theta\|\beta,\theta}, & \alpha = \theta, \gamma = \theta \end{cases}. \tag{5}$$

Покажем, что существуют такие функции s', что произвольная невырожденная линейная комбинация координатных функций $g(x)$ тождественно равна 0 или 1 и сама функция s' имеет достаточно высокую нелинейность. Например, произвольная $(2m,m)$ бент-функция с одной выколотой точкой обладает таким свойством.

Утверждение 5 ([92]). *Пусть* $b(x,y)\colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ — *бент-функция, имеющая ровно одну выколотую точку* $\dot{y}$. *Тогда произвольная невырожденная линейная комбинация координатных функций* $g(x) = b(x,\dot{y})$ *тождественно равна 0 или 1.*

Следствие 3 ([92]). *В условиях утверждения 4 верхняя и нижняя границы на линейность* L_s *функции* s *задаются следующими неравенствами:*

$$L_{s'} - L_{\widehat{\pi}} \leqslant L_s \leqslant L_{s'} + L_{\widehat{\pi}}.$$

Если s' — векторная бент-функция, то

$$L_{s'} < L_s \leqslant L_{s'} + L_{\widehat{\pi}}.$$

В частности, следствие 3 гарантирует способ построения $(2m,m)$-функции s по формуле (4) с нелинейностью не ниже $L_s \leqslant L_{s'} + L_{\widehat{\pi}}$. В случае $m = 4$ наименьшее возможное значение $L_{\widehat{\pi}}$ равно 4. Тогда используя в качестве s' бент-функции можем получить $(8,4)$-функцию, имеющую линейность 12.

Обратно тоже верно. Пусть выбрана некоторая граница $\mathbf{L}$ и стоит задача построения $(2m,m)$-функций, имеющих линейность не выше $\mathbf{L}$. Тогда выбирая подстановки, имеющие наименьшее возможное значение $L_{\widehat{\pi}}$ и выбрав $(2m,m)$-функцию s', имеющую ровно одну выколотую точку $\dot{y}$ так, что $s'(x, \dot{y}) = \text{const}$, и линейность не выше $\mathbf{L} - L_{\widehat{\pi}}$, по следствию 3 можем построить $(2m,m)$-функцию s с линейностью не выше $\mathbf{L}$.

Приведем пример $(2m,m)$-функций s', имеющих ровно одну выколотую точку $\dot{y}$ и при этом $s'(x, \dot{y}) = \text{const}$. При этом, для рассмотренных функций в некоторых условиях доказано, что они имеют высокую нелинейность. Все эти функции можно использовать в качестве функций F_i в F-конструкции.

Пусть $n = 2m$, $x, y \in \mathbb{F}_2^m$, $m \in \mathbb{N}$. Рассмотрим следующие функции.

- $s'(x,y) = L(x \cdot \pi(y)) + G(y)$, где $\pi, L \in S(\mathbb{F}_2^m)$, G — произвольная (m,m)-функция. В случае, когда L — линейная подстановка, s' является бент-функцией Майорана-Макфараленда [18];
- $s'(x,y) = P(x,y) + G(y)$, где G — произвольная (m,m)-функция, P — $(2m,m)$-функция такая, что для любого фиксированного $x \neq 0$, $P(x,y)$ является подстановкой по y. В случае, когда при фиксации $y \in \mathbb{F}_2^m$ функция P линейна по переменной x, s' является бент-функцией, которую называют расширенной конструкцией Майорана-Макфараленда [18];
- $s'(x,y) = G\left(x \cdot y^{-1}\right)$, где G — сбалансированная $(2m,m)$-функция. Тогда s' — бент-функция, которую называют PS_{ap} бент-функция [18].
- $s'(x,y) = \pi_1(x) \cdot \pi_2(x)$, где $\pi_1, \pi_2 \in S(\mathbb{F}_2^m)$. В случае, когда хотя бы одна из подстановок π_1 или π_2 является линейной, то функция s' является частным случаем конструкции Майорана-Макфараленда.

Пусть s'_1 и s'_2 две $(2m,m)$-функции, имеющие выколотые точки $\dot{y}_1$ и $\dot{y}_2$ соответственно, $\widehat{\pi}_1$ и $\widehat{\pi}_2$ — две подстановки пространства $\mathbb{F}_2^m$. Зададим функции F_1 и F_2 согласно формуле (4) и определим подстановку $F \in S\left(\mathbb{F}_2^{2m}\right)$, $F(x_1, x_2) = (y_1, y_2)$,

с помощью F-конструкции по формуле (1):

$$y_1 = F_1(x_1,x_2) = \begin{cases} s'_1(x_1,x_2), & x_2 \neq \dot{y}_1 \\ \widehat{\pi}_1(x_1), & x_2 = \dot{y}_1 \end{cases}, \tag{6}$$

$$y_2 = F_2(x_2,y_1) = \begin{cases} s'_2(x_2,y_1), & y_1 \neq \dot{y}_2 \\ \widehat{\pi}_2(x_2), & y_1 = \dot{y}_2 \end{cases}. \tag{7}$$

Согласно используемым предположениям при фиксации произвольного $x_2 \neq \dot{y}_i$, функция $s'_i(x_1,x_2)$ (для произвольного $i \in \overline{1,2}$) является биекцией по переменной x_1. Тогда для $x_2 \neq \dot{y}_i$ корректно определены биективные отображения $s'^{-1}_i(y,x_2)$ как функции от одной переменной y при фиксированном $x_2 \neq \dot{y}_i$. Аналогично корректно определены функции $F_i^{-1}(y,x_2)$ как подстановки по переменной y при фиксированном значении $x_2 \in \mathbb{F}_2^m$.

Выпишем выражение для подстановки $F^{-1}(y_1,y_2) = (x_1,x_2)$ обратной к F, задаваемой по формулам (6)–(7):

$$x_2 = F_2^{-1}(y_1,y_2) = \begin{cases} s'^{-1}_2(y_2,y_1), & y_1 \neq \dot{y}_2 \\ \widehat{\pi}_2^{-1}(y_2), & y_1 = \dot{y}_2 \end{cases}, \tag{8}$$

$$x_1 = F_1^{-1}(y_1,x_2) = \begin{cases} s'^{-1}_1(y_1,x_2), & x_2 \neq \dot{y}_1 \\ \widehat{\pi}_1^{-1}(y_1), & x_2 = \dot{y}_1 \end{cases}. \tag{9}$$

При этом F_2^{-1}, как и F_1^{-1}, являются функциями с одной выколотой точкой вида (4), а значения y_2 и x_1 не выражаются напрямую через x_1,x_2 и y_1,y_2 соответственно. Например y_2 выражается через x_1 и x_2 из (7) достаточно громоздкой формулой:

$$y_2 = \begin{cases} s'_2(x_2,s'_1(x_1,x_2)), & x_2 \neq \dot{y}_1, s'_1(x_1,x_2) \neq \dot{y}_2 \\ s'_2(x_2,\widehat{\pi}_1(x_1)), & x_2 = \dot{y}_1, \widehat{\pi}_1(x_1) \neq \dot{y}_2 \\ \widehat{\pi}_2(x_2) & x_2 \neq \dot{y}_1, s'_1(x_1,x_2) = \dot{y}_2 \\ \widehat{\pi}_2(x_2) & x_2 = \dot{y}_1, \widehat{\pi}_1(x_1) = \dot{y}_2 \end{cases}. \tag{10}$$

Задав ограничения на функции s'_1 и s'_2 можно упростить выражения для y_2 как функции от x_1,x_2 и x_1 как функции от y_1,y_2 и привести его к виду (4).

Утверждение 6 ([92])**.** *Пусть подстановка $F(x_1,x_2) = (y_1,y_2)$ задается по формулам* (6)–(7)*. Пусть также*

1. $\widehat{\pi}_1(x_1) = \dot{y}_2 \Leftrightarrow F_1(x_1, x_2) = \dot{y}_2$,
2. $x_2 = \dot{y}_1 \Leftrightarrow F_2(x_2, y_1) = \widehat{\pi}_2(\dot{y}_1)$.

Тогда

1. y_2 *выражается через* x_1, x_2 *следующей формулой:*

$$y_2 = FI_2(x_1, x_2) = \begin{cases} s'_2(x_2, s'_1(x_1,x_2)), & x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2) \\ \widehat{\pi}_2(x_2), & x_1 = \widehat{\pi}_1^{-1}(\dot{y}_2) \end{cases}, \tag{11}$$

2. x_1 *выражается через* y_1, y_2 *следующей формулой:*

$$x_1 = FI_1(y_1, y_2) = \begin{cases} s_1'^{-1}\left(y_1, s_2'^{-1}(y_2,y_1)\right), & y_2 \neq \dot{y}_1 \\ \widehat{\pi}_1^{-1}(y_1), & y_2 = \dot{y}_1 \end{cases}. \tag{12}$$

Таким образом, при верности условий утверждения 6 подстановка $F(x_1, x_2) = (y_1, y_2)$ задается по формулам (6) и (11), а обратная подстановка $F^{-1}(y_1, y_2) = (x_1, x_2)$ задается формулами (8) и (12). Каждая из этих формул задается формулой вида (4) при помощи функций с одной выколотой точкой. Перечислим эти функции:

- y_1 при $x_2 \neq \dot{y}_1$ задается формулой $s'_1(x_1,x_2)$;
- y_2 при $x_1 \neq \widehat{\pi}^{-1}(\dot{y}_1)$ задается формулой $s'_2(x_2,s'_1(x_1,x_2)) = s''(x_2, x_1)$;
- x_1 при $y_2 \neq \dot{y}_1$ задается формулой $s_1'^{-1}\left(y_1,s_2'^{-1}(y_2, y_1)\right) = s''_1(y_1, y_2)$;
- x_2 при $y_1 \neq \dot{y}_2$ задается формулой $s_2'^{-1}(y_2,y_1)$.

Так как нелинейность F равняется нелинейности F^{-1}, то можно предложить алгоритм построения подстановки с линейностью не выше $\mathbf{L}$ на основе утверждений 4 и 6, подробно описанный в [92].

