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

На правах рукописи

Высоцкая Виктория Владимировна

Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки

2.3.6. Методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
кандидат физико-математических наук
Чижов Иван Владимирович

Москва – 2025

Оглавление

Введение 4

Обозначения, определения и общие сведения 26

1. Сведения из общей алгебры 26
2. Линейные коды 27
3. Дуальные коды 30
4. Задачи на кодах 32
5. Квазициклические коды 33
6. Коды Рида–Маллера 34
7. Обобщенные коды Рида–Соломона 36
8. Электронная подпись CFS 38

Глава 1. Свойства ключей электронной подписи CFS на основе подкодов кодов Рида–Маллера 48

1.1. Электронная подпись на подкодах кодов $\mathsf{RM}(2, m)$ 48

1.2. Электронная подпись на подкодах кодов $\mathsf{RM}(r, m)$ 53

1.3. Доля нестабильных подкодов кодов $\mathsf{RM}(r, m)$ 60

1.4. Выводы к первой главе 65

Глава 2. Генерация ключей в электронной подписи CFS на основе квазициклических кодов 67

2.1. Дополнительные определения 68

2.2. О связях матриц многочленов, квазициклических матриц и матриц весов 70

2.3. Оценка доли обратимых матриц 73

2.4. Приведение матрицы к треугольной форме 80

2.5. Построение случайной обратимой матрицы 84

2.6. Выводы ко второй главе 92

Глава 3. Структура ключей электронной подписи CFS на основе конструкции Сидельникова 94

3.1. Дополнительные определения 95

3.2. Пространство ключей подписи CFS на основе конструкции Сидельникова на линейных кодах общего вида 95

3.3. Пространство ключей подписи CFS на основе конструкции Сидельникова на кодах, основанных на OPC и имеющих разложимый квадрат 104

3.4. Неразложимость квадратов кодов на основе OPC 106

3.5. Выводы к третьей главе 115

Глава 4. Построение стойкой схемы подписи на основе кодов общего типа 117

4.1. Синтез схемы подписи 118

4.2. Обоснование стойкости новой схемы подписи 121

4.3. Выводы к четвертой главе 144

Заключение 146

Список литературы 148

Приложение А. Программная реализация Алгоритма 1 157

Введение

Общая характеристика работы. Диссертация посвящена исследованию методов построения электронных подписей на основе кодов, исправляющих ошибки. Электронные подписи представляют собой неотъемлемый элемент современных криптографических протоколов, обеспечивая гарантии целостности данных, аутентификации отправителя и невозможности отказа от авторства. Применение кодов, исправляющих ошибки, в схемах электронной подписи является перспективным направлением, поскольку такие схемы обладают потенциальной устойчивостью к атакам с использованием квантовых вычислений.

Синтез схем электронной подписи, а также выбор соответствующих классов кодов и их параметров представляют собой значимые задачи как с теоретической, так и с прикладной точки зрения в контексте обеспечения криптографической стойкости. Эксплуатационные характеристики разработанных схем, включая скорость вычисления, объем хранимых данных и уровень криптографической стойкости, зависят как от используемой схемы подписи, так и от свойств применяемых классов кодов. Обоснованный выбор параметров, основанный на оценках криптостойкости или ориентированный на противодействие известным атакам, позволяет формировать защищенные криптографические системы.

Одновременно с этим для оценки устойчивости к возможным атакам схем электронной подписи требуется детальный математический анализ структуры и свойств различных классов кодов, исправляющих ошибки. В рамках данного анализа формулируются и доказываются строгие математические утверждения, имеющие самостоятельную значимость не только в области криптографии, но и в теории кодирования. Методы формального обоснования криптографической стойкости опираются на аппарат теории вероятностей, теории кодирования и алгебраических методов.

Диссертация содержит анализ характеристик схем электронной подписи

в зависимости от класса используемых базовых кодов. Полученные результаты могут быть использованы при выборе и стандартизации криптографических схем с открытым ключом, основанных на кодах, исправляющих ошибки. Кроме того, разработана новая схема электронной подписи, криптографическая стойкость которой не зависит от конкретного типа корректирующих кодов. В настоящее время схема проходит процедуру стандартизации в качестве постквантового стандарта электронной подписи Российской Федерации.

Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6. (Методы и системы защиты информации, информационная безопасность, физико-математические науки) по направлению:

11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

В рамках исследования применяется математический аппарат и подходы различных разделов математики, таких как теория кодирования, комбинаторная теория вероятностей, теория алгоритмов, теория сложности вычислений, теория графов.

Актуальность. Стойкость стандартизованных криптографических алгоритмов, используемых по всему миру, основана на сложности нескольких задач из теории чисел. Обычно это задачи дискретного логарифмирования или факторизации. Однако в 1994 году П. Шор показал [1], что квантовые компьютеры могут взломать все схемы, построенные таким образом. В 2001 году алгоритм Шора был реализован на квантовом компьютере с 7 кубитами [2]. С тех пор стали разрабатываться все более и более мощные квантовые компьютеры, что

представляет реальную угрозу современной криптографии с открытым ключом.

Существует несколько областей, на которых могут основываться постквантовые криптографические схемы. Примерами таких областей являются целочисленные решетки, коды, исправляющие ошибки, хэш-функциии, многомерные квадратичные системы, а также симметричное шифрование и шифрование на основе изогений эллиптических кривых. Тем не менее построенные схемы требуют исследования стойкости, в том числе к атакам с использованием квантовых компьютеров.

Сложные задачи, на которых основаны постквантовые схемы, хуже изучены по сравнению с теми, что лежат в основе классических криптосистем. Поэтому вероятность успешной атаки на новые схемы выше. Однако среди атак на квантовых компьютерах лучшую оценку дает алгоритм Гровера [3], и эта оценка корневая. Поэтому постквантовые схемы внушают больше доверия, нежели классические, подверженные полиномиальным атакам Шора. При этом некоторые задачи, считающиеся постквантовыми, оказываются нестойкими даже к атакам на классических компьютерах. Так, например, базовая задача SIDH на изогениях, которая некоторое время считалась сложной, была атакована в работе [4]. Это, в свою очередь, свидетельствует об отсутствии стойкости схем, доказательства безопасности которых сводились к сложности этой задачи. Так что в настоящее время остро стоит задача поиска лучшего подхода.

Коды, исправляющие ошибки, как математический объект имеют историю длиною более 70-ти лет. Однако с точки зрения криптографии они стали рассматриваться только спустя десятилетия, после предложения в 1978 году Робертом Мак-Элисом своей криптосистемы [5]. Но даже после этого долгое время не было попыток стандартизовать кодовые схемы. Наконец в 2016 году Национальный Институт Стандартов и Технологий США (NIST) [6] объявил открытый конкурс на новый постквантовый стандарт США. В этом конкурсе участвовали алгоритмы шифрования с открытым ключом, схемы цифровых подписей и

схемы распределения ключей, среди которых были и варианты, построенные на кодах.

Результаты получились неоднозначными. Большое число поданных схем оказались подвержены атакам на классическом вычислителе. Среди них были и все 3 схемы электронной подписи на кодах, исправляющих ошибки [7]: pqsigRM [8], RaCoSS-R [9], RankSgn [10]. Первая была позже доработана [11], но все равно оказалась уязвимой. Другие схемы, которые остаются стойкими, имеют неоптимальные эксплуатационные параметры и потенциально могут быть атакованы в будущем.

Поэтому, несмотря на объявление победителей, параллельно был запущен еще один дополнительный конкурс, нацеленный исключительно на алгоритмы электронной подписи. Уже к июлю 2023 года был опубликован список из 40 новых претендентов. Схем на кодах, исправляющих ошибки, на первом раунде было 6: CROSS [12], Enhanced pqsigRM [13], FuLeeca [14], LESS [15], MEDS [16] и Wave [17]. Схемы CROSS и LESS прошли во 2 раунд и имеют возможность в дальнейшем быть стандартизованными.

Параллельно с конкурсом NIST в России также начался процесс выбора постквантовой схемы электронной подписи. Схемы на основе кодов были выбраны Техническим комитетом по стандартизации «Криптографические и защитные механизмы» (ТК 26) [18] как одно из направлений разработки проектов российских национальных стандартов постквантовых криптографических алгоритмов. Диссертационная работа мотивирована задачами, которые возникли в процессе работ, проводимых в рамках ТК 26.

Помимо России, процессы по выбору и стандартизации постквантовых алгоритмов идут и в других странах. Так, например, в 2021–2025 годах в Южной Корее проводился конкурс KpqC [19]. Аналогичные инициативы реализуются и в рамках международных организаций по стандартизации, таких как ISO [20] и IETF [21].

Исторически синтез электронной подписи на основе кодов продвигался не

очень удачно. На протяжении длительного времени атаки на все предложенные схемы подписей строились столь быстро, что возникло опасение, что такие схемы вообще невозможно создать [22]. Одним из первых успешных вариантов можно назвать схему KKS, которая была предложена Г. Кабатянским, Е. Круком и Б. Смитом в 1997 году [23]. Однако, согласно дальнейшим исследованиям [24], схема является стойкой только при одноразовом использовании.

Прорывом стало предложение Н. Куртуа, М. Финиаша и Н. Сендриера инвертировать порядок алгоритмов в схеме шифрованя, то есть использовать алгоритм расшифрования в качестве алгоритма генерации подписи и шифрования для ее проверки. Эта идея была представлена в 2001 году и в дальнейшем получила название CFS [25]. Позже Л. Далло предложил доказуемо стойкую версию этой подписи, известную как mCFS [26]. В диссертации эти схемы отождествлены под названием CFS.

Классическими примерами схем шифрования на основе кодов являются криптосистемы Р. Мак-Элиса [5] и Х. Нидеррайтера [27]. В первом случае код задан своей порождающей, а во втором — проверочной матрицей. Соответственно, стойкость схем первого типа сводится к сложности решения задачи декодирования, а второго типа — к сложности задачи синдромного декодирования. Эти задачи эквивалентны по сложности, таким образом схемы на них эквивалентны по уровню стойкости.

Задачи декодирования и синдромного декодирования для кодов общего вида являются NP-полными как задачи разрешимости и NP-трудными как задачи поиска [28; 29]. Это гарантирует стойкость криптографических схем, построенных на таких кодах. Также пока остаются стойкими схемы, построенные с использованием кодов, которые предложил В. Д. Гоппа [30].