При верности условий утверждения 6 получается гарантировать максимально возможную алгебраическую степень подстановок F и F^{-1}. В этом случае подстановки F и F^{-1} выражаются по формулам:

$$(y_1, y_2) = F(x_1, x_2) = (F_1(x_1, x_2), FI_2(x_1, x_2)), \tag{13}$$

$$(x_1, x_2) = F^{-1}(y_1, y_2) = \left(FI_1(y_1, y_2), F_2^{-1}(y_1, y_2)\right).$$

Определение 8. $(2m,m)$*-функцию* $s'(x,y)$ *назовем функцией с одной выколотой точкой* $\dot{y}$*, если для всех* $y \neq \dot{y}$ *функция* $s'(x,y)$ *является подстановкой по переменной* x *и* $s'(x,\dot{y})$ *не является подстановкой по переменной* x*. Если при этом* $s'(x,\dot{y}) = const$*, то такую функцию будем называть* C*-функцией с выколотой точкой* $\dot{y}$*.*

В случае, когда значение выколотой точки ясно из контекста, будем говорить просто о C-функции. Верно следующее

Утверждение 7 ([91]). *Пусть подстановка F задается формулой* (13). *Тогда*

– *если* $\deg(s'_i) \neq 2m-1$ *и* $(2m,m)$ *функция* s'_i *является* C*-функцией, то*

$$\deg(F_i) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_i) = m-1, i \in \overline{1,2};$$

– *если* $\deg\left(s'^{-1}_i\right) \neq 2m-1$ *и* $(2m,m)$ *функция* s'^{-1}_i *является* C*-функцией, то*

$$\deg\left(F_i^{-1}\right) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_1) = m-1, i \in \overline{1,2};$$

– *если* $\deg(s''_i) \neq 2m-1$ *и* $(2m,m)$ *функция* s''_i *является* C*-функцией, то*

$$\deg(FI_i) = 2m-1 \Leftrightarrow \deg(\widehat{\pi}_2) = m-1, i \in \overline{1,2}.$$

Следствие 4 ([91]). *Пусть выполняются все условия утверждения 7 и*

$$\deg(F_i) = \deg\left(F_i^{-1}\right) = \deg(FI_i) = 2m-1.$$

Тогда подстановка F и подстановка F^{-1} имеют максимально возможную алгебраическую степень равную $2m-1$.

Рассмотрим вопрос связи показателя дифференциальной равномерности подстановки F с параметрами преобразований, используемых при ее построении.

Лемма 1 ([91]). *Пусть подстановка F вычисляется по формуле* (13), *$a_1, a_2, b_1, b_2 \in \mathbb{F}_2^m$, тогда $\delta_F^{a_1\|a_2, b_1\|b_2}$ больше либо равно количеству решений системы уравнений*

$$\begin{cases} s'_1(x_1, x_2) \oplus s'_1(x_1 \oplus a_1, x_2 \oplus a_2) = b_1 \\ s''_2(x_1, x_2) \oplus s''_2(x_1 \oplus a_1, x_2 \oplus a_2) = b_2 \end{cases} \tag{14}$$

со следующими ограничениями на значения переменных x_1 и x_2:

1. $x_2 \neq \dot{y}_1$, $x_2 \neq \dot{y}_1 \oplus a_2$;
2. $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2)$, $x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2) \oplus a_1$.

Замечание 1. *Лемма 1 позволяет осуществлять направленный поиск пар функций $s'_1(x_1, x_2)$ и $s''_2(x_1, x_2)$ так, чтобы показатель дифференциальной равномерности построенной подстановки F был не выше заранее заданной границы Δ. Необходимым условием дифференциальной Δ-равномерности подстановки F является то, что количество решений системы* (14) *будет меньше либо равно Δ.*

Покажем на примере параметрических семейств подстановок, рассмотренных в работах [82], что лемма 1 позволяет ограничить возможные значения параметров, при которых подстановка F будет иметь показатель дифференциальной равномерности не меньше заданного.

Пусть функции

$$y_1 = F_1(x_1, x_2) = \begin{cases} \pi_1(x_1) \cdot x_2, & x_2 \neq \theta \\ \widehat{\pi}_1(x_1), & x_2 = \theta \end{cases}, \tag{15}$$

$$y_2 = F_2(x_2, y_1) = \begin{cases} \pi_2(x_2 \cdot y_1), & y_1 \neq \theta \\ \widehat{\pi}_2(x_2), & y_1 = \theta \end{cases}, \tag{16}$$

где подстановки π_i, $\widehat{\pi}_i$, $i \in \overline{1,2}$ являются параметрами семейства подстановок, задаваемых формулой (1).

Заметим, что функции

$$s'_1(x_1, x_2) = \pi_1(x_1) \cdot x_2 \text{ и } s'_2(x_2,y_1) = \pi_2(x_2 \cdot y_1)$$

есть C-функции, имеющие одну выколотую точку $x_2 = \theta$ и $y_1 = \theta$ соответственно. Для этих функций применимо утверждение 4 и следствие 3. Стоит отметить, что s'_1 является бент-функцией, принадлежащей классу Майорана-Макфараленда, а функция s'_2 принадлежит расширенному классу бент-функций Майорана-Макфараленда, если π_2 — линейная подстановка (см. напр. [18]).

Выразим y_2 как функцию от x_1 и x_2, используя утверждение 6 работы. Для выполнения условий указанного утверждения необходимо, чтобы

$$F_1\left(\widehat{\pi}_1^{-1}(\theta), x_2\right) = \theta, \tag{17}$$

$$F_2(\theta, y_1) = \widehat{\pi}_2(\theta). \tag{18}$$

Из равенства (17) следует, что $\pi_1(x_1) = \theta \Leftrightarrow \widehat{\pi}(x_1) = \theta$, а из равенства (18) следует, что $\pi_2(\theta) = \widehat{\pi}_2(\theta)$. Тогда

$$y_2 = \begin{cases} \pi_2\left((x_2)^2 \cdot \pi_1(x_1)\right), & x_1 \neq \widehat{\pi}^{-1}(\theta) \\ \widehat{\pi}_2(x_2), & x_1 = \widehat{\pi}^{-1}(\theta) \end{cases}. \tag{19}$$

Пусть $\widehat{\pi}_1^{-1}(\theta) = c_1$, $\widehat{\pi}_2(\theta) = c_2$, подстановка $F(x_1, x_2) = (y_1, y_2)$ определяется формулами (15), (19). Тогда аффинно-эквивалентная подстановка $G =$

$F(x_1+c_1, x_2)+(\theta, c_2)$, очевидно, также определяется формулами (15), (19) (с другими параметрами). В связи с этим, не теряя общности далее будем рассматривать только случай, когда θ является неподвижной точной для π_i, $\widehat{\pi}_i$, $i \in \overline{1,2}$.

Определение 9 ([91]). *Пусть* $x_1, x_2 \in \mathbb{F}_2^m$, $\pi_i, \widehat{\pi}_i \in S\left(\mathbb{F}_2^m\right)$, $\pi_i(\theta) = \theta$, $\widehat{\pi}_i(\theta) = \theta$, $i \in \overline{1,2}$, *тогда подстановку* F_A, *определяемую равенствами*

$$y_1 = \begin{cases} \pi_1(x_1) \cdot x_2, & x_2 \neq \theta \\ \widehat{\pi}_1(x_1), & x_2 = \theta \end{cases},$$

$$y_2 = \begin{cases} \pi_2\left((x_2)^2 \cdot \pi_1(x_1)\right), & x_1 \neq \theta \\ \widehat{\pi}_2(x_2), & x_1 = \theta \end{cases}.$$

будем называть подстановкой из параметрического семейства типа «A» или просто подстановкой типа «A».

Следующее утверждение позволяет существенно сократить параметрическое семейство типа «A». Можно не рассматривать подстановки с линейным параметром π_2 так как в этом случае такие подстановки будут дифференциально $\delta_{F_A} \geqslant 2^m - 2$-равномерными, что не позволит их использовать при синтезе безопасных алгоритмов конфиденциальности данных.

Утверждение 8 ([91]). *Пусть* F_A *— подстановка из параметрического семейства типа «A». Если параметр* π_2 *есть линейная подстановка, то* $\delta_{F_A} \geqslant 2^m - 2$.

В случае, когда π_2 — линейная функция, функция s_1', определенная в этом разделе, является бент-функцией и обладает наибольшей возможной нелинейностью, но, согласно утверждению 8, построенная подстановка в целом будет иметь высокий показатель дифференциальной равномерности.

Остается вопрос выбора конкретных подстановок π_i, $\widehat{\pi}_i$, $i \in \overline{1,2}$. В работе [82] рассматривались подстановки типа «A» для случая $m = 4$.

Для простоты параметры π_i, $i \in \overline{1,2}$ будем фиксировать мономиальными подстановками. Такие подстановки имеют вид x^d, где НОД$(d, 2^m - 2) = 1$. Учитывая малую теорему Ферма, нас интересуют только $d < 2^m - 2$.

В этом случае, формулы, задающие подстановку, можно переписать в следующем виде:

$$y_1 = \begin{cases} x_1^{\alpha} \cdot x_2, & x_2 \neq \theta \\ \widehat{\pi}_1(x_1), & x_2 = \theta \end{cases},$$

$$y_2 = \begin{cases} \left(x_2^2 \cdot x_1^{\alpha}\right)^{\beta}, & x_1 \neq \theta \\ \widehat{\pi}_2\left(x_2\right), & x_1 = \theta \end{cases} = \begin{cases} x_2^{2\beta} \cdot x_1^{\alpha\beta}, & x_1 \neq \theta \\ \widehat{\pi}_2\left(x_2\right), & x_1 = \theta \end{cases}.$$

При этом, согласно утверждению 8 преобразование x^{β} должно быть нелинейным преобразованием. Такие подстановки рассматривались в работе [82] для случая $m = 4$, в которой экспериментально исследовались подстановки типа «А» с мономиальными значениями параметров. Для случая $m = 4$ существует 8 значений d таких, что НОД $\left(d, 2^4 - 2\right) = 1$ это 1, 2, 4, 7, 8, 11, 13, 14. При этом, если $d \in \{1,2,4,8\}$, то x^d задает линейную подстановку. Согласно утверждению 8 π_2 не может быть линейной. В работе [82], фиксированием α произвольным значением из множества $\alpha \in \{1,2,4,7,8,11,13,14\}$, а $\beta \in \{1,2,4,8\}$, при подходящем выборе $\widehat{\pi}_i$ получены подстановки со следующими показателями нелинейности:

– нелинейность — 108,
– показатель дифференциальной равномерности — 6,
– алгебраическая степень — 7.

То есть в наиболее интересном с практической точки зрения случае $m = 4$ утверждение 8 задает достаточное условие на построение подстановок с «хорошими» показателями нелинейности.

Пусть функции

$$F_1\left(x_1, x_2\right) = \begin{cases} x_1 \cdot \pi_1\left(x_2\right), & \pi_1\left(x_2\right) \neq \theta \\ \widehat{\pi}_1\left(x_1\right), & \pi_1\left(x_2\right) = \theta \end{cases},$$

$$F_2\left(x_2, y_1\right) = \begin{cases} x_2 \cdot \pi_2\left(y_1\right), & \pi_2\left(y_2\right) \neq \theta \\ \widehat{\pi}_2\left(x_2\right), & \pi_2\left(y_2\right) = \theta \end{cases},$$

где подстановки π_i, $\widehat{\pi}_i$, $i \in \overline{1,2}$ являются параметрами семейства подстановок, задаваемых выражением (1).

Отметим, что функции $s'(x_1, x_2) = x_1 \cdot \pi_1(x_2)$ и $s'(x_2, y_1) = x_2 \cdot \pi_2(y_1)$ есть C-функции, а также бент-функции Майорана-Макфараленда, [18].

Как и ранее, выразим y_2 как функцию от x_1 и x_2, используя утверждение 6. И аналогично будем рассматривать только случай, когда θ является неподвижной точной для π_i, $\widehat{\pi}_i$, $i \in \overline{1,2}$.

Определение 10 ([91]). *Пусть* $x_1, x_2 \in \mathbb{F}_2^m$, $\pi_i, \widehat{\pi}_i \in S\left(\mathbb{F}_2^m\right)$, $\pi_i(\theta) = \theta$, $\widehat{\pi}_i(\theta) = \theta$, $i \in \overline{1,2}$, *тогда подстановку* F_B, *определяемую равенствами*

$$y_1 = \begin{cases} x_1 \cdot \pi_1\left(x_2\right), & x_2 \neq \theta \\ \widehat{\pi}_1\left(x_1\right), & x_2 = \theta \end{cases},$$

$$y_2 = \begin{cases} x_2 \cdot \pi_2\left(x_1 \cdot \pi_1\left(x_2\right)\right), & x_1 \neq \theta \\ \widehat{\pi}_2\left(x_2\right), & x_1 = \theta \end{cases},$$

будем называть подстановкой из параметрического семейства типа «Б» или просто подстановкой типа «Б».

Зададим подстановку, обратную к подстановке типа «Б».

$$x_1 = \begin{cases} y_1 \cdot \pi_2\left(y_2\right)^{-1}, \pi_2\left(y_2\right) \neq \theta \\ \widehat{\pi}_2^{-1}\left(y_1\right), \pi_2\left(y_2\right) = \theta \end{cases},$$

$$x_2 = \begin{cases} y_2 \cdot \pi_1\left(x_2\right)^{-1}, \pi_1\left(x_2\right) \neq \theta \\ \widehat{\pi}_1^{-1}\left(y_2\right), \pi_1\left(x_2\right) = \theta \end{cases}.$$

Таким образом, подстановка, обратная к подстановке типа «Б», сама является подстановкой типа «Б».

Воспользуемся леммой 1 и опишем значение параметров, при которых подстановка заведомо будет иметь высокий показатель дифференциальной равномерности.

Утверждение 9 ([91]). *Пусть* $H < S\left(\mathbb{F}_2^m\right)$ *— множество линейных подстановок. Если* $\pi_2 \in H$ *или* $\pi_1 \in x^{-1}H$, *то* $\delta_{S_B} \geqslant 2^m - 2$.

Рассмотрим случай мономиальных подстановок: $\pi_1 = x^\alpha$, $\pi_2 = x^\beta$ где α, β удовлетворяет равенству НОД $\left(\alpha, 2^4 - 2\right) = 1$, НОД $\left(\beta, 2^4 - 2\right) = 1$. Тогда

$$y_2 = \begin{cases} x_1 \cdot x_2^\alpha, x_2 \neq \theta \\ \widehat{\pi}_1\left(x_1\right), x_2 = \theta \end{cases},$$

$$y_1 = \begin{cases} x_2 \cdot \left(x_1 \cdot x_2^\alpha\right)^\beta, x_1 \neq \theta \\ \widehat{\pi}_2\left(x_2\right), x_1 = \theta \end{cases} = \begin{cases} x_1^\beta \cdot x_2^{\alpha\beta+1}, x_1 \neq \theta \\ \widehat{\pi}_2\left(x_2\right), x_1 = \theta \end{cases}.$$

В работе [82] были экспериментально исследованы подстановки типа «Б» в случае $m = 4$. По утверждению 9 значения параметров α и β принадлежат следующим множествам: $\alpha \in \{1,2,4,8\}$, $\beta \in \{7,11,13,14\}$. Покажем, что при фиксации α существует единственное β, при котором подстановка не будет иметь высокий показатель дифференциальной δ-равномерности.

Утверждение 10 ([91]). *Пусть* $m = 4$ *и* $\pi_1 = x^\alpha$, $\pi_2 = x^\beta$ *где* α, β *удовлетворяет равенству НОД* $\left(\alpha, 2^4 - 2\right) = 1$, *НОД* $\left(\beta, 2^4 - 2\right) = 1$. *Тогда, если* $\alpha\beta + 1 \neq 14 \pmod{15}$, *то* $\delta_{F_B} \geqslant 2^m - 2$.

Таким образом, возможны следующие случаи, которые были экспериментально обнаружены в работе [82].

1. $\pi_1(x) = x$, $\pi_2(x) = x^{13}$,
2. $\pi_1(x) = x^2$, $\pi_2(x) = x^{14}$,
3. $\pi_1(x) = x^4$, $\pi_2(x) = x^7$,
4. $\pi_1(x) = x^8$, $\pi_2(x) = x^{11}$.

При этом, случаи 2 и 4 являются обратными соответственно случаям 1 и 3. Для указанных случаев при правильном выборе $\widehat{\pi}_i$ в работе [82] были получены подстановки со следующими показателями нелинейности:

– нелинейность — 108,
– показатель дифференциальной равномерности — 6,
– алгебраическая степень нелинейности — 7.

Рассмотрим семейство подстановок, которые обобщают подстановки типа «А» и «Б» при фиксации мономиальных параметров подстановок, рассмотренных ранее. Рассмотрим семейство подстановок, параметрами которого является четверка степеней $(\alpha, \beta, \gamma, \delta)$ и подстановки $\widehat{\pi}_i$, $i \in \overline{1,2}$:

$$\begin{aligned} G_1(x_1, x_2) = y_1 &= \begin{cases} x_1^\alpha \cdot x_2^\beta, & x_2 \neq 0 \\ \widehat{\pi}_1(x_1), & x_2 = 0 \end{cases}, \\ G_2(x_1, x_2) = y_2 &= \begin{cases} x_1^\gamma \cdot x_2^\delta, & x_1 \neq 0 \\ \widehat{\pi}_2(x_2), & x_1 = 0 \end{cases}. \end{aligned} \tag{20}$$

Для того, чтобы уравнение (20) задавало биективное преобразование достаточно, чтобы уравнение

$$\begin{cases} G_1(x_1, x_2) = a_1 \\ G_2(x_1, x_2) = a_2 \end{cases}$$

имело решение для произвольных $a_1, a_2 \in \mathbb{F}_2^m$.

Рассмотрим случай $m = 4$. По малой теореме Ферма всего имеется 8 не равных между собой мономиальных подстановок поля $\mathbb{F}_{2^4}$. Воспользуемся леммой 1 можно ограничить значения параметров $(\alpha, \beta, \gamma, \delta)$ в уравнении (20) с использованием ЭВМ, аналогично работе [82]. Как и в работе [82] при правильном выборе параметров $\widehat{\pi}_i$, $i \in \overline{1,2}$ получаются подстановки, обладающие следующими показателями нелинейности:

– нелинейность — 108,
– показатель дифференциальной равномерности — 6,
– алгебраическая степень нелинейности — 7.

Экспериментально проверено, что указанные показатели нелинейности достигаются, например, в случае, когда $\widehat{\pi}_i(x) = x^d$, $d \in \{7,11,13,14\}$.

В работе [84] показано, что обобщенная конструкция также является F-конструкцией. Для случая $m = 4$ проведена классификация значений параметров $(\alpha, \beta, \gamma, \delta)$ с использованием леммы 1 и показано, что подстановки, обладающие указанными выше показателями нелинейности могут быть построены только с использованием параметров, приведенных в [91].

Легко показать, что у для большого количества значений параметров рассмотренных параметрических семейств подстановок значение графовой алгебраической иммунности равняется 2, что потенциально может привести к использованию алгебраических методов анализа алгоритмов обеспечения конфиденциальности данных, [21]. Рассмотрим $(2m,m)$-функции s'_1, s'_2, s''_1, s''_2 вида:

1. $y = x_1 \cdot x_2 \oplus \mathrm{Ind}_\theta(x_2)$;
2. $y = x_1 \cdot x_2^{-1} \oplus \mathrm{Ind}_\theta(x_2)$;
3. $y = x_1^{-2} \cdot x_2 \oplus \mathrm{Ind}_\theta(x_2)$.