Однако в общем случае криптосистемы на основе выделенных классов линейных кодов могут быть подвержены атакам, поскольку замена кода приводит к модификации постановки задачи. Поэтому при синтезе схем на кодах, исправляющих ошибки, обычно выбирают базовый код с эффективным алгоритмом

декодирования, но маскируют его под код общего вида, все известные алгоритмы для которого экспоненциальны. Маскировка может осуществляться при помощи умножения на одну (криптосистема Богданова–Ли [31]) или две матрицы (криптосистемы Мак-Элиса [5] и Нидеррайтера [27]), которые становятся частью секретного ключа криптосистемы.

Тем не менее, известны случаи, когда секретный ключ такого вида (или эквивалентный ему) удавалось восстановить по открытым данным. Так была атакована криптосистема Мак-Элиса на кодах Рида–Маллера [32; 33]. Известны атаки на эту же криптосистему на кодах Рида–Соломона [34; 35]. Проблемы со стойкостью оказались и у вариантов на основе других классов кодов [36—39].

Одним из подходов к дополнительному сокрытию структуры кода с сохранением его эффективности является переход к некоторому его подкоду. При этом стоит учитывать, что многие предложенные системы на основе подкодов также оказались уязвимыми. Так, в работах [40; 41] К. Вишебринк построил эффективные атаки на некоторые особые случаи криптосистемы Бергера–Луадро [42], основанной на подкодах кодов Рида–Соломона. Криптосистема Мак-Элиса, построенная на подкодах алгебраических геометрических кодов, была атакована в [36]. А в работе [37] И. Чижову и М. Бородину удалось редуцировать стойкость криптосистемы на подкодах кодов Рида–Маллера коразмерности один до стойкости схемы на полных кодах, где под коразмерностью понимается количество векторов, отсутствующих в базисе кода. Тем не менее аналогичных результатов для подкодов кодов Рида–Маллера больших коразмерностей получено не было.

Еще одним способом усиления стойкости схемы с сохранением структуры кодов является вариант, предложенный в 1994 году В. Сидельниковым [43] для кодов Рида–Маллера. Криптосистемы такого типа используют не одну, а несколько копий кода. Матрицы таких кодов объединены по столбцам. Несмотря на то, что этот подход позволил избежать прямого переноса атак, направленных на вариант с одной копией кода Рида–Маллера, в работе [44] был пред-

ложен специальный алгоритм восстановления секретного ключа и для модифицированной схемы. Работы [45] и [46] решают эту же задачу для варианта криптосистемы, в которой используются одновременно код Рида–Маллера и линейный код общего вида. Приведенные атаки работают при выполнении типичного условия, которое, согласно работе [47], будет выполнено для случайного кода с вероятностью близкой к 1. Однако полностью вопрос применимости конструкции Сидельникова не закрыт, поскольку она не была доисследована для других классов кодов, для которых могут найтись потенциально стойкие коды специального вида.

Выбор класса кодов может существенно улучшить эффективность схемы. Так квазициклические коды позволяют критически сократить размер открытого ключа, поскольку для хранения каждой циклической подматрицы достаточно хранения одной ее строки. Такой подход был отражен в рамках конкурса NIST в схемах QC-MDPC [48] и LEDAcrypt [49], предлагающих схемы шифрования и механизм инкапсуляции ключа на кодах со средней и малой плотностью проверок на четность (QC-MDPC и QC-LDPC кодах, соответственно). Первая схема в первый же год подверглась атаке по времени, восстанавливающей секретный ключ за $O(2^{28})$ битовых операций вместо $O(2^{256})$ заявленных. Вторая работа дошла до второго раунда конкурса, но далее была отклонена из-за появления работы [50], обнаружившей большой класс слабых ключей, уязвимых к раскрытию. Еще две схемы, эксплуатировавшие квазициклическую структуру кодов, BIKE [51] и HQC [52], дошли до 4 раунда конкурса, а модифицированная версия последней [53] в 2025 году стала победителем.

В 2020 году на конференции CTCrypt'20 было высказано предложение [54] использовать QC-LDPC-коды для построения электронной подписи. Для решения этой задачи авторы работы подставили алгоритм генерации квазициклических ключей из схемы [55] в классическую схему подписи CFS. Однако изменение параметров для адаптации схемы шифрования под схему подписи привело к росту параметров, для которых выросло время внутреннего алгоритма гене-

рации вспомогательной невырожденной квазициклической матрицы. Оптимизация этого алгоритма могла бы поспособствовать повышению эффективности всей схемы подписи.

Другой подход к построению схемы электронной подписи на кодах, исправляющих ошибки, заключается в применении преобразования Фиата–Шамира [56] к некоторому протоколу идентификации. В качестве такого протокола можно использовать схемы Я. Штерна [57], А. Джаина и др. [58], CVE [59] и прочие. Такой подход позволяет отказаться от использования алгоритма декодирования, что дает возможность использовать в схеме произвольный линейный код, а не ограничиваться узкими классами кодов с эффективными алгоритмами декодирования.

Несмотря на то, что подпись на основе схемы идентификации Штерна неоднократно упоминалась в литературе, ее полное описание до сих пор не было представлено. Например, в обзоре Р. Овербека и Н. Сендриера [60] лишь отмечена возможность построения такой подписи, но сам алгоритм не приведен. В работе [61] схема сформулирована с ошибкой, что приводит к значительному снижению уровня стойкости по сравнению с ожидаемым значением. Корректное, но краткое описание схемы можно найти в [62].

Обоснование стойкости такой схемы подписи упоминается в работе Д. Пуаншеваля и Я. Штерна [63]. В этой статье представлена так называемая лемма разветвления (Forking lemma). Авторы утверждают ее применимость к доказательству стойкости подписи Штерна, однако этот факт не был доказан ни в данной работе, ни в последующих. При этом наличие доказательства стойкости позволило бы существенно продвинуть исследования в области построения схем электронной подписи на основе кодов, исправляющих ошибки. Это связано с тем, что стойкость такой электронной подписи не только исключает возможность структурных атак, но и строго сводится к исходной NP-трудной задаче.

Цели и задачи диссертационной работы: анализ методов построения схем электронной подписи на основе кодов, исправляющих ошибки, путем иссле-

дования их структурных свойств, а также рассмотрение подходов, не зависящих от конкретного класса кодов.

Для достижения поставленной цели были решены следующие задачи:

1. исследовать стойкость электронной подписи CFS на подкодах кодов Рида–Маллера;
2. исследовать возможность эффективного построения электронной подписи CFS на основе квазициклических кодов;
3. исследовать стойкость электронной подписи CFS на основе конструкции Сидельникова;
4. разработать новую схемы электронной подписи на основе кодов, исправляющих ошибки, стойкость которой не зависела бы от структуры используемого кода.

Положения, выносимые на защиту:

1. Метод описания структурных свойств подкодов кода Рида–Маллера, схема подписи CFS на которых является стойкой к известному типу атак. Способы построения таких подкодов и метод оценки их доли.
2. Два эффективных алгоритма построения невырожденных квазициклических матриц, необходимых для эффективной реализации схемы подписи CFS на квазициклических кодах.
3. Метод получения нижней оценки мощности множества открытых ключей схемы подписи CFS, построенной на основе конструкции Сидельникова. Описание структуры множества секретных ключей на кодах общего вида и обобщенных кодах Рида–Соломона, схема подписи на которых подвержена атакам, разделяющим копии кода. Метод построения секретных ключей подписи CFS с использованием обобщенных кодов Рида–Соломона, позволяющий избежать известных атак.

4. Схема электронной подписи, стойкость которой не зависит от сложности задач на известном классе кодов. Обоснование стойкости построенной подписи.

Научная новизна. В диссертации получены следующие новые результаты.

1. Описаны структурные свойства подкодов кода Рида–Маллера $RM(2, m)$, устойчивых к атакам, применимым к полному коду. Описаны структурные свойства подкодов кода $RM(r, m)$, обеспечивающих стойкость к известным структурным атакам на полный код, и построен алгоритм их генерации. Получена оценка доли стойких подкодов кода $RM(r, m)$ с ростом параметра m.

2. Доказаны связи между невырожденностью квазициклической матрицы, соответствующей матрицы над факторкольцом $\mathbb{F}_2[x]/(x^r - 1)$ и матрицы, состоящей из весов соответствующих многочленов. Получены нижние оценки доли невырожденных матриц среди всех матриц заданного размера над факторкольцом $\mathbb{F}_2[x]/(f(x))$. Разработаны эффективные алгоритмы вычисления определителя над факторкольцом $\mathbb{F}_2[x]/(f(x))$ и алгоритм генерации невырожденных матриц с равномерным распределением на множестве всех невырожденных матриц заданного размера. Предложена и теоретически обоснована специализированная версия алгоритма генерации для случая, когда $f(x) = x^r - 1$.

3. Получена оценка снизу на мощность множества открытых ключей схемы подписи CFS, построенной на основе конструкции Сидельникова. Описана структура классов эквивалентности секретных ключей схемы через группы автоморфизмов линейного кода и его квадрата. Уточнена структура классов эквивалентности для случая, когда в схеме используется обобщенный код Рида–Соломона. Выделены три класса ключей схемы подписи,

такие что квадрат кода, задающего открытый ключ, не раскладывается в прямое произведение квадратов базовых кодов.

4. Построена схема электронной подписи на основе протокола идентификации Штерна. Доказана теорема о стойкости подписи к экзистенциальной подделке при атаке с выбором сообщения (модель EUF-CMA).

Публикации по теме исследования.

Основные результаты диссертационной работы опубликованы в 5 печатных работах (общим объемом 4.88 п.л.), из них 4 работы (объемом 4.69 п.л.) в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index».

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index»:

[64] Vysotskaya V. Characteristics of Hadamard Square of Special Reed–Muller Subcodes // Прикладная дискретная математика. – 2021. – №– 53. С. 75–88. – EDN: TEDEFN.

0.88 п.л., Scopus, RSCI, импакт-фактор 0.11 (JCI).

[65] Высоцкая В. В., Высоцкий Л. И. Обратимые матрицы над некоторыми факторкольцами: идентификация, построение и анализ // Дискретная математика. 2021. – Т. 33. – №2. – С. 46–65. – EDN: VASNIG.

1.25 п.л., RSCI, импакт-фактор 0.39 (РИНЦ).

Соавтору принадлежит алгоритм приведения матрицы над факторкольцом кольца многочленов к верхнетреугольному виду (Алгоритм 1 по тексту статьи), остальные результаты статьи получены Высоцкой В. В., 90%, 1.06 п.л.

На англ. языке: Vysotskaya V., Vysotsky L. Invertible matrices over some quotient rings: identification, generation, and analysis // Discrete Mathematics and Applications. – 2022. – 32(4). – pp. 263–278. – EDN: EDHYGI.
1 п.л., вклад автора 90%, 0.94 п.л., Scopus, WoS, импакт-фактор 0.22 (JCI).

[66] Высоцкая В. В. О структурных особенностях пространства ключей криптосистемы Мак-Элиса–Сидельникова на обобщенных кодах Рида–Соломона // Дискретная математика. – 2024. – Т. 36. №4. – С. 28–43. – EDN: IBRMIU.
1 п.л., RSCI, импакт-фактор 0.39 (РИНЦ).

[67] Vysotskaya V., Chizhov I. The security of the code-based signature scheme based on the Stern identification protocol // Прикладная дискретная математика. 2022. – №57. – С. 67–90. – EDN: FFRFUH.
1.56 п.л., Scopus, RSCI, импакт-фактор 0.11 (JCI).
Соавтору принадлежит постановка задачи и верификация результатов, остальные результаты статьи получены Высоцкой В. В., 95%, 1.56 п.л.

В прочих изданиях:

[68] Vysotskaya V. New estimates for dimension of Reed–Muller subcodes with maximum Hadamard square // Прикладная дискретная математика. Приложение. – 2020. – №13. – С. 98–100. – EDN: TCYZCI.
0.19 п.л., ВАК, импакт-фактор 0.06 (РИНЦ).

Апробация результатов. Результаты, полученные в диссертации, докладывались на международных конференциях и научно-исследовательских семинарах:

- семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2020 год;

- IX международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2020), Московская область, 15–17 сентября, 2020 год;

- международной научно-практической конференции РусКрипто 2021, Солнечногорск, 23–26 марта, 2021 год;
- научном семинаре кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2021 год;
- научном семинаре кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2022 год;
- XIII международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2024), Петрозаводск, 3–6 июня, 2024 год.

Теоретическая значимость. Проведенное исследование позволило получить результаты, углубляющие математические подходы к построению и обоснованию стойкости криптографических схем, основанных на кодах, исправляющих ошибки.

В рамках изучения схемы электронной подписи CFS, основанной на подкодах кодов Рида–Маллера, был проведен анализ структуры квадратов Адамара этих подкодов путем сведения задачи к задаче из теории графов. Анализ комбинаторных свойств позволил оценить долю подкодов, которые не подвержены известным атакам. Совокупность полученных результатов обеспечила формализованное описание структурных характеристик подкодов, применение которых в данной криптографической схеме обеспечивает стойкость за счет отличия от полного кода Рида–Маллера и сохраняет эффективность благодаря унаследованному алгоритму декодирования.

Применение теории полей и фактор-колец позволило провести расширенное исследование линейных свойств квазициклических матриц, представляющих интерес в силу обеспечиваемого ими существенного сокращения размера открытого ключа в схеме электронной подписи CFS. Полученные резуль-

таты наряду с анализом комбинаторных характеристик множества квазициклических матриц позволили разработать эффективные алгоритмы генерации ключей этой схемы.

Исследование алгебраических свойств конкатенированных кодов позволило, с одной стороны, получить оценки мощности множества открытых ключей соответствующей схемы электронной подписи CFS, а с другой — описать структуру множества секретных ключей. Особенности строения обобщенных кодов Рида–Соломона дали возможность уточнить полученные результаты и выделить подклассы секретных ключей, обладающих стойкостью к известным атакам.

Схема электронной подписи на основе протокола идентификации Штерна была синтезирована с целью преодоления ограничений подходов, в которых криптографическая стойкость существенно зависит от структуры используемого кода. Основной задачей являлось построение схемы, для которой возможно строгое обоснование стойкости, не опирающееся на практические знания о существующих атаках. Обоснование оценки уровня стойкости разработанной конструкции опирается на методы сведения к вычислительно сложным задачам и вероятностные оценки, применяемые в соответствующих моделях нарушителя.

Практическая значимость. Внедрение разработанной в диссертации схемы электронной подписи в средства защиты информации решает практическую задачу обеспечения аутентификации и целостности сообщения, подтверждения авторства и неотказуемости от него в таких прикладных системах, как службы электронной почты, облачные хранилища, системы электронного документооборота, мессенджеры и другие системы асинхронной передачи сообщений, а также распределенные реестры и блокчейн-платформы. Особая актуальность предлагаемого решения обусловлена их стойкостью к атакам, реализуемым с использованием квантовых вычислений. Полученные обоснованные оценки уровня информационной безопасности позволяют осуществлять выбор безопасных значений параметров.

Полученные результаты, связанные с анализом использования специальных классов кодов в схеме подписи CFS, позволяют обоснованно оценить их применимость с точки зрения криптографической стойкости и вычислительной эффективности, а также выработать практические рекомендации для реализаций на их основе. Результаты диссертации также могут войти в состав учебных пособий и быть частью лекционных курсов.

Разработанная схема подписи на основе схемы идентификации Штерна рассматривается в Техническом комитете 26 как вариант будущего постквантового стандарта.

Структура и объем диссертации. Диссертационная работа состоит из введения, вспомогательного раздела, четырех глав, заключения, списка литературы и одного приложения. Общий объем диссертации 159 страниц, включая 6 рисунков, 4 таблицы, 4 алгоритма и 1 приложение. Список литературы включает 84 наименования на 9 страницах.

Содержание работы.

Во **Введении** обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

Раздел **Обозначения, определения и общие сведения** устанавливает основные обозначения и формулирует определения, относящиеся к теории кодов, исправляющих ошибки. В нем вводятся понятия линейной зависимости и обратимости матриц в кольце, а также перечислены некоторые специальные виды матриц.

Формулируются определения линейных и дуальных кодов, их параметров, способов задания и операций над ними. Задаются классы кодов, которые (или производные от которых) изучаются в рамках диссертационной работы: квазициклические коды, коды Рида–Маллера, обобщенные коды Рида–Соломона. Также приведены некоторые сведения о этих кодах и их свойства.

Приведена формальная модель протокола электронной подписи, изложено описание оригинальной схемы CFS [25], а также рассмотрены особенности ее построения в случае использования квазициклических кодов вместо кодов Гоппы и при формировании ключей на основе конструкции Сидельникова. Описан протокол идентификации Штерна [57], который может быть использован в качестве основы для построения схемы электронной подписи [56].

Кроме того, в этом разделе представлен перечень вычислительных задач, обладающих доказанной алгоритмической сложностью либо не имеющих известных эффективных решений и, как следствие, рассматриваемых в качестве основы для построения криптографических схем.

В **Главе 1** исследуется структура ключей электронной подписи CFS на основе подкодов кодов Рида–Маллера. Следуя результатам работы [37], подкоды, квадрат Адамара которых совпадает с квадратом соответствующего кода Рида–Маллера, считаются небезопасными для внедрения в криптографическую схему. Это обусловлено тем, что атака на такую схему за полиномиальное сводится время к атаке на схему, построенную на полном коде Рида–Маллера, для которой уже известны эффективные структурные атаки. Для описания таких подкодов вводится термин *стабильные подкоды*. С целью выявления подкодов, потенциально пригодных для криптографического применения, рассматриваются так называемые *нестабильные подкоды*, базис которых получен исключением из стандартного базиса кода Рида–Маллера, заданного векторами значения мономов

$$1, x_1, x_2, \ldots, x_m, x_1x_2, \ldots, x_{m-1}x_m, \ldots, x_1x_2\ldots x_r, \ldots, x_{m-r+1}x_{m-r+2}\ldots x_m,$$

$q(m,r)$ мономов старшей степени. Стабильные подкоды можно представить как линейную оболочку объединения кода Рида–Маллера порядка $r-1$ с набором из $w(m,r)$ векторов порядка r, где между величинами $q(m,r)$ и $w(m,r)$ существует взаимно однозначное соответствие.

С практической точки зрения важна задача определения минимального

значения $q(m,r)$, при котором квадрат подкода совпадает с квадратом полного кода, что означает потерю стойкости. В эквивалентной дуальной постановке необходимо максимизировать параметр $w(m,r)$. Знание этих величин позволяет конструировать безопасные подкоды, удаляя из стандартного базиса $q(m,r)+1$ вектор максимальной степени.

В Разделе 1.1 рассматриваются подкоды кодов Рида–Маллера порядка 2. Для этого случая получено полное описание структуры стабильных и нестабильных подкодов, а также найдено точное значение параметра $w(m,2)$ (Теорема 2, Следствия 3 и 4). Раздел 1.2 посвящен обобщению подхода на случай произвольного порядка r. В нем приводятся верхняя и нижняя оценки параметра $w(m,r)$ (Теоремы 3 и 4), что позволяет количественно оценить возможности построения нестабильных подкодов при различных параметрах. Завершает главу Раздел 1.3, в котором рассматриваются подкоды, полученные исключением из стандартного базиса фиксированного числа мономов. Доказано, что доля нестабильных подкодов такого типа кода $\mathsf{RM}(r,m)$ стремится к нулю при $m \to \infty$ (Теорема 6).

Таким образом, результаты диссертации показывают, что при случайной генерации маловероятно попасть в подкод, на основе которого может быть построена стойкая криптографическая схема. Однако, следуя предложенной в работе методике систематического исключения векторов максимальной степени, можно конструктивно формировать гарантировано нестабильные подкоды, что, в свою очередь, обеспечивает потенциальную стойкость соответствующих криптосистем, в частности схемы подписи CFS.

Глава 2 посвящена анализу возможностей построения схемы электронной подписи на основе квазициклических кодов.