Для каждой из этих функций можно привести функцию $g(x_1, x_2, y)$ невыраженная линейная комбинация координатных функций которой равняется 0, имеющей алгебраическую степень не выше двух, что говорит о том, что значение графовой алгебраической иммунности подстановок с такими координатными функциями будет равняться 2. Действительно, для первой функции $g(x_1, x_2,x_3) = x_2 \cdot y \oplus x_1 \cdot x_2^2 = 0$, для второй — $g(x_1, x_2,x_3) = x_2 \cdot y \oplus x_1 = 0$, для третей — $g(x_1, x_2,x_3) = y \cdot x_2 \oplus y \cdot x_1 = \mathrm{Ind}_\theta(x_2)$. В случае мономиального выбора подстановок π_i, $i = 1,2$ для параметрического семейства типа «Б» все подстановки будут иметь значение $AI_{gr}(F) = 2$, как и для параметрического семейства типа

«А» при мономиальном выборе π_i, $i = 1{,}2$ при линейной подстановке π_1, а также в случае нелинейного выбора, когда $\widehat{\pi}_2 = x^{-1}$.

Таким образом, предложены три параметрических семейств нелинейных биективных преобразований, для наиболее интересного с практической точки зрения случая $m = 4$ фиксированы некоторые параметры, позволяющие вырабатывать подстановки, обладающие «хорошими» показателями нелинейности при подходящем выборе $\widehat{\pi}_i$, $i = 1{,}2$. при правильном выборе параметров $\widehat{\pi}_i$, $i \in \overline{1{,}2}$ получаются подстановки, обладающие следующими показателями нелинейности:

– нелинейность — 108,
– показатель дифференциальной равномерности — 6,
– алгебраическая степень нелинейности — 7;
– показатель графовой алгебраической иммунности — 3.

Рассмотрим способ построения $\widehat{\pi}_i$, $i = 1{,}2$ с использованием эвристического алгоритма, основанного на известном генетическом алгоритме [30]. Данный подход ранее был успешно использован при реализации спектрально-линейного и спектрально разностного метода построения подстановок [56]. Подробное описание алгоритма, его корректность и способы оптимизации подробно описаны в [87]. Кратко суть предлагаемого алгоритма заключается в последовательном умножении подстановок $\widehat{\pi}_i$, $i = 1{,}2$ на транспозиции и отборе среди полученных подстановок пространства $\mathbb{F}_2^8$ лучших по нелинейности, показателю дифференциальной равномерности и соответствующим значениям в линейном и разностном спектрах. Таким образом, текущее поколение подстановок порождает некоторое количество новых пар, из них «выживают» только небольшое количество лучших. При этом скрещивания не производится, только «случайные мутации» внутри $\widehat{\pi}_i$, $i = 1{,}2$.

Рассмотрим конструкцию нелинейного биективного преобразования алгоритма Кузнечик, представление которого было взято за основу для рассмотренных в диссертации параметрических семейств подстановок.

Утверждение 11 ([83]). *Для подстановка π алгоритма Кузнечик существуют следующие подгруппы $(\mathsf{A}_i, \mathsf{B}_i)$, $i = 1{,}2$, группы $\mathbb{F}_2^8$*

– $\mathsf{A}_1 = \left\{ \alpha^{-1}\left(\mathtt{0xd} \cdot x \| x\right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}_1 = \left\{ \beta\left(\mathtt{0x0} \| y\right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,
– $\mathsf{A}_2 = \left\{ \alpha^{-1}\left(x \| \mathtt{0x0}\right) \middle| \, x \in \mathbb{F}_{2^4} \right\}$, $\mathsf{B}_2 = \left\{ \beta\left(y \| \mathtt{0x0}\right) \middle| \, y \in \mathbb{F}_{2^4} \right\}$,

такие, что существуют $a, b \in \mathbb{F}_2^8$: $\pi(\mathsf{A}_i \oplus a) = \mathsf{B}_i \oplus b$.

Определение 11 ([83]). *Пару подгрупп пространства* $\mathbb{F}_q$ (A, B) *будем называть I-парой для подстановки* $\pi\colon \mathbb{F}_q \to \mathbb{F}_q$, *если существуют* $a,b \in \mathbb{F}_q$ *такие, что*

$$\pi(\mathsf{A} \oplus a) = \mathsf{B} \oplus b.$$

При этом A *и* B *будем называть LI и RI множеством для* π *соответственно.*

Путь $\mathrm{span}(S)$ — линейная оболочка множества S. Тогда с использованием идей, предложенных в [49], можно предложить следующий алгоритм поиска I-пар для подстановки $\pi\colon \mathbb{F}_q \to \mathbb{F}_q$:

1. $i := 0$
2. `для всех` $a, b \in \mathbb{F}_q$:
   а) $\mathsf{A}_i \leftarrow \{0\}$;
   б) $\mathsf{B}_i \leftarrow \mathrm{span}\left(\pi\left(\mathsf{A}_i \oplus a\right) \oplus b\right)$;
   в) $\mathsf{A}_i \leftarrow \mathrm{span}\left(\pi^{-1}\left(\mathsf{A}_i \oplus b\right) \oplus a\right)$;
   г) `если` $\mathsf{A}_i = \mathrm{span}(\mathsf{A}_i)$ `тогда:`
      – `если` $|\mathsf{A}_i| \neq 2^8$, `вывести`$(A_i = \mathsf{A}_i \oplus a, B_i = \mathsf{B}_i \oplus b)$, $i \leftarrow i + 1$;
      – `для всех` $x \in \mathbb{F}_2^8 \backslash \mathsf{A}_i$: $\mathsf{A}_i \leftarrow \mathrm{span}\left(\mathsf{A}_i \cup x\right)$, `на шаг` (2.б);

В утверждении 11 были найдены две I-пары $(\mathsf{A}_i, \mathsf{B}_i)$ для подстановки π алгоритма Кузнечик; мощность каждого множества равняется 16. С использованием представленного выше алгоритма возможно найти все I-пары для подстановки π:

– 2 I-пары $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 16$;
– 1 943 I-пар $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 4$;
– 2 730 I-пар $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{A}_i| = |\mathsf{B}_i| = 2$.

Для подстановок из предложенных параметрических семейств также существуют I-пары мощности 2^m каждая вида:

1. $\mathsf{A}'_1 = \{(\theta \| x) |\, x \in \mathbb{F}_{2^m}\}$, $\mathsf{B}'_1 = \{(\theta \| y) |\, y \in \mathbb{F}_{2^m}\}$,
2. $\mathsf{A}'_2 = \{(x \| \theta) |\, x \in \mathbb{F}_{2^m}\}$, $\mathsf{B}'_2 = \{(y \| \theta) |\, y \in \mathbb{F}_{2^m}\}$,

Таким образом, необходимо уметь обосновывать стойкость алгоритмов защиты конфиденциальности данных относительно методов анализа, использующих инварианты преобразований.

Четвертая глава диссертации посвящена влиянию конструктивных особенностей предлагаемых параметрических семейств подстановок на безопасность алгоритмов защиты конфиденциальности данных. Будем использовать обозначения из первого раздела.

Определение 12 ([88]). *Матрицами типа II будем называть матрицы* $C \in (\mathbb{F}_2)_{n'm,n'm}$ *вида*

$$C = \begin{pmatrix} C_{1,1} & \dots & C_{1,m} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,m} \end{pmatrix},$$

где $C_{i,j} \in (\mathbb{F}_2)_{n',n'}$ *невырождены,* $i,j = 1,\dots,m$.

Рассмотрим алгоритм обеспечения конфиденциальности данных, построенный на основе XSL-сети с линейным преобразованием, задаваемым матрицей типа II. Опишем один подход к поиску множеств $G_K \subset \mathbb{F}_2^n$, инвариантных относительно композиции преобразований $\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}$. Пусть имеется пара семейств множеств $(\mathcal{A}, \mathcal{B})$, где

$$\mathcal{A} = \{A_1, A_2, \dots, A_{e_a}\}, A_i \subseteq \mathbb{F}_2^{n'},$$

$$\mathcal{B} = \{B_1, B_2, \dots, B_{e_b}\}, B_i \subseteq \mathbb{F}_2^{n'},$$

и для любого $i \in \{1,\dots,e_a\}$ существует $j \in \{1,\dots,e_b\}$ такой, что $A_i^{\pi} \subseteq B_j$. Рассмотрим семейства $\mathcal{A}^m$ и $\mathcal{B}^m$ — декартовы степени множеств $\mathcal{A}$ и $\mathcal{B}$ соответственно. Тогда для любого элемента $A_{i_1} \times \dots \times A_{i_m} \in \mathcal{A}^m$ существует элемент $B_{j_1} \times \dots \times B_{j_m} \in \mathcal{B}^m$ такой, что

$$(A_{i_1} \times \dots \times A_{i_m})^{\mathrm{S}} = \left(A_{i_1}^{\pi} \times \dots \times A_{i_m}^{\pi}\right) \subseteq B_{j_1} \times \dots \times B_{j_m}.$$

Множество G_K будем искать среди подмножеств множества $\mathcal{A}^m$, то есть элементами множества G_K являются множества вида $A_{i_1} \times A_{i_2} \times \dots \times A_{i_m} \in \mathcal{A}^m$.