С точки зрения хранения открытой информации такой подход является высокоэффективным, поскольку позволяет хранить в памяти не каждый элемент матрицы открытого ключа, а лишь первую строку каждой подматрицы. В результате объем памяти, необходимый для хранения квазициклической мат-

рицы размера $k_0 r \times n_0 r$, снижается с $k_0 n_0 r^2$ бит до $k_0 n_0 r$ бит.

Одним из шагов рассмотренного в диссертационной работе алгоритма генерации ключей на основе квазициклического кода является построение случайной невырожденной двоичной квазициклической матрицы. Для реализации этого алгоритма необходимо эффективно проверять матрицу на невырожденность. Сложность проверки на невырожденность матрицы в поле $\mathbb{F}_2$ стандартным образом определяется по алгоритму гауссова исключения и может быть оценена как $O(n_0^3 r^3)$ при $n = n_0 r, n_0 \to \infty$. Однако такой способ не учитывает квазициклическую структуру и не оптимизирован для матриц такого вида.

Другой подход к решению этой задачи был предложен в работе, посвященной схеме LEDAcrypt [55]. Он основан на представлении квазициклической матрицы как матрицы многочленов $M(Q)$ над факторкольцом кольца многочленов $K_f = \mathbb{F}_2[x]/(x^r - 1)$, полученной заменой каждого циркулянта Q с первым столбцом $\widehat{q}$ степени r на многочлен $\widehat{q}_1 + \widehat{q}_2 x + \cdots + \widehat{q}_r x^{r-1}$. Для колец не работают классические алгоритмы линейной алгебры над полем, включающие алгоритм Гаусса. Поэтому авторы предлагают вместо этого применить к матрице $M(Q)$ экспоненциальный алгоритм вычисления перманента. Такой алгоритм возможно использовать при малых значениях параметра n_0 (например, $n_0 = 4$). Но схема подписи CFS требует значительно бóльших параметров [54], таких как $n_0 = 63$, и для них экспоненциальная сложность построения подходящей матрицы становится запретительной.

В работе для решения этой задачи квазициклическая матрица рассматривается в форме матрицы многочленов $M(Q)$, по аналогии с тем, как это было сделано в LEDAcrypt. Далее, на основе этой матрицы, вводится вспомогательная матрица $\mathrm{wt}_2(M(Q))$, элементы которой представляют собой четность весов соответствующих многочленов, то есть четность количества их ненулевых коэффициентов. Раздел 2.1 посвящен строгому заданию этих матриц, а в Разделе 2.2 формализована связь между свойствами их обратимости (Теорема 7 и Следствие 6). Раздел 2.3 посвящен оценке доли невырожденных матриц в

факторкольцах K_f и K_{x^r-1} (Следствие 7 и Теорема 10).

В Разделе 2.4 предложен эффективный алгоритм приведения матрицы $A \in K_f^{n\times n}$ к верхнетреугольному виду. На его основе в Разделе 2.5 построен алгоритм генерации случайной обратимой матрицы над кольцом K_f. Алгоритм реализуется посредством случайной генерации матрицы многочленов и последующей проверки обратимости ее определителя. В случае отрицательного результата генерация повторяется. Простроенный алгоритм эффективен (Теорема 12).

В качестве альтернативного подхода был предложен другой алгоритм решения той же задачи, но специализированный для колец K_{x^r-1} (Теорема 13). На первом этапе осуществляется генерация случайной двоичной матрицы с последующей проверкой ее обратимости. В случае положительного результата данная матрица интерпретируется как матрица весов, на основе которой формируется матрица многочленов таким образом, чтобы вес каждого многочлена совпадал со значением в соответствующем элементе. На завершающем этапе вновь требуется проверка обратимости построенной матрицы через вычисление ее определителя.

В **Главе 3** рассматривается возможность построения ключей электронной подписи CFS на основе конструкции Сидельникова. Если раньше открытый ключ был произведением $MR\Gamma$ тройки матриц, составляющих секретный ключ, где M была невырожденной матрицей, R — проверочной матрицей некоторого линейного кода, а Γ — перестановочной матрицей, то теперь рассматриваются открытые ключи вида $(M_1R_1\|M_2R_2)\Gamma$, где обе матрицы M_1, M_2 невырождены и входят в секретный ключ, а R_1, R_2 — порождающие матрицы, вообще говоря, не обязательно одинаковых кодов.

В силу того, что один открытый ключ как в оригинальной, так и в модифицированной криптосистеме может быть получен из различных секретных ключей, их множество естественным образом разбивается на классы эквивалентности. Тогда для изучения особенностей структуры каждого класса можно использовать любого его представителя. В частности, можно обращаться к от-

крытым ключам вида $(R_1 \| MR_2)\Gamma$, где $M = M_1^{-1} M_2$.

В работе рассматриваются только случаи, когда матрицы R_1 и R_2 совпадают. Код, заданный такой порождающий матрицей, в работе обозначен через $\mathcal{C}[M]$, а также для него введено определение: такой код называется *кодом с разложимым квадратом*, если $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$ и *кодом с неразложимым квадратом*, если $(\mathcal{C}[M])^2 \subsetneq \mathcal{C}^2 \times \mathcal{C}^2$.

Способ задания ключей криптосистемы на основе конструкции Сидельникова неоднократно подвергался изучению [44—46; 69]. Работа [44] рассматривает случай, когда схема строится полностью на кодах Рида–Маллера (авторы рассматривают обобщение, где используется некоторое произвольное число копий кода $u \geqslant 2$). Она предлагает полиномиальную атаку восстановления секретного ключа по открытому ключу криптосистем, использующих код Рида–Маллера с разложимым квадратом.

Полиномиальная атака на вариант, в котором R_1 — порождающая матрица кода Рида–Маллера, а R_2 — порождающая матрица случайного линейного кода, также возможна в предположении о разложимости квадрата соответствующего кода [46]. Эти результаты были обобщены в работе [69], где для криптографической схемы на основе u порождающих матриц произвольных линейных кодов построено сведение к стойкости схем на каждом коде по-отдельности.

В то же время в работе [47] показано, что с вероятностью близкой к 1 случайный линейный код обладает разложимым квадратом. Это делает введенное понятие кода с неразложимым квадратом актуальным необходимым условием стойкой криптосистемы.

Раздел 3.1 вводит дополнительное определение *укорочения кода* и связанное с ним свойство. В Разделе 3.2 вводится понятие эквивалентных секретных ключей схемы подписи, а также показано взаимно однозначное соответствие между классом эквивалентности и некоторым введенным множеством перестановок $\mathcal{G}_R(M_1, M_2)$ (Теорема 14). Полученный результат есть обобщение результата из работы [70], доказанного для кодов Рида–Маллера. Еще одним обобще-

нием является полученная в этом разделе оценка снизу на мощность открытых ключей соответствующей схемы подписи CFS (Теорема 15).

Введено понятие кода с разложимым и неразложимым квадратом и доказано, что любой линейный код обязан удовлетворять одному из этих определений (Теорема 16). Получено описание класса эквивалентности секретных ключей схемы подписи CFS на основе конструкции Сидельникова, построенной на произвольном линейном коде, если код $\mathcal{C}[M]$ имеет разложимый квадрат (Утверждение 28 и Утверждение 29). Раздел 3.3 уточняет результат, полученный для произвольных линейных кодов, за счет сужения области исследования до обобщенных кодов Рида–Соломона (Теорема 17).

Раздел 3.4 содержит примеры невырожденных матриц M, задающих коды с неразложимым квадратом (Теорема 18, Следствие 12 и Теорема 20). Такие коды не могут быть найдены случайно в силу их малой вероятности, при этом они являются потенциальной основой для построения стойких криптографических схем, не подверженных упомянутым выше атакам.

Глава 4 посвящена разработке альтернативного подхода к построению схемы электронной подписи на основе кодов, исправляющих ошибки. Недостатком схемы CFS является то, что использование некоторых классов кодов может привести к снижению ее криптографической стойкости. Это связано с некорректностью предположения о сложности для конкретных классов кодов задачи синдромного декодирования, которая заключается в поиске вектора e веса t такого, что $He^T = s^T$ для заданной матрицы H, вектора s и числа t. На сегодняшний день доказательство NP-трудности известно только для линейного кода общего вида [28]. Поэтому целесообразным представляется построение схемы электронной подписи на основе оригинальной вычислительно сложной задачи, стойкость которой не зависит от структуры используемого кода. Такой поход исключает возможность использования алгоритмов декодирования, непосредственно опирающихся на внутренние свойства кодов, что обусловливает необходимость поиска принципиально иного подхода по сравнению со схемой CFS.

Вариант решения поставленной задачи предложен в Разделе 4.1, также в нем введены формальные модели нарушителя. В качестве основы для построения новой схемы электронной подписи выбрана схема идентификации, предложенная Я. Штерном [57]. Как показали А. Фиат и А. Шамир в 1987 году [56], на базе схемы идентификации возможно построение схемы электронной подписи, посредством внедрения дополнительной хэш-функции, имитирующий интерактивный ответ второй стороны. Для построенной схемы в Разделе 4.2 через серию сведений получено обоснование стойкости в модели EUF-CMA, в которой нарушитель, с целью построения подделки, имеет возможность запрашивать подписи на выбранные им сообщения, а также вычислять значения внутренней хэш-функции. Стойкость построенной схемы подписи описывает Следствие 13.

Схема подписи на основе схемы идентификации Штерна разрабатывалась в рамках деятельности рабочей группы Технического комитета 26 по стандартизации.

В **Заключении** представлены основные результаты диссертации.

Приложение включает код одного из приведенных в Главе 1 алгоритмов, написанный на языке `Python`.

Благодарности. Автор диссертации выражает благодарность за постановку задачи, внимание к работе и советы своему научному руководителю кандидату физико-математических наук Чижову Ивану Владимировичу. Также автор благодарит мужа и друзей за поддержку, оказанную в процессе написания работы.

Обозначения, определения и общие сведения

Настоящий раздел посвящен введению понятий и свойств, которые используются далее по тексту диссертации.

1. Сведения из общей алгебры

Определение 1. *Линейной оболочкой* $\operatorname{span}(S)$ конечного множества S векторов из линейного пространства V над полем $\mathbb{F}$ называется множество

$$\operatorname{span}(S) = \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \mid v_1, \ldots v_n \in S, |S| = n, \lambda_1, \ldots, \lambda_n \in \mathbb{F}\}.$$

Определение 2. Для произвольного коммутативного кольца K с единицей набор векторов $u_1, \ldots, u_k \in K^n$, $k, n \geqslant 1$ будем называть *линейно независимым*, если для любых элементов $\alpha_1, \ldots, \alpha_k \in K$, одновременно не равных нулю, верно

$$\alpha_1 u_1 + \ldots + \alpha_k u_k \neq 0.$$

Пустой набор векторов будем считать линейно независимым по определению.

Определение 3. Для произвольного коммутативного кольца K с единицей матрица $A \in K^{n \times n}$ называется *невырожденной*, если ее определитель является обратимым элементом кольца. Матрица A называется *обратимой*, если существует матрица B такая, что $AB = BA = I$.

Определение 4. *Порядком* числа $g \in \mathbb{Z}$ по модулю $d \in \mathbb{N}$ такому, что $\text{НОД}(g, d) = 1$, называется минимальное $k > 0$ такое, что $g^k = 1 \pmod{d}$. Будем обозначать его $\operatorname{ord}_d(g)$.

Определение 5. *Подстановкой* на конечном множестве Ω называется любое взаимно однозначное отображение этого множества на себя.

Если $\Omega = \mathbb{N}_n = \{1, 2, \ldots, n\}$, то для обозначения множества подстановок используется символ $\mathcal{S}_n$. Далее будут рассматриваться только такие подстановки.

Подстановка может быть задана несколькими способами. Первый из них — это определить функцию $\pi : \mathbb{N}_n \to \mathbb{N}_n$. Другой способ заключается в использовании перестановочной матрицы.

Определение 6. Матрица P размера $n \times n$, состоящая из элементов поля $\mathbb{F}_{q^m}$, называется *перестановочной*, если все ее элементы равны нулю или единице, причем для каждого $1 \leqslant j \leqslant n$ единицы стоят на пересечении строки $\pi(j)$ и столбца j, а остальные элементы равны нулю.

Таким образом, любой перестановочной $n \times n$-матрице P можно взаимно однозначно сопоставить подстановку $\pi \in \mathcal{S}_n$. Так, если обозначить через P_{ij} элемент, находящийся на пересечении строки с номером i и столбца с номером j матрицы P, то $P_{ij} = 1$ тогда и только тогда, когда $\pi(j) = i$. Таким образом, умножение некоторого вектора $(w_1, \dots w_n)$ справа на матрицу P, также как и непосредственное поэлементное применение подстановки π, дает в результате вектор $(w_{\pi(1)}, \dots, w_{\pi(n)})$. Поэтому в дальнейшем мы не будем делать различий между подстановками и перестановочными матрицами.

Определение 7. *Единичной матрицей* I_n называется квадратная матрица размера $n \times n$, все элементы I_{ij} которой задаются как

$$I_{ij} = \begin{cases} 1, & \text{если } i = j; \\ 0, & \text{иначе.} \end{cases}$$

2. Линейные коды

В общем смысле понятие кода обозначает множество слов, заданных над некоторым фиксированным алфавитом. Однако в настоящей работе все результаты были получены для более узкого класса кодов, который обладает свойством линейности.

Определение 8. Пусть $\mathbb{F}_q$ — поле Галуа порядка q и V_n — линейное пространство над полем $\mathbb{F}_q$ размерности n. Тогда *линейным блоковым q-ичным кодом*

называется линейное k-мерное подпространство $\mathcal{C}$ пространства V_n. При этом k называется *размерностью* кода, а n — его *длиной*.

В дальнейшем под «кодом» всегда будем понимать именно линейный код. Также иногда код длины n и размерности k будем называть $[n, k]$-*кодом*.

Определение 9. Пусть $\mathcal{C}$ — линейный код размерности k над полем $\mathbb{F}_q$. *Подкодом* кода $\mathcal{C}$ называется любое линейное подпространство $\mathcal{C}' \subseteq \mathcal{C}$ над $\mathbb{F}_q$. Если подкод $\mathcal{C}'$ имеет размерность k', то его *коразмерность* в коде $\mathcal{C}$ определяется как разность $k - k'$.

Коды играют важную роль при передаче информации, поскольку позволяют обнаруживать и исправлять возникающие в процессе ошибки. Эффективность конкретного кода при решении этих задач определяется характеристикой, называемой минимальным расстоянием. Определим это понятие ниже.

Определение 10. *Расстоянием Хэмминга* (или просто *расстоянием*) $\rho(x, y)$ между двумя векторами x и y называется число координат, в которых эти векторы различаются.

Определение 11. *Весом Хэмминга* (или просто *весом*) $\mathrm{wt}(x)$ вектора x называется число ненулевых координат этого вектора.

Определение 12. *Минимальным (или кодовым) расстоянием* линейного кода $\mathcal{C}$ называется число d, равное минимальному расстоянию между кодовыми словами кода $\mathcal{C}$, то есть

$$d = \min_{\substack{x \in \mathcal{C},\, y \in \mathcal{C}, \\ x \neq y}} \rho(x, y) = \min_{x \in \mathcal{C},\, x \neq 0} \mathrm{wt}(x).$$

Утверждение 1 ([71]). *Код с минимальным расстоянием d может исправлять $\lfloor (d-1)/2 \rfloor$ ошибок. Если d четное, то код может одновременно исправлять $(d-2)/2$ ошибок и обнаруживать $d/2$ ошибок.*

Линейный код как линейное пространство может быть задан своим базисом, который можно представить в виде матрицы.

Определение 13. Матрица G размера $k \times n$, состоящая из элементов поля, строками которой являются векторы базиса кода $\mathcal{C}$, называется *порождающей матрицей* кода $\mathcal{C}$.

Порождающая матрица кода не уникальна, что показывает следующее утверждение. Его справедливость очевидным образом следует из свойств линейных подпространств.

Утверждение 2. *Матрицы G_1 и G_2 являются порождающими матрицами одного и того же кода $\mathcal{C}$, если и только если существует невырожденная квадратная матрица M такая, что $G_1 = M \cdot G_2$.*

Определение 14. Под *произведением Адамара* (или просто *произведением*) двух векторов b и c будем понимать вектор, полученный покомпонентным перемножением координат исходных векторов:

$$(b_1, \ldots, b_n) \circ (c_1, \ldots, c_n) = (b_1 c_1, \ldots, b_n c_n)$$

Будем обозначать его как $b \circ c$.

Определение 15. *Произведением Адамара* (или просто *произведением*) двух кодов $\mathcal{B}$ и $\mathcal{C}$, обозначенным как $\mathcal{B} \circ \mathcal{C}$, будем называть линейную оболочка множества

$$\{b_1 \cdot b_2 \mid b_1 \in \mathcal{C}_1,\ b_2 \in \mathcal{C}_2\}.$$

Выражение $\underbrace{\mathcal{C} \circ \ldots \circ \mathcal{C}}_{k \text{ раз}}$ есть k-тая степень кода $\mathcal{C}$. Кратко будем обозначать ее как $\mathcal{C}^k$. В случае, когда $k = 2$, будем называть полученный код *квадратом кода* $\mathcal{C}$.

Определение 16. Под *декартовым произведением* двух кодов $\mathcal{B}$ и $\mathcal{C}$ будем понимать множество $\mathcal{B} \times \mathcal{C}$, элементами которого являются все возможные упорядоченные конкатенации кодовых слов вида:

$$\mathcal{B} \times \mathcal{C} = \{b \| c \,\Big|\, b \in \mathcal{B}, c \in \mathcal{C}\}.$$

Определение 17. Подстановка координат, отображающая код $\mathcal{C}$ "на себя", то есть переводящая каждое кодовое слово в кодовое слово того же кода, возможно, отличное от исходного, называется *автоморфизмом* кода $\mathcal{C}$. Множество всех автоморфизмов кода $\mathcal{C}$ обозначается $\mathrm{Aut}(\mathcal{C})$.

Утверждение 3 ([71]). *Множество автоморфизмов данного кода является группой относительно операции композиции подстановок.*

3. Дуальные коды

Определение 18. Пусть $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ — векторы над полем $\mathbb{F}_q$. Тогда *скалярным произведением* векторов x и y называется число $(x, y) \in \mathbb{F}_q$:

$$(x, y) = x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_n \cdot y_n.$$

Векторы, скалярное произведение которых равно нулю, принято называть *ортогональными.*

Каждый код $\mathcal{C}$ однозначно задает так называемый дуальный код.

Определение 19. *Дуальным кодом* $\mathcal{C}^\perp$ к коду $\mathcal{C}$ называется линейный код, состоящий из всех возможных векторов длины n, которые ортогональны любому кодовому слову кода $\mathcal{C}$, то есть

$$\mathcal{C}^\perp = \{u \mid (u, c) = 0, \forall c \in \mathcal{C}\}.$$

Код $\mathcal{C}^\perp$ имеет длину n и размерность $n-k$, другими словами, $\mathcal{C}^\perp$ есть $[n, n-k]$-код.

Определение 20. Порождающая матрица H размера $(n-k)\times n$ кода $\mathcal{C}^{\perp}$, дуального к $\mathcal{C}$, называется *проверочной матрицей* кода $\mathcal{C}$.

Из этого определения следует также, что порождающая матрица G кода $\mathcal{C}$ является проверочной для кода $\mathcal{C}^{\perp}$.

Утверждение 4 ([71]). *Проверочная и порождающая матрицы линейного кода $\mathcal{C}$ связаны соотношением*

$$H\cdot G^{T}=G\cdot H^{T}=0.$$

Введение проверочной матрицы позволяет дать альтернативное определение линейного блокового кода.

Определение 21. Если H — произвольная q-ичная матрица, то *линейный блоковый q-ичный код* с проверочной матрицей H состоит из всех таких векторов x, что $Hx^{T}=0$.

Легко заметить, что определения 8 и 21 эквивалентны.

Два утверждения ниже можно считать общеизвестными, однако приведем их вместе с доказательствами.