Пусть $\mathcal{C}$ — такое семейство множеств, что для любого элемента элемента $B_{j_1} \times \dots \times B_{j_m} \in \mathcal{B}^m$ существует элемент C семейства $\mathcal{C}$, для которого выполняется включение

$$(B_{j_1} \times \dots \times B_{j_m})^{\mathrm{L}} \subseteq C.$$

Пусть также существует такой $K \in \left(\mathbb{F}_2^{n'}\right)^m$, что $\mathcal{C}^{\mathrm{X}[K]} = \mathcal{A}^m$, то есть верна следующая диаграмма:

$$\mathcal{A}^m \xrightarrow{\mathrm{S}} \mathcal{B}^m \xrightarrow{\mathrm{L}} \mathcal{C} \xrightarrow{\mathrm{X}[K]} \mathcal{A}^m. \tag{21}$$

Все дальнейшие рассуждения будем проводить в предположении выполнимости диаграммы 21. В этом случае, очевидно, выполняется равенство: $|\mathcal{C}| = |\mathcal{A}^m|$. Действительно, рассмотрим элемент $A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m} \in \mathcal{A}^m$, $i_1, \ldots, i_m \in \{1, \ldots, e_a\}$. Пусть $K = (k_1, k_2, \ldots, k_m)$. Тогда

$$(A_{i_1} \oplus k_1) \times (A_{i_2} \oplus k_2) \times \ldots \times (A_{i_m} \oplus k_m) \in \mathcal{C}.$$

Таким образом множество C состоит из прямого произведения множеств вида $A_j \oplus k_i$, $j \in \{1, \ldots, e_a\}$, $i \in \{1, \ldots, m\}$.

Утверждение 12 ([88])**.** *Пусть имеется алгоритм обеспечения конфиденциальности данных, построенный на основе XSL-сети, линейное преобразование которого* $L = (l_{a,b})_{m \times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1, \ldots, m$, *задается матрицей типа II. Рассмотрим множества*

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}^m,\ i_1, \ldots, i_m \in \{1, \ldots, e_b\},$$

и

$$C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C},\ j_1, \ldots, j_m \in \{1, \ldots, e_a\},$$

такие, что $B^{\mathrm{L}} \subseteq C$*, и для некоторого ключа* $K \in \left(\mathbb{F}_2^{n'}\right)^m$ *выполнена диаграмма 21. Тогда для любого* $j \in \{j_1, \ldots, j_m\}$ *выполнено неравенство* $|C_j| \geqslant \max\limits_{i \in \{i_1, \ldots, i_m\}} |B_i|$.

Из верности диаграммы 21 следует, что для любых $i_1, \ldots, i_m \in \{1, \ldots, e_a\}$ существуют такие $j_1, \ldots, j_m \in \{1, \ldots, e_a\}$, что будет верна диаграмма:

$$A_{i_1} \times \ldots \times A_{i_m} \xrightarrow{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} A_{j_1} \times \ldots \times A_{j_m}.$$

Зададим на семействе $\mathcal{A}^m$ ориентированный граф Γ с помеченными дугами следующим образом. Вершинами этого графа являются элементы семейства $\mathcal{A}^m$, при этом вершины $X, Y \in \mathcal{A}^m$, соединены дугой с пометкой K тогда и только тогда, когда существует ключ K такой, что $X^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} \to Y$. При этом, если $\mathbb{F}_2^{n'} \in \mathcal{A}$, то очевидно, что для произвольного ключа K

$$\left(\left(\mathbb{F}_2^{n'}\right)^m\right)^{\mathrm{X}[K] \circ \mathrm{L} \circ \mathrm{S}} = \left(\mathbb{F}_2^{n'}\right)^m$$

есть цикл, который будем называть тривиальным. Для построения множества G_K необходимо уметь искать нетривиальные циклы в графе Γ. В частности G_K

— множество вершин графа Γ, лежащих на циклах длины 1 (петлях) с пометкой K. Однако далее предлагается рассматривать и более общий случай, когда цикл состоит из более чем одной вершины. Предположим, что в графе Γ существует нетривиальный цикл длины r, задаваемый подсемейством семейства $\mathcal{A}^m$. Это эквивалентно тому, что некоторое подмножество $\mathcal{A}^m$ является инвариантным относительно r раундов рассматриваемого алгоритма обеспечения конфиденциальности данных для некоторых ключей $K_1, \ldots, K_r$. Найдем необходимые условия существования нетривиального цикла и предложим конструктивный алгоритм его поиска.

Пусть здесь и далее $\mathcal{A}' \subset \mathcal{A}^m$ — множество вершин графа Γ, задающее некоторый нетривиальный цикл длины r. Обозначим $\mathcal{B}' = (\mathcal{A}')^{\mathrm{S}}$, $\mathcal{C}' = (\mathcal{B}')^{\mathrm{L}}$. При этом, для каждого $A \in \mathcal{A}'$ существует ключ K и множество $C \in \mathcal{C}'$ такие, что $C^{\mathrm{X}[K]} = A$.

Утверждение 13 ([88]). *Пусть имеется алгоритм обеспечения конфиденциальности данных, построенный на основе XSL-сети, линейное преобразование которого* $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1,\ldots,m$, *задается матрицей типа II, элементы семейства* $\mathcal{A}'$ *задают некоторый нетривиальный цикл графа* Γ, $A_{a_1} \times \ldots \times A_{a_m} \in \mathcal{A}'$, *и*

$$B_{b_1} \times \ldots \times B_{b_m} \in \mathcal{B}',\ B_{b_1} \times \ldots \times B_{b_m} = \mathrm{S}\left(A_{a_1} \times \ldots \times A_{a_m}\right),$$

$$C_{c_1} \times \ldots \times C_{c_m} \in \mathcal{C}',\ C_{c_1} \times \ldots \times C_{c_m} = \mathrm{L}\left(B_{b_1} \times \ldots \times B_{b_m}\right).$$

Тогда

1. $|A_{a_1}| = |B_{b_1}| = |C_{c_1}|$,
2. $|A_{a_1}| = |A_{a_2}| = \ldots = |A_{a_m}|$,
3. $|B_{b_1}| = |B_{b_2}| = \ldots = |B_{b_m}|$,
4. $|C_{c_1}| = |C_{c_2}| = \ldots = |C_{c_m}|$.

Следующее утверждение позволяет сформулировать алгоритм поиска циклов в графе Γ или доказать, что нетривиальных циклов нет.

Утверждение 14 ([88]). *Пусть для алгоритма обеспечения конфиденциальности данных, построенного на основе XSL-сети, линейное преобразование которого* $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1,\ldots,m$, *задается матрицей типа II, элементы семейства* $\mathcal{A}'$ *задают некоторый нетривиальный цикл графа* Γ. *Пусть также*

$$B = B_{i_1} \times B_{i_2} \times \ldots \times B_{i_m} \in \mathcal{B}',$$

$$C = C_{j_1} \times C_{j_2} \times \ldots \times C_{j_m} \in \mathcal{C}',$$

где $C = B^{\mathrm{L}}$. *Тогда*

1. *для произвольного* $v \in \{1, \ldots, m\}$ *множество* B_{i_v} *является смежным классом по некоторому подпространству пространства* $\mathbb{F}_2^{n'}$;
2. *для произвольного* $v \in \{1, \ldots, m\}$ *множество* C_{j_v} *является смежным классом по некоторому подпространству пространства* $\mathbb{F}_2^{n'}$;

Следствие 5 ([88]). *Пусть в условиях утверждения*

$$A = A'_{i_1} \times A'_{i_2} \times \ldots \times A'_{i_m} \in \mathcal{A}'.$$

Тогда для любого $j \in \{1, \ldots, m\}$ *множество* A'_{i_j} *является смежным классом по некоторому подпространству пространства* $\mathbb{F}_2^{n'}$.

Таким образом, нас в первую очередь интересуют такие пары множеств (A, B), что $A^{\pi} = B$, $A = H_A \oplus h_A$, $B = H_B \oplus h_B$, и H_A, H_B — подпространства пространства $\mathbb{F}_2^{n'}$, h_A,$h_B \in \mathbb{F}_2^{n'}$.

Предположим, имеется M пар таких множеств (A_i, B_i), $i \in \{1, \ldots, M\}$, при этом $A_i = H_{A,i} \oplus h_{A,i}$, $B_i = H_{B,i} \oplus h_{B,i}$, $|A_i| = |A_j|$ $\forall i,j \in \{1, \ldots, M\}$. Необходимость одинаковости мощностей множеств A_i обусловлена аналогичным требованием для множеств, образующих цикл в графе Г. Рассмотрим вектор $h \in \left(\mathbb{F}_2^{n'}\right)^m$:

$$h = \left(h_{B,i_1}, h_{B,i_2}, \ldots, h_{B,i_m}\right), i_1, \ldots, i_m \in \{1, \ldots, M\}.$$

Всего таких векторов $|M|^m$.

Для каждых $v,w = 1, \ldots, m$ вычислим множество $C(h,v,w) \subset \mathbb{F}_2^{n'}$:

$$C(h,v,w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} + y \cdot l_{v,w} \,\middle|\, y \in H_{B,v} \right\}$$

и проверим существует ли такой $g(w) \in \mathbb{F}_2^{n'}$ и такой $j(w) \in \{1, \ldots, M\}$, зависящий от w, что:

$$C(h,v,w) \oplus g(w) = A_{j(w)}.$$

То есть при разных v, но одинаковых w множество $A_{j(w)}$ и элемент $g(w)$ должны быть одинаковыми.

Теорема 1 ([88]). *Пусть для алгоритма обеспечения конфиденциальности данных, построенного на основе XSL-сети, линейное преобразование которого* $L = (l_{a,b})_{m\times m}$, $l_{a,b} \in GL_{n'}(2)$, $a,b = 1,\ldots,m$, *задается матрицей типа II, элементы семейства* $\mathcal{A}'$ *задают некоторый нетривиальный цикл в графе* Γ. *Пусть также* $A_i = H_{A,i} \oplus h_{A,i}$, $H_{A,i}$ *— подпространство пространства* $\mathbb{F}_2^{n'}$, $h_{A,i} \in \mathbb{F}_2^{n'}$, $i \in \{1,\ldots,M\}$, *при этом* $|A_i| = |A_j|\ \forall i,j \in \{1,\ldots,M\}$. *Для множества* $A \in \mathcal{A}'$,

$$A = A_{i_1} \times A_{i_2} \times \ldots \times A_{i_m},\ i_1,\ldots,i_m \in \{1,\ldots,M\}$$

существует такой ключ K, *что* $A^{\mathrm{L}\circ\mathrm{S}\circ\mathrm{X}[K]} = A' \in \mathcal{A}'$,

$$A' = A_{j_1} \times A_{j_2} \times \ldots \times A_{j_m},\ j_1,\ldots,j_m \in \{1,\ldots,M\}$$

тогда и только тогда, когда для каждого $w \in \{1,\ldots,m\}$ *существует вектор* $g(w) \in \mathbb{F}_2^{n'}$ *и номер* $j(w) \in \{1,\ldots,M\}$ *такие, что для любого* $v \in \{1,\ldots,m\}$ *выполнено равенство*

$$C(h,v,w) \oplus g(w) = A_{j(w)},$$

где

$$C(h,v,w) = \left\{ \sum_{b=1}^{m} h_{B,i_b} \cdot l_{b,w} \oplus y \cdot l_{v,w} \,\middle|\, y \in H_{B,v} \right\}.$$

С использованием доказанной теоремы возможно конструктивно строить инварианты для раундового преобразования алгоритма обеспечения конфиденциальности данных, построенного на основе XSL-сети рассматриваемого вида.