Утверждение 5. *Если для двух кодов $\mathcal{B}$ и $\mathcal{C}$ выполнено, что $\mathcal{C}\subseteq\mathcal{B}$, то также выполнено $\mathcal{B}^{\perp}\subseteq\mathcal{C}^{\perp}$.*

Доказательство. Рассмотрим кодовое слово $x\in\mathcal{B}^{\perp}$. По определению,

$$\forall v\in\mathcal{B}:\ (x,v)=0\quad\Rightarrow\quad\forall v\in\mathcal{C}:\ (x,v)=0,$$

поэтому $x\in\mathcal{C}^{\perp}$. □

Утверждение 6. $(\mathcal{C}\times\mathcal{C})^{\perp}=\mathcal{C}^{\perp}\times\mathcal{C}^{\perp}$.

Доказательство. Пусть для некоторого вектора выполнено вложение $x\|y\in(\mathcal{C}\times\mathcal{C})^{\perp}$. Тогда $(x\|y,c\|0)=0$ для любого $c\in\mathcal{C}$, а, следовательно, $x\in\mathcal{C}^{\perp}$. Аналогично можно показать, что $y\in\mathcal{C}^{\perp}$. Таким образом, $x\|y\in\ \mathcal{C}^{\perp}\times\mathcal{C}^{\perp}$.

Для доказательства в другую сторону зафиксируем произвольные вектора $a \in \mathcal{C},\ b \in \mathcal{C},\ x \in \mathcal{C}^{\perp},\ y \in \mathcal{C}^{\perp}$. Тогда $(x\|y, a\|b) = (x, a) + (y, b) = \ 0$, то есть $x\|y \in (\mathcal{C} \times \mathcal{C})^{\perp}$. □

4. Задачи на кодах

На линейных кодах возможно поставить ряд задач, которые являются доказано сложными. Это позволяет использовать их как основу для целого ряда криптографических схем. Ниже приведем (не исчерпывающий) список таких задач в форме разрешимости.

Задача γ-GSD. **Декодирование кода класса** γ

Дано: порождающая $k \times n$-матрица G некоторого кода над $\mathbb{F}_{q^m}$, ненулевой вектор $y \in \mathbb{F}_{q^m}^n$ и число t.

Вопрос: существует ли такая пара векторов $(x, e), x \in \mathbb{F}_{q^m}^k, e \in \mathbb{F}_{q^m}^n$, что $\mathrm{wt}(e) = t$ и $y = xG + e$?

Задача γ-SD. **Синдромное декодирование кода класса** γ

Дано: проверочная $r \times n$-матрица H некоторого кода заданного класса γ над $\mathbb{F}_{q^m}$, вектор $s \in \mathbb{F}_{q^m}^r$ (который называется *синдромом*) и число t.

Вопрос: существует ли такой вектор $e \in \mathbb{F}_{q^m}^n$, что $\mathrm{wt}(e) = t$ и $He^T = s^T$?

Задача γ-CF. **Поиск кодового слова кода класса** γ

Дано: проверочная $r \times n$-матрица H кода заданного класса γ над $\mathbb{F}_{q^m}$ и число t.

Вопрос: существует ли такой вектор $e \in \mathbb{F}_{q^m}^n$, что $\mathrm{wt}(e) = t$ и $He^T = 0$?

Задача γ-PE. **Перестановочная эквивалентность кодов**

Дано: $r \times n$-матрица G над $\mathbb{F}_{q^m}$.

Найти: такой набор матриц (H, R, Γ) над $\mathbb{F}_{q^m}$, что $r \times n$-матрица R — проверочная или порождающая матрица заданного класса γ, $r \times r$-матрица H невырожденная, $n \times n$-матрица Γ перестановочная и $G = H \cdot R \cdot \Gamma$.

Задача SD для случайного кода является NP-полной (см. [28], [29]). Лучший из известных алгоритмов, решающих эту задачу, описан в работе [72] и требует $O(2^{0.0465n})$ битовых операций. Задача GSD эквивалентна по сложности задаче SD, соответственно также является NP-полной. Работа [28] показала, что это же верно для задачи CF. При этом задачи поиска, соответствующие задачам разрешимости SD, GSD и CF, NP-трудны. Задача PE, согласно работе [73], не может быть слишком легкой и не может быть сильно сложной (и точно не является NP-полной). Для конкретного семейства кодов сложность задач зависит от структуры этого семейства.

В следующих разделах остановимся подробнее на нескольких выделенных классах кодов. При этом будем опускать соответствующий префикс γ, если класс кодов однозначно определен текстом.

5. Квазициклические коды

Введем понятие квазициклического кода и рассмотрим его частные примеры. В дальнейшем тексте диссертации будут изучаться только квазициклические коды над полем $\mathbb{F}_2$.

Определение 22. Квадратная матрица $A \in \mathbb{F}_2^{r\times r}$ называется *циклической матрицей* (или *циркулянтом*) порядка r, если $a_{ij} = \widehat{a}_{1+(i-j) \bmod r}$ для некоторого вектора $\widehat{a} \in \mathbb{F}_2^r$. Иначе говоря, первый столбец матрицы A есть $\widehat{a}$, а каждый следующий получается из предыдущего циклическим сдвигом на один элемент вниз.

Множество циркулянтов порядка r образует кольцо с единицей.

Определение 23. *Весом* циркулянта $A \in \mathbb{F}_2^{r\times r}$ назовем вес Хэмминга его первого столбца, то есть количество единиц в нем.

Определение 24. *Квазициклической матрицей* называется матрица вида

$$Q = \begin{pmatrix} Q_{1,1} & Q_{1,2} & \dots & Q_{1,n} \\ Q_{2,1} & Q_{2,2} & \dots & Q_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{k,1} & Q_{k,2} & \dots & Q_{k,n} \end{pmatrix},$$

где матрицы $Q_{i,j}$ — циркулянты порядка r.

Определение 25. *(Систематическими) квазициклическими кодами* называются коды с (систематической) квазициклической проверочной матрицей.

Определение 26. *Кодом с малой плотностью проверок на четность (LDPC-кодом)* называется представитель бесконечного семейства линейных $[n, k]$-кодов, каждые строка и столбец проверочной матрицы которых при $n \to \infty$ имеет фиксированный вес $w = O(1)$.

Определение 27. *Кодом со средней плотности проверки на четность (MDPC-кодом)* называется представитель бесконечного семейства линейных $[n, k]$-кодов, каждые строка и столбец проверочной матрицы которых при $n \to \infty$ имеет фиксированный вес $w = O(\sqrt{n \log n})$.

Определение 28. Линейные коды называются *QC-LDPC (QC-MDPC)-кодами*, если они являются одновременно LDPC (MDPC)-кодами и квазициклическими кодами.

6. Коды Рида–Маллера

Настоящий раздел посвящен кодам Рида–Маллера. Этот класс кодов известен более 70 лет и интересен благодаря своей алгебраической структуре, которая допускают явное задание параметров и обладает рядом свойств, полезных для исправления ошибок.

Определение 29. *Кодом Рида–Маллера* $\mathsf{RM}(r,m)$ называется множество вектор-значений f всех булевых функций $f(x_1,\ldots,x_m)$, степень нелинейности (максимальная степень монома, входящего в полином Жегалкина функции f) которых не превосходит r, то есть

$$\mathsf{RM}(r,m) = \Big\{\Omega_f = (f_1,\ldots,f_n), n = 2^m \;\Big|$$

$$f_j(x_1,\ldots,x_m) = a_{j_0} \oplus \bigoplus_{s=1}^{t} \bigoplus_{1\leqslant i_1<\cdots<i_s\leqslant m} a_{j_{i_1,\ldots,i_s}} x_{i_1}\ldots x_{i_s},\ t\leqslant r, j=1,\ldots,n\Big\}.$$

В дальнейшем не будем делать различий в обозначении булевых функций и их векторов значений.

Следующее утверждение связывает параметры (n,k,t) и параметры (r,m) кодов Рида–Маллера.

Утверждение 7 ([71]). *Заданный относительно произвольного m и произвольного $r: 0\leqslant r\leqslant m$ двоичный код $\mathsf{RM}(r,m)$ имеет:*

1. *длину $n = 2^m$;*
2. *размерность*
$$k = \sum_{i=0}^{r} \tbinom{m}{i}; \tag{1}$$
3. *кодовое расстояние 2^{m-r}.*

Код Рида–Маллера удобно задавать через выделенный базис специального вида. Иногда его называют мономиальным базисом, мы же будем обращаться к нему как к стандартному.

Определение 30. *Стандартный базис кода Рида–Маллера* $\mathsf{RM}(r,m)$ включает все мономы от m переменных степени от 0 до r включительно, т.е.

$$1, x_1, x_2, \ldots, x_m, x_1x_2, \ldots, x_{m-1}x_m, \ldots, x_1\cdots x_r, \ldots, x_{m-r-1}\cdots x_m.$$

Далее отметим несколько свойств таких кодов. Первые два из них следуют непосредственно из определения кода и определения операции возведения в квадрат Адамара.

Утверждение 8. *Для всех* $0 \leqslant r \leqslant m-1$ *выполнено вложение*

$$\mathsf{RM}(r,m) \subset \mathsf{RM}(r+1,m).$$

Утверждение 9. *Для всех* $0 \leqslant r_1 \leqslant m-1$, $0 \leqslant r_2 \leqslant m-1$ *выполнено:*

$$\mathsf{RM}(r_1,m) \circ \mathsf{RM}(r_2,m) = \mathsf{RM}(r_1+r_2,m).$$

Утверждение 10 ([71])**.** *Для всех* $0 \leqslant r \leqslant m-1$ *код* $\mathsf{RM}(m-r-1,m)$ *дуален коду* $\mathsf{RM}(r,m)$*, то есть*

$$\mathsf{RM}^{\perp}(r,m) = \mathsf{RM}(m-r-1,m).$$

Тем самым код, дуальный к коду Рида–Маллера, сам является кодом Рида–Маллера.

7. Обобщенные коды Рида–Соломона

Класс кодов Рида–Соломона, рассмотренный в данном разделе, обладает максимально возможным кодовым расстоянием, поскольку достигает так называемой границы Синглтона. Благодаря этому такие коды способны исправлять наибольшее возможное число ошибок для заданной длины и размерности.