С использованием результатов теоремы 1 возможно предложить следующий подход к обоснованию невозможности применения предложенного метода анализа для алгоритма Кузнечик. Пусть $(\mathsf{A}_i, \mathsf{B}_i)$ I-пара для подстановки π. Рассмотрим

$$B_i^{(j)} = \underbrace{\{\theta\} \times \ldots \times \{\theta\}}_{j-1} \times \mathsf{B}_i \times \{\theta\} \times \ldots \times \{\theta\},$$

$$\mathrm{L}\left(B_i^{(j)}\right) = C_i^{(j)} = \left\{ \left(c_{i,k}^{(j,1)}, \ldots, c_{i,k}^{(j,m)} \right), k = 1,\ldots,|\mathsf{B}_i| \right\}.$$

Тогда согласно теореме 1 каждое множество

$$C_i^{(j,l)} = \left\{ c_{i,k}^{(j,l)}, k = 1,\ldots,|\mathsf{B}_i| \right\}$$

есть некоторое LI-множество A_d для π. Тогда

$$\exists\, c_1, c_2 \in \mathbb{F}_{2^4} \colon \pi\left(\mathsf{A}_d \oplus c_1\right) \oplus c_2$$

есть подгруппа $(\mathbb{F}_q, \oplus)$. Верно следующее

Утверждение 15 ([83]). *Пусть* π *— подстановка,* L *— линейное и* S *— нелинейное преобразование алгоритма Кузнечик. Тогда любая I пара* $(\mathsf{A}_i, \mathsf{B}_i)$, $|\mathsf{B}_i| > 1$, *для подстановки* π *и для любого* $j = \{1, \ldots, m\}$, *существует* $l = \{1, \ldots, m\}$ *такое, что* $C_i^{(j,l)}$ *не является подмножеством никакой из подгрупп* A_d *таких, что*

$$\exists\, c_1, c_2 \in \mathbb{F}_{2^4} \colon \pi\left(\mathsf{A}_d \oplus c_1\right) \oplus c_2$$

является подгруппой $(\mathbb{F}_q, \oplus)$.

Работа выполнена на кафедре компьютерной безопасности Московского института электроники и математики им. А. Н. Тихонова — Национальный исследовательский университет «Высшая школа экономики».

Список опубликованных статей по теме диссертации: Основные положения по теме диссертации изложены в 13 научных работах. 9 из них входят в Списки журналов, издательств и конференций НИУ ВШЭ:

1. *Fomin, D. B.* A timing attack on CUDA implementations of an AES-type block cipher / D. B. Fomin // Математические вопросы криптографии. 2016. Т. 7, № 2. С. 121—130
2. *Fomin, D. B.* New Classes of 8-bit Permutations Based on a Butterfly Structure / D. B. Fomin // Математические вопросы криптографии. 2019. Т. 10, № 2. С. 169—180
3. *Фомин, Д. Б.* Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций / Д. Б. Фомин // Математические вопросы криптографии. 2020. Т. 11, № 3. С. 121—138
4. *Фомин, Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m,m)$-функций / Д. Б. Фомин // Математические вопросы криптографии. 2020. Т. 11, № 4. С. 133—149
5. *Трифонов, Д. И.* Об инвариантных подпространствах в XSL-шифрах / Д. И. Трифонов, Д. Б. Фомин // Прикладная дискретная математика. 2021. Т. 54. С. 58—76

   /Фомину Д.Б. принадлежат результаты, следующие за доказательством утверждения 4, стр. 67–71./
6. Об одном представлении нелинейного преобразования алгоритма «Кузнечик» с помощью логических функций / О. Д. Авраамова, Д. Б. Фомин,

В. А. Серов [и др.] // Математические вопросы криптографии. 2021. Т. 12, № 2. С. 21—38

/Фомину Д.Б. принадлежит постановка задачи, а также результаты раздела 3.3./

7. *Kovrizhnykh*, *M. A.* On differential uniformity of permutations derived using a generalized construction / M. A. Kovrizhnykh, D. B. Fomin // Математические вопросы криптографии. 2022. Т. 13, № 2. С. 37—52

   /Фомину Д.Б. принадлежит постановка задачи и методика исследований./

8. *Fomin*, *D. B.* On the impossibility of an invariant attack on Kuznyechik / D. B. Fomin // Journal of Computer Virology and Hacking Techniques. 2022. Т. 18, № 1. С. 61—67

9. *Коврижных*, *М. А.* Об эвристическом алгоритме построения подстановок с заданными криптографическими характеристиками с использованием обобщённой конструкции / М. А. Коврижных, Д. Б. Фомин // Прикладная дискретная математика. 2022. Т. 57. С. 5—21

   /Фомину Д.Б. принадлежит постановка задачи, методика исследований, а также результаты раздела 3.1./

При этом 5, 8 и 9 статьи из этого списка проиндексированы в международной системе Scopus.

Публикации автора по теме диссертационного исследования в других изданиях:

10. *Фомин*, *Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований / Д. Б. Фомин // Обозрение прикладной и промышленной математики. 2018. Т. 25, № 4. С. 379—381

11. *Фомин*, *Д. Б.* Об аппаратной реализации одного класса байтовых подстановок / Д. Б. Фомин, Д. И. Трифонов // Прикладная дискретная математика. Приложение. 2019. Т. 12. С. 134—137

    /Фомину Д.Б. принадлежит способ выбора нелинейных биективных преобразований специального вида./

12. *Фомин*, *Д. Б.* О способе построения дифференциально 2δ-равномерных подстановок на $\mathbb{F}_{2^{2m}}$ / Д. Б. Фомин // Прикладная дискретная математика. Приложение. 2021. Т. 14. С. 51—55

13. *Коврижных*, *М. А.* Об эвристическом подходе к построению биективных векторных булевых функций с заданными криптографическими харак-

теристиками / М. А. Коврижных, Д. Б. Фомин // Прикладная дискретная математика. Приложение. 2021. Т. 14. С. 181—184
/Фомину Д.Б. принадлежит постановка задачи и методика исследований./

Заключение

Основные результаты работы заключаются в следующем.

1. Разработан метод анализа алгоритмов обеспечения конфиденциальности данных специального вида, реализованного на графических вычислителях, по информации о времени выполнения операций. Показана принципиальная возможность применения методов анализа алгоритмов защиты информации, реализованных на графических вычислителях, по информации из побочных каналов утечки. Показана практическая возможность применения предложенного метода анализа для алгоритма AES.
2. Предложены параметрические семейства подстановок, оценены для них такие показателей нелинейности, как нелинейность, алгебраическая степень, дифференциальная δ-равномерность. Разработаны алгоритмы построения нелинейных биективных преобразований из рассмотренных параметрических семейств.
3. Предложен метод анализа, основанный на поиске инвариантов преобразований, используемых в алгоритмах обеспечения конфиденциальности данных, построенных на основе XSL-сети.
4. Показана неэффективность применения предложенных методов анализа для алгоритма Кузнечик.

Список литературы

1. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования. — М. : Стандартинформ, 2018. — 25 с. — (Межгосударственный стандарт).
2. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. — М. : Стандартинформ, 2018. — 14 с. — (Межгосударственный стандарт).
3. Доктрина информационной безопасности Российской Федерации. — Российская газета, 2016. — URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html.
4. Методический документ. Методика оценки угроз безопасности информации. — М. : ФСТЭК России, 2021. — 83 с.
5. Рекомендации по стандартизации Р 1323565.1.012-2017. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. — М. : Стандартинформ, 2018. — 23 с. — (Рекомендации по стандартизации).
6. *Aziz*, *A.* A look-up-table implementation of AES / A. Aziz, N. Ikram //. — 01.2007. — С. 187—191.
7. *Bao*, *Z.* Bitsliced Implementations of the PRINCE, LED and RECTANGLE Block Ciphers on AVR 8-bit Microcontrollers. / Z. Bao, P. Luo, D. Lin // IACR Cryptology ePrint Archive. — 2015. — Т. 2015. — С. 1118. — URL: http://dblp.uni-trier.de/db/journals/iacr/iacr2015.html#BaoLL15.
8. *Bernstein*, *D. J.* Cache-timing attacks on AES : тех. отч. / D. J. Bernstein. — 2005.
9. *Biham*, *E.* A Fast New DES Implementation in Software. / E. Biham // FSE. Т. 1267 / под ред. E. Biham. — Springer, 1997. — С. 260—272. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse97.html#Biham97a.
10. *Biham*, *E.* Differential Cryptanalysis of DES-like Cryptosystems. / E. Biham, A. Shamir // J. Cryptology. — 1991. — Т. 4, № 1. — С. 3—72. — URL: http://dblp.uni-trier.de/db/journals/joc/joc4.html#BihamS91.

11. *Biryukov*, *A.* Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. / A. Biryukov, L. Perrin, A. Udovenko. — 2016. — http://eprint.iacr.org/2016/071.

12. *Biryukov*, *A.* Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. / A. Biryukov, L. Perrin, A. Udovenko. — 2016. — URL: http://dblp.uni-trier.de/db/conf/eurocrypt/eurocrypt2016-1.html#BiryukovPU16.

13. Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs. / A. Bogdanov, T. Eisenbarth, C. Paar [и др.] // CT-RSA. Т. 5985 / под ред. J. Pieprzyk. — Springer, 2010. — С. 235—251. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/ctrsa/ctrsa2010.html#BogdanovEPW10.

14. Strong 8-bit Sboxes with efficient masking in hardware extended version. / E. Boss, V. Grosso, T. Güneysu [и др.] // J. Cryptographic Engineering. — 2017. — Т. 7, № 2. — С. 149—165. — URL: http://dblp.uni-trier.de/db/journals/jce/jce7.html#BossGGL0017.

15. An APN permutation in dimension six / K. Browning, J. Dillon, M. McQuistan [и др.]. — 2010.

16. *Buchfuhrer*, *D.* The complexity of Boolean formula minimization. / D. Buchfuhrer, C. Umans // J. Comput. Syst. Sci. — 2011. — Т. 77, № 1. — С. 142—153. — URL: http://dblp.uni-trier.de/db/journals/jcss/jcss77.html#BuchfuhrerU11.

17. *Canteaut*, *A.* Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version). / A. Canteaut, S. Duval, G. Leurent // IACR Cryptology ePrint Archive. — 2015. — Т. 2015. — С. 711. — URL: http://dblp.uni-trier.de/db/journals/iacr/iacr2015.html#CanteautDL15 ; http://eprint.iacr.org/2015/711.

18. *Carlet*, *C.* Vectorial Boolean functions for cryptography / C. Carlet // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. — 2006.

19. Building Your Private Cloud Storage on Public Cloud Service Using Embedded GPUs / W. Cheng, F. Zheng, W. Pan [и др.] // Security and Privacy in Communication Networks. — Cham : Springer International Publishing, 2018. — С. 512—528.

20. *Christophe Clavier*, *L. R.* Systematic and Random Searches for Compact 4-Bit and 8-Bit Cryptographic S-Boxes / L. R. Christophe Clavier // IACR Cryptology ePrint Archive. — 2019.

21. *Courtois*, *N.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations / N. Courtois, J. Pieprzyk. — 2002. — https://eprint.iacr.org/2002/044. Cryptology ePrint Archive, Report 2002/044.

22. *Cruz Jiménez*, *R. A. de la*. Generation of 8-bit S-Boxes having almost optimal cryptographic properties using smaller 4-bit S-Boxes and finite field multiplication / R. A. de la Cruz Jiménez. — www.cs.haifa.ac.il/~orrd/LC17/paper60.pdf.

23. *Cruz Jiménez*, *R. A. de la*. On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks / R. A. de la Cruz Jiménez. — 2018. — URL: https://eprint.iacr.org/2018/618 ; https://eprint.iacr.org/2018/618. Cryptology ePrint Archive, Paper 2018/618.

24. *Daemen*, *J.* Rijndael for AES. / J. Daemen, V. Rijmen // AES Candidate Conference. — National Institute of Standards, Technology, 2000. — С. 343—348. — URL: http://dblp.uni-trier.de/db/conf/aes/aes2000.html#DaemenR00.

25. *Dobbertin*, *H.* Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity. / H. Dobbertin // FSE. Т. 1008 / под ред. B. Preneel. — Springer, 01.01.2008. — С. 61—74. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse94.html#Dobbertin94.

26. First-Round and Last-Round Power Analysis Attack Against AES Devices / S. D. Putra, A. D. W. Sumari, I. Asrowardi [и др.] // 2020 International Conference on Information Technology Systems and Innovation (ICITSI). — 2020. — С. 410—415.

27. *Fomin*, *D. B.* Implementation of an XSL block cipher with MDS-matrix linear transformation on NVIDIA CUDA / D. B. Fomin // Математические вопросы криптографии. — 2015. — Т. 6, № 2. — С. 99—108.

28. *Freyre-Echevarria*, *A.* On the Generation of Cryptographically Strong Substitution Boxes from Small Ones and Heuristic Search / A. Freyre-Echevarria // 10th Workshop on Current Trends in Cryptology (CTCrypt 2021). Pre-proceedings. — 2021. — С. 112—128.

29. *Gao*, *Y.* Side-Channel Attacks With Multi-Thread Mixed Leakage / Y. Gao, Y. Zhou // IEEE Transactions on Information Forensics and Security. — 2021. — T. 16. — C. 770—785.

30. Genetic Programming – An Introduction / W. Banzhaf, P. Nordin, R. E. Keller [и др.]. — San Francisco, CA, USA : Morgan Kaufmann Publishers, 1998.

31. Block Ciphers That Are Easier to Mask: How Far Can We Go? / B. Gérard, V. Grosso, M. Naya-Plasencia [и др.] // CHES. T. 8086 / под ред. G. Bertoni, J.-S. Coron. — Springer, 2013. — C. 383—399. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/ches/ches2013.html#GerardGNS13.

32. LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. / V. Grosso, G. Leurent, F.-X. Standaert [и др.] // FSE. T. 8540 / под ред. C. Cid, C. Rechberger. — Springer, 2014. — C. 18—37. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse2014.html#GrossoLSV14.

33. *Gullasch*, *D.* Cache Games - Bringing Access-Based Cache Attacks on AES to Practice. / D. Gullasch, E. Bangerter, S. Krenn // IEEE Symposium on Security and Privacy. — IEEE Computer Society, 2011. — C. 490—505. — URL: http://dblp.uni-trier.de/db/conf/sp/sp2011.html#GullaschBK11.

34. *Heys*, *H. M.* A Tutorial on Linear and Differential Cryptanalysis. / H. M. Heys // Cryptologia. — 2002. — T. 26, № 3. — C. 189—221. — URL: http://dblp.uni-trier.de/db/journals/cryptologia/cryptologia26.html#Heys02.

35. *Hlavicka*, *J.* A Heuristic Boolean Minimizer / J. Hlavicka, P. Fiser // ICCAD'01. — 2001.

36. *Iwai*, *K.* Acceleration of AES encryption on CUDA GPU. / K. Iwai, N. Nishikawa, T. Kurokawa // Int. J. Netw. Comput. — 2012. — T. 2, № 1. — C. 131—145. — URL: http://dblp.uni-trier.de/db/journals/ijnc/ijnc2.html#IwaiNK12.

37. *Jakobsen*, *T.* Attacks on Block Ciphers of Low Algebraic Degree / T. Jakobsen, L. R. Knudsen // Journal of Cryptology. — 2001. — Июнь. — T. 14, № 3. — C. 197—210. — URL: https://doi.org/10.1007/s00145-001-0003-x.

38. Optimizing Implementations of Lightweight Building Blocks. / J. Jean, T. Peyrin, S. M. Sim [и др.] // IACR Trans. Symmetric Cryptol. — 2017. — Т. 2017, № 4. — С. 130—168. — URL: http://dblp.uni-trier.de/db/journals/tosc/tosc2017.html#JeanPST17.

39. *Jiang*, *Z. H.* A complete key recovery timing attack on a GPU. / Z. H. Jiang, Y. Fei, D. R. Kaeli // HPCA. — IEEE Computer Society, 2016. — С. 394—405. — URL: http://dblp.uni-trier.de/db/conf/hpca/hpca2016.html#JiangFK16.

40. *Jiang*, *Z. H.* Exploiting Bank Conflict-based Side-channel Timing Leakage of GPUs. / Z. H. Jiang, Y. Fei, D. R. Kaeli // TACO. — 2020. — Т. 16, № 4. — 42:1—42:24. — URL: http://dblp.uni-trier.de/db/journals/taco/taco16.html#JiangFK20.

41. A Timing Side-Channel Attack on a Mobile GPU. / E. Karimi, Z. H. Jiang, Y. Fei [и др.] // ICCD. — IEEE Computer Society, 2018. — С. 67—74. — URL: http://dblp.uni-trier.de/db/conf/iccd/iccd2018.html#KarimiJFK18.

42. *Kipper*, *M. S.* Implementing AES on GPU: Final Report / M. S. Kipper, J. Slavkin, D. Denisenko //. — 2011.

43. *Knudsen*, *L. R.* Non-Linear Approximations in Linear Cryptanalysis / L. R. Knudsen, M. J. B. Robshaw // Advances in Cryptology — EUROCRYPT '96 / под ред. U. Maurer. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1996. — С. 224—236.

44. *Kocher*, *P. C.* Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems / P. C. Kocher // Lecture Notes in Computer Science. — 1996. — Т. 1109. — С. 104—113. — URL: citeseer.ist.psu.edu/kocher96timing.html.

45. A performance prediction model for the CUDA GPGPU platform / K. Kothapalli, R. Mukherjee, M. S. Rehman [и др.] // 2009 International Conference on High Performance Computing (HiPC). — 2009. — С. 463—472.

46. *Krasovsky*, *A. V.* Actual and Historical State of Side Channel Attacks Theory / A. V. Krasovsky, E. A. Maro // Proceedings of the 12th International Conference on Security of Information and Networks. — Sochi, Russia : Association for Computing Machinery, 2019. — (SIN '19). — URL: https://doi.org/10.1145/3357613.3357627.

47. *Kundi*, *D.-e.-S.* Implementation of T-box/T-1-Box Based AES Design on Latest Xilinx FPGA / D.-e.-S. Kundi, A. Aziz // Mehran University Research Journal of Engineering & Technology ISSN 0254-7821. — 2015. — Окт. — Т. 34. — С. 441—446.

48. *Kutzner*, *S.* Enabling 3-Share Threshold Implementations for all 4-Bit S-Boxes. / S. Kutzner, P. H. Nguyen, A. Poschmann // ICISC. Т. 8565 / под ред. H.-S. Lee, D.-G. Han. — Springer, 2013. — С. 91—108. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/icisc/icisc2013.html#KutznerNP13.

49. *Leander*, *G.* On Invariant Attacks / G. Leander //. — 2019. — Invited talk.

50. *Lim*, *C. H.* A Revised Version of Crypton - Crypton V1.0. / C. H. Lim // FSE. Т. 1636 / под ред. L. R. Knudsen. — Springer, 1999. — С. 31—45. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse99.html#Lim99.

51. *Lim*, *C. H.* CRYPTON: A New 128-bit Block Cipher - Specification and Analysis / C. H. Lim. — 1998.

52. *Lo*, *O.* Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device. / O. Lo, W. J. Buchanan, D. Carson // ARES / под ред. S. Doerr, M. Fischer, S. Schrittwieser [и др.]. — ACM, 2018. — 21:1—21:6. — URL: http://dblp.uni-trier.de/db/conf/IEEEares/ares2018.html#LoBC18.

53. *Matsuda*, *S.* Lightweight Cryptography for the Cloud: Exploit the Power of Bitslice Implementation. / S. Matsuda, S. Moriai // CHES. Т. 7428 / под ред. E. Prouff, P. Schaumont. — Springer, 2012. — С. 408—425. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/ches/ches2012.html#MatsudaM12.

54. *Matsui*, *M.* New Block Encryption Algorithm MISTY. / M. Matsui // FSE. Т. 1267 / под ред. E. Biham. — Springer, 01.01.2008. — С. 54—68. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse97.html#Matsui97.

55. *Matsui*, *M.* The First Experimental Cryptanalysis of the Data Encryption Standard. / M. Matsui // CRYPTO. Т. 839 / под ред. Y. Desmedt. — Springer, 1994. — С. 1—11. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/crypto/crypto94.html#Matsui94.

56. *Menyachikhin, A. V.* Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters / A. V. Menyachikhin // Математические вопросы криптографии. — 2017. — Т. 8, № 2. — С. 97—116.

57. Mixed Bases for Efficient Inversion in F((22)2)2 and Conversion Matrices of SubBytes of AES. / Y. Nogami, K. Nekado, T. Toyota [и др.] // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. — 2011. — Т. 94—A, № 6. — С. 1318—1327. — URL: http://dblp.uni-trier.de/db/journals/ieicet/ieicet94a.html#NogamiNTHM11.

58. *Nishikawa, N.* Implementation of Bitsliced AES Encryption on CUDA-Enabled GPU / N. Nishikawa, H. Amano, K. Iwai // Network and System Security / под ред. Z. Yan, R. Molva, W. Mazurczyk [и др.]. — Cham : Springer International Publishing, 2017. — С. 273—287.

59. Mixed Bases for Efficient Inversion in $\mathbb{F}((2^2)^2)2$ and Conversion Matrices of SubBytes of AES / Y. Nogami, K. Nekado, T. Toyota [и др.] //. — 08.2010. — С. 234—247.

60. *NVIDIA Corporation*. NVIDIA CUDA C Programming Guide. Design Guide / NVIDIA Corporation. — 2022. — URL: https://docs.nvidia.com/cuda/pdf/CUDA_C_Programming_Guide.pdf ; Version 11.8.

61. *Olofsson, M.* VLSI Aspects on Inversion in Finite Fields : дис. … канд. / Olofsson Mikael. — 02.2002.

62. *Perrin, L.* Cryptanalysis, Reverse-Engineering and Design of Symmetric Cryptographic Algorithms. : дис. … канд. / Perrin Léo. — University of Luxembourg, 2017.

63. *Perrin, L.* Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem (Full Version). / L. Perrin, A. Udovenko, A. Biryukov // IACR Cryptology ePrint Archive. — 2016. — Т. 2016. — С. 539. — URL: http://dblp.uni-trier.de/db/journals/iacr/iacr2016.html#PerrinUB16 ; http://eprint.iacr.org/2016/539.

64. *Raddum, H.* Algebraic Analysis of the Simon Block Cipher Family / H. Raddum //. Т. 9230. — 08.2015. — С. 157—169.

65. *Rebeiro*, *C.* Bitslice Implementation of AES / C. Rebeiro, D. Selvakumar, A. S. L. Devi // Cryptology and Network Security / под ред. D. Pointcheval, Y. Mu, K. Chen. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. — С. 203—212.

66. *Rijmen*, *V.* The KHAZAD Block Cipher / V. Rijmen, P. Barreto. — 2000.

67. *Rudell*, *R.* Multiple-Valued Logic Minimization for PLA Synthesis / R. Rudell // Technical report, EECS Department, University of California, Berkeley. — 1986.

68. Rolled architecture based implementation of AES using T-Box / P. V. S. Shastry, N. Somani, A. Gadre [и др.] //. — 08.2012. — С. 626—630.

69. Side-channel power analysis of a GPU AES implementation / C. Luo, Y. Fei, P. Luo [и др.] // 2015 33rd IEEE International Conference on Computer Design (ICCD). — 2015. — С. 281—288.

70. *Stallings*, *W.* The Whirlpool Secure Hash Function. / W. Stallings // Cryptologia. — 2008. — 23 июля. — Т. 30, № 1. — С. 55—67. — URL: http://dblp.uni-trier.de/db/journals/cryptologia/cryptologia30.html#Stallings06.

71. ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. / F.-X. Standaert, G. Piret, G. Rouvroy [и др.] // FSE. Т. 3017 / под ред. B. K. Roy, W. Meier. — Springer, 2004. — С. 279—299. — (Lecture Notes in Computer Science). — URL: http://dblp.uni-trier.de/db/conf/fse/fse2004.html#StandaertPRQL04.

72. *Sun*, *B.* New Cryptanalysis of Block Ciphers with Low Algebraic Degree / B. Sun, L. Qu, C. Li // Fast Software Encryption / под ред. O. Dunkelman. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2009. — С. 180—192.

73. Highly efficient GF(28) inversion circuit based on hybrid GF representations. / R. Ueno, N. Homma, Y. Nogami [и др.] // J. Cryptographic Engineering. — 2019. — Т. 9, № 2. — С. 101—113. — URL: http://dblp.uni-trier.de/db/journals/jce/jce9.html#UenoHNA19.

74. Finding Optimal Bitsliced Implementations of 4 x 4-bit S-boxes / M. Ullrich, C. D. Cannière, S. Indesteege [и др.]. — 2011. — Ecrypt II.

75. *Zhou*, *Y.* Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing / Y. Zhou, D. Feng. — 2005. — URL: http://eprint.iacr.org/2005/388.

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

77. *Комиссаров*, *С. М.* Об алгоритмической реализации s-боксов 16x16 со структурами ARX и «Бабочка» / С. М. Комиссаров // Прикладная дискретная математика. Приложение. — 2019. — Т. 12. — С. 101—107.

78. *Малышев*, *Ф. М.* Методы линейных и разностных соотношений в криптографии / Ф. М. Малышев // Дискрет. матем. — 2022. — Т. 34, № 1. — С. 36—63.

79. *Малышев*, *Ф. М.* Линейный и разностный методы в криптографии (другой взгляд) / Ф. М. Малышев, А. Е. Тришин //. — 2018. — С. 42—45.

80. *Чичаева*, *А. А.* Поиск эффективно реализуемых подстановок с оптимальными криптографическими характеристиками / А. А. Чичаева // Рускрипто 2021. — 2021.

Публикации автора по теме диссертации

81. *Fomin*, *D. B.* A timing attack on CUDA implementations of an AES-type block cipher / D. B. Fomin // Математические вопросы криптографии. — 2016. — Т. 7, № 2. — С. 121—130.

82. *Fomin*, *D. B.* New Classes of 8-bit Permutations Based on a Butterfly Structure / D. B. Fomin // Математические вопросы криптографии. — 2019. — Т. 10, № 2. — С. 169—180.

83. *Fomin*, *D. B.* On the impossibility of an invariant attack on Kuznyechik / D. B. Fomin // Journal of Computer Virology and Hacking Techniques. — 2022. — Т. 18, № 1. — С. 61—67.

84. *Kovrizhnykh*, *M. A.* On differential uniformity of permutations derived using a generalized construction / M. A. Kovrizhnykh, D. B. Fomin // Математические вопросы криптографии. — 2022. — Т. 13, № 2. — С. 37—52.

85. Об одном представлении нелинейного преобразования алгоритма «Кузнечик» с помощью логических функций / О. Д. Авраамова, Д. Б. Фомин, В. А. Серов [и др.] // Математические вопросы криптографии. — 2021. — Т. 12, № 2. — С. 21—38.

86. *Коврижных*, *М. А.* Об эвристическом алгоритме построения подстановок с заданными криптографическими характеристиками с использованием обобщённой конструкции / М. А. Коврижных, Д. Б. Фомин // Прикладная дискретная математика. — 2022. — Т. 57. — С. 5—21.

87. *Коврижных*, *М. А.* Об эвристическом подходе к построению биективных векторных булевых функций с заданными криптографическими характеристиками / М. А. Коврижных, Д. Б. Фомин // Прикладная дискретная математика. Приложение. — 2021. — Т. 14. — С. 181—184.

88. *Трифонов*, *Д. И.* Об инвариантных подпространствах в XSL-шифрах / Д. И. Трифонов, Д. Б. Фомин // Прикладная дискретная математика. — 2021. — Т. 54. — С. 58—76.

89. *Фомин*, *Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований / Д. Б. Фомин // Обозрение прикладной и промышленной математики. — 2018. — Т. 25, № 4. — С. 379—381.

90. *Фомин*, *Д. Б.* О способе построения дифференциально 2δ-равномерных подстановок на $\mathbb{F}_{2^{2m}}$ / Д. Б. Фомин // Прикладная дискретная математика. Приложение. — 2021. — Т. 14. — С. 51—55.

91. *Фомин*, *Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m,m)$-функций / Д. Б. Фомин // Математические вопросы криптографии. — 2020. — Т. 11, № 4. — С. 133—149.

92. *Фомин*, *Д. Б.* Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций / Д. Б. Фомин // Математические вопросы криптографии. — 2020. — Т. 11, № 3. — С. 121—138.

93. *Фомин*, *Д. Б.* Об аппаратной реализации одного класса байтовых подстановок / Д. Б. Фомин, Д. И. Трифонов // Прикладная дискретная математика. Приложение. — 2019. — Т. 12. — С. 134—137.