Определение 31. $[q^m-1,k]$*-обобщенным кодом Рида–Соломона (сокращенно ОРС)* $\mathsf{GRS}_k(\alpha,v)$ для вектора $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$, где α_i — попарно различные элементы поля $\mathbb{F}_{q^m}$, и вектора $v=(v_1,v_2,\ldots,v_n)$, где v_i — не обязательно различные ненулевые элементы поля $\mathbb{F}_{q^m}$, называется k-мерное векторное пространство

$$\big\{(v_1F(\alpha_1),v_2F(\alpha_2),\ldots,v_nF(\alpha_n)) \mid F \in \mathbb{F}_{q^m}[x],\ \deg(F(x)) < k\big\}.$$

Иногда для простоты изложения мы будем использовать многочлен $F(x)$ и его вектор значений $(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n))$ взаимозаменяемо.

Утверждение 11 ([71]). *Матрица вида*

$$\begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \ldots & \alpha_n v_n \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \ldots & \alpha_n^{k-1} v_n \end{pmatrix} = \tag{2}$$

$$= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & 0 & \ldots & 0 \\ 0 & v_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & v_n \end{pmatrix}.$$

является порождающей матрицей кода Рида–Соломона.

Определение обобщенного кода Рида–Соломона позволяет записать следующее утверждение.

Утверждение 12. *Для всех k_1 и k_2, таких что $1 \leqslant k_1 < k_2 \leqslant n$, выполнено вложение*

$$\mathsf{GRS}_{k_1}(\alpha, v) \subsetneq \mathsf{GRS}_{k_2}(\alpha, v). \tag{3}$$

Следующее утверждение также использует определение кода ОРС в совокупности с правилом возведения в квадрат Адамара.

Утверждение 13. *Произведение Адамара двух обобщенных кодов Рида–Соломона при условии $k_1 + k_2 \leqslant n + 1$ имеет вид*

$$\mathsf{GRS}_{k_1}(\alpha, v') \circ \mathsf{GRS}_{k_2}(\alpha, v'') = \mathsf{GRS}_{k_1+k_2-1}(\alpha, v'v'').$$

Следствие 1. $\dim(\mathsf{GRS}_k(\alpha, v))^2 = 2k - 1.$

Следствие 2. *При $k \leqslant \frac{n+1}{2}$ справедливо равенство*

$$\dim\big((\mathsf{GRS}_k(\alpha, v))^2 \times (\mathsf{GRS}_k(\alpha, v))^2\big) = 4k - 2. \tag{4}$$

Утверждение 14 ([71]). *Параметры (n, k, d) кода Рида–Соломона связаны соотношением*

$$d = n - k + 1.$$

Как и в случае с кодами Рида–Маллера, дуальный код к коду Рида–Соломона сам является кодом Рида–Соломона.

Утверждение 15. $\mathsf{GRS}_k(\alpha, v)^\perp = \mathsf{GRS}_{n-k}(\alpha, v')$ *для некоторого* v'.

Утверждение 16. *Для любого вектора $v \in (\mathbb{F}_{q^m}^*)^n$ существует вектор $v' \in (\mathbb{F}_{q^m}^*)^n$ такой, что для любого $1 \leqslant k \leqslant n-1$ выполнено*

$$(\mathsf{GRS}_k(\alpha, v))^\perp = \mathsf{GRS}_{n-k}(\alpha, v'). \tag{5}$$

Несмотря на различие формулировок последних двух утверждений, их доказательства совпадают и содержатся в книге [71] (доказательство Теоремы 4 из Раздела 10.8).

Закончим раздел еще одним вспомогательным фактом об обобщенных кодах Рида–Соломона.

Утверждение 17. *Для любого вектора $u = (\gamma_1, \gamma_2, \ldots, \gamma_k, 0, \ldots, 0) \in \mathbb{F}_{q^m}^n$ верно, что $Ru^T \neq 0$, если R — порождающая матрица вида (2) кода $\mathsf{GRS}_k(\alpha, v)$.*

Доказательство. Любая матрица вида (2), составленная из столбцов порождающей матрицы кода $\mathsf{GRS}_k(\alpha, v)$ с номерами $1, 2, \ldots, i$, где $1 \leqslant i \leqslant n$, будет невырожденной. Это верно в силу того, что определитель такой матрицы отличается от определителя матрицы Вандермонда лишь умножением на ненулевой скаляр. В то же время условие $Ru^T = 0$ означает вырожденность такой матрицы, что приводит к противоречию. □

8. Электронная подпись CFS

Одним из широко используемых криптографических механизмов является электронная подпись, которая представляет собой аналог классической под-

писи, выполненной чернилами на бумаге. Электронная подпись решает задачи контроля целостности данных и неотказуемости от авторства. Приведем ее формальное определение.

Определение 32. Для заданного пространства сообщений $\mathcal{M}$ *протоколом электронной подписи* называется тройка полиномиальных вероятностных алгоритмов $(\mathsf{KGen}, \mathsf{SigGen}, \mathsf{SigVer})$, называемых алгоритмами генерации ключей, генерации подписей и проверки подписей соответственно, таких, что

1. KGen — полиномиальная вероятностная машина Тьюринга такая, что $\mathsf{KGen}(1^\lambda) = (\mathsf{pk}, \mathsf{sk})$, где pk — открытый ключ, а sk — секретный.

2. SigGen — полиномиальная вероятностная машина Тьюринга такая, для произвольного $m \in \mathcal{M}$ возвращающая $\mathsf{SigGen}(\mathsf{sk}, m) = \sigma$.

3. SigVer — полиномиальная машина Тьюринга такая, что

$$\mathsf{SigVer}(\mathsf{pk}, m, \sigma) = \begin{cases} 1, & \text{если } \sigma \text{ корректная подпись} \\ & \text{под сообщением } m; \\ 0, & \text{иначе.} \end{cases}$$

   Кроме того, для любой пары ключей $(\mathsf{pk}, \mathsf{sk})$ и любого сообщения m верно, что $\mathsf{SigVer}(\mathsf{pk}, m, \mathsf{SigGen}(\mathsf{sk}, m)) = 1$.

Оригинальная схема CFS

В 2001 году Н. Куртуа, М. Финиаш и Н. Сендриер в работе [25] предложили схему электронной подписи, которую, следуя устоявшейся традиции, будем называть схемой CFS. Ее особенностью является то, что только честный подписывающий может использовать возможность исправления ошибок секретного кода. Этот эффект достигается за счет того, что схема подписи строится на основе схемы шифрования. При идентичных алгоритмах генерации ключа меняются местами алгоритмы шифрования и расшифрования таким образом, что

алгоритм генерации подписи представляет собой расшифрование некоторого вектора, полученного из сообщения (чаще всего это хэш-значение этого сообщения), а алгоритм проверки подписи — перешифрование подписи и сравнение результата с сообщением. Таким образом, секретный алгоритм декодирования, который существенно использует структуру кода, вызывается в алгоритме генерации подписи, а для проверки подписи синдром вычисляется через проверочную матрицу, поскольку это уже простая задача.

Основная сложность заключается в том, далеко не каждый вектор может быть декодирован таким образом. В оригинальной работе для решения этой проблемы авторы предлагают добавить к хэш-значению сообщения счетчик и увеличивать значение счетчика до тех пор, пока не получится вектор, который может быть успешно декодирован. Однако в 2008 году, Л. Далло показал [26], что использование счетчика i дает противнику дополнительную информацию, поскольку если в подпись входит число i, значит все $j < i$ не могут быть декодированы. Он предложил заменить последовательный выбор i на случайный. Это позволило не только устранить найденную уязвимость, но и формально обосновать стойкость схемы подписи к подделке при условии, что задачи PE и SD (с ослабленным условием на вес вектора ошибки) являются сложными для заданного класса кодов. Ниже приведем включающее модификацию Далло описание схемы CFS.

Параметры схемы: $[n, k]$-код $\mathcal{C}$, заданный над полем $\mathbb{F}_q$, и хэш-функция $h : \mathbb{F}_q^* \to \mathbb{F}_q^{n-k}$.

Алгоритм генерации пары ключей KGen:

1. Случайно выбирается невырожденная матрица M размера $(n-k)\times(n-k)$, перестановочная матрица Γ размера $n\times n$ и проверочная матрица R кода $\mathcal{C}$ размера $(n-k)\times n$.

2. $W = MR\Gamma$ — матрица размера $(n-k)\times n$ — открытый ключ, (M, R, Γ) — секретный ключ.

Алгоритм генерации подписи SigGen**:**

1. Выбрать случайный номер $i \in \{1, \ldots, q^{n-k}\}$.
2. Вычислить $v = h(h(m)\|i)M^{-T}$.
3. Декодировать $x = \mathrm{Dec}_R(v)$.
4. Если не удалось найти вектор x, то повторить шаги 1.–3.
5. Вычислить $y = x\Gamma^{-T}$.
6. Получить подпись $\mathrm{Sign} = (i, y)$.

Алгоритм проверки подписи SigVer**:**

1. Вычислить $s' = yW^T$.
2. Вычислить $s = h(h(m)\|i)$.
3. Вернуть результат сравнения $s = s'$.

Корректность:

Подпись $\mathrm{Sign} = (i, y)$, вычисленная согласно алгоритму генерации подписи, пройдет проверку, поскольку верна следующая цепочка преобразований: $s' = yW^T = (x\Gamma^{-T})(\Gamma^T R^T M^T) = xR^T M^T \overset{(*)}{=} vM^T = h(h(m)\|i)M^{-T}M^T = h(h(m)\|i) = s$. Переход $(*)$ верен в силу того, что, согласно шагу 3. алгоритма генерации подписи $xR^T = v$.

Оригинальная версия подписи CFS строилась на кодах Гоппы, однако имела параметры, которые не позволили бы применить ее на практике. Тем не менее, подпись может быть полностью аналогично построена на основе любого линейного кода, при этом изменения будут касаться лишь алгоритма декодирования Dec. И для ряда известных кодов параметры схемы уже приемлемы

для использования. Однако нужно иметь в виду, что замена кода может также ослабить стойкость схемы. Исходя из совокупности этих факторов в настоящей работе матрица R есть проверочная матрица некоторого подкода кода Рида–Маллера.

Модификация схемы CFS на основе конструкции Сидельникова

Алгоритм генерации ключей подписи CFS для некоторых классов кодов может быть модифицирован с целью обеспечения защиты к ряду атак. В качестве одной из таких модификаций можно предложить конструкция В. М. Сидельникова, которая в оригинальной работе [43] применялась к кодовой криптосистеме Мак-Элиса [5]. Вариант Сидельникова подразумевал использование кодов Рида–Маллера, однако в настоящей работе будет рассмотрен общий случай кодов общего вида, а также кодов Рида–Соломона.

Основная модификация затрагивает алгоритм генерации ключевой пары, однако незначительные изменения вносятся и в алгоритмы генерации и проверки подписи. Поэтому приведем ниже всю тройку алгоритмов. Отметим, что параметры схемы подписи остаются идентичными оригинальному варианту, при этом добавляется новый параметр u задающий количество используемых копий кода.

Параметры схемы: $[n, k]$-код $\mathcal{C}$, заданный над полем $\mathbb{F}_q$, хэш-функция $h : \mathbb{F}_q^* \to \mathbb{F}_q^{un-k}$ и $u \in \mathbb{N}$.

Алгоритм генерации пары ключей KGen**:**

1. Случайно выбираются невырожденные матрицы $M_1, M_2, \ldots, M_u$, каждая размера $k \times k$, перестановочная матрица Γ размера $un \times un$ и проверочная матрица R кода $\mathcal{C}$ размера $k \times n$.

2. $W = (M_1 R \,\|\, M_2 R \,\|\, \ldots \,\|\, M_u R) \cdot \Gamma$ — матрица размера $k \times un$ — открытый ключ, $(M_1, M_2, \ldots, M_u, R, \Gamma)$ — секретный ключ.

Алгоритм генерации подписи SigGen**:**

1. Вычислить проверочную матрицу H кода с порождающей матрицей W.
2. Выбрать случайный номер $i \in \{1, \ldots, q^{un-k}\}$.
3. Вычислить $s = h(h(m)\|i)$.
4. Найти вектор y из системы уравнений $s^T = Hy^T$.
5. Вычислить $x = y\Gamma^{-1}$.
6. Декодировать методом Сидельникова $m = \mathrm{Dec}_{R,M_1,\ldots,M_u}(x)$, обозначить номер успешно декодированной компоненты через j.
7. Если не удалось декодировать, то повторить шаги 2.–6.
8. Вычислить $e = mW + y$.
9. Получить подпись $\mathrm{Sign} = (i, e)$.

Алгоритм проверки подписи SigVer**:**

1. Вычислить проверочную матрицу H кода с порождающей матрицей W.
2. Вычислить $s = h(h(m)\|i)$.
3. Вычислить $s' = e'H^T$.
4. Подпись верна, если $s = s'$.

Корректность:

Подпись $\mathrm{Sign} = (i, y)$, вычисленная согласно алгоритму генерации подписи, пройдет проверку, поскольку

$$s' = eH^T = e\Gamma H^T = (mW + y)H^T = mWH^T + yH^T = s.$$

Далее в работе будем рассматривать только частный случай, когда $u = 2$.

Модификация схемы CFS для квазициклического кода

Схема CFS на основе квазициклического кода отличается от оригинальной сильнее, чем вариант, рассмотренный в разделе выше. Снова основная модификация касается алгоритма генерации ключей, но изменениям подвергаются, соответственно, и алгоритмы генерации и проверки подписи. При описании этого варианта будем опираться на схему шифрования из работы [74], используя в качестве алгоритма генерации подписи алгоритм расшифрования, а в качестве алгоритма проверки подписи — алгоритм шифрования.

Параметры схемы: простое число r, код $\mathcal{C}$ с параметрами $n = rn_0, k = r(n_0 - 1)$, заданный над полем $\mathbb{F}_2$, и хэш-функция $h : \mathbb{F}_2^* \to \mathbb{F}_2^r$.

Алгоритм генерации пары ключей KGen**:**

1. Случайно выбирается невырожденная квазициклическая матрица Q размера $n_0 r \times n_0 r$,
$$Q = \begin{pmatrix} Q_{1,1} & Q_{1,2} & \cdots & Q_{1,n_0} \\ Q_{2,1} & Q_{2,2} & \cdots & Q_{2,n_0} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{n_0,1} & Q_{n_0,2} & \cdots & Q_{n_0,n_0} \end{pmatrix},$$
и проверочная матрица $H = (H_1 \| \ldots \| H_{n_0})$ размера $r \times n_0 r$ некоторого квазициклического кода с нечетным весом каждой строки.

2. Вычисляется матрица $L = (L_1 \| \ldots \| L_{n_0}) = H(Q^T)^{-1}$ размера $r \times n_0 r$.

3. Вычисляется матрица $M = (M_1 \| \ldots \| M_{n_0 - 1} \| I) = L_{n_0}^{-1} L$ размера $r \times n_0 r$.

4. Матрица M — открытый ключ, пара (H, Q) — секретный ключ.

Алгоритм генерации подписи SigGen**:**

1. Вычислить $L = (L_1 \| \ldots \| L_{n_0}) = H(Q^T)^{-1}$.

2. Выбрать случайный номер $i \in \{1, \ldots, 2^r\}$.

3. Вычислить $v = h(h(m)\|i))L_{n_0}^T$.

4. Декодировать $x = \mathrm{Dec}_L(v)$.

5. Если не удалось найти вектор x, то повторить шаги 2.–4.

6. Получить подпись $\mathrm{Sign} = (i, x)$.

Алгоритм проверки подписи SigVer**:**

1. Вычислить $s' = xM^T$.

2. Вычислить $s = h(h(m)\|i)$.

3. Вернуть результат сравнения $s = s'$.

Корректность:

Выход алгоритма SigGen вида (i, x) гарантирует выполнение условия на шаге 3. алгоритма проверки подписи, поскольку $s' = xM^T = xL^T L_{n_0}^{-T} \overset{(*)}{=} vL_{n_0}^{-T} = h(h(m)\|i)L_{n_0}^T L_{n_0}^{-T} = h(h(m)\|i) = s$. Переход $(*)$ верен в силу того, что, согласно шагу 4. алгоритма генерации подписи $xL^T = v$.

8.1. Протокол идентификации Штерна

Под схемой идентификации обычно понимается интерактивный протокол, в котором одна сторона, доказывающий (Prover), пытается убедить другую сторону, проверяющего (Verifier), в знании секретного ключа и таким образом пройти проверку личности. Протоколы идентификации состоят из предварительного алгоритма генерации ключей KGen и непосредственного интерактивного протокола доказательства, развернутого между двумя участниками.

К числу известных протоколов идентификации относится схема Я. Штерна, впервые предложенная автором в 1993 году на конференции CRYPTO. Полноценное описание протокола представлено в его работе 1994 года [57]. Штерн предложил такую схему генерации ключевой пары, что задача восстановления

секретного ключа по открытому в точности совпадала с классической задачей синдромного декодирования. При использовании случайного кода, с учетом сложности последней задачи, этот факт гарантировал отсутствие атак, направленных на восстановление секретного ключа.

При этом предложенный протокол несложно подделать. В своей статье Штерн предлагает стратегию для противника, при которой возможно пройти идентификацию без знания секретного ключа с вероятностью успеха, равной 2/3. Чтобы уменьшить эту вероятность и достичь требуемого уровня стойкости, алгоритм необходимо повторить несколько раз.

Параметры протокола зависят от параметров основного кода: его длины n, размерности k и минимального расстояния d. Проверочной матрицей этого кода является случайная матрица $H \in \mathbb{F}_2^{(n-k)\times n}$. Также протокол использует криптографическую хэш-функцию $h(\cdot) : \mathbb{F}^* \to \mathbb{F}_2^\ell$.

Алгоритм генерации пары ключей KGen**:**

1. Выбрать случайный вектор s из множества $\left\{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = d\right\}$.

2. Вычислить $y = Hs^T$.

3. Вектор y — открытый ключ, вектор s — секретный ключ.

Описание протокола идентификации показано на рис. 1. В нем запись $s \overset{\mathcal{U}}{\leftarrow} S$ означает, что s выбрано из множества S случайно равновероятно. А выражение $x \leftarrow v$ означает присваивание значения v переменной x.

Prover(s)		**Verifier**(y)
$u \overset{\mathcal{U}}{\leftarrow} \mathbb{F}_2^n, \sigma \overset{\mathcal{U}}{\leftarrow} \mathcal{S}_n$		
$c_0 \leftarrow h(\sigma \Vert Hu^T)$		
$c_1 \leftarrow h(\sigma(u))$		
$c_2 \leftarrow h(\sigma(u \oplus s))$		
	$\xrightarrow{c_0, c_1, c_2}$	
		$b \overset{\mathcal{U}}{\leftarrow} \{0, 1, 2\}$
	$\xleftarrow{b}$	
if $b = 0 : r_0 \leftarrow \sigma, r_1 \leftarrow u$		
if $b = 1 : r_0 \leftarrow \sigma, r_1 \leftarrow u \oplus s$		
if $b = 2 : r_0 \leftarrow \sigma(u), r_1 \leftarrow \sigma(s)$		
	$\xrightarrow{r_0, r_1}$	
		if $b = 0$:
		Check $c_0 \overset{?}{=} h(r_0 \Vert Hr_1^T)$,
		$c_1 \overset{?}{=} h(r_0(r_1))$
		if $b = 1$:
		Check $c_0 \overset{?}{=} h(r_0 \Vert (Hr_1^T \oplus y))$,
		$c_2 \overset{?}{=} h(r_0(r_1))$
		if $b = 2$:
		Check $c_1 \overset{?}{=} h(r_0)$,
		$c_2 \overset{?}{=} h(r_0 \oplus r_1)$,
		$\mathrm{wt}(r_1) \overset{?}{=} d$

Рис. 1. Схема идентификации Штерна

Глава 1

Свойства ключей электронной подписи CFS на основе подкодов кодов Рида–Маллера

Исследования криптографических схем на подкодах кодов Рида–Маллера проводилось в работе [37]. В ней показано, что если для подкода $\mathcal{C}$ кода Рида–Маллера $\mathsf{RM}(r, m)$ выполняется равенство

$$\mathcal{C}^2 = \mathsf{RM}^2(r, m), \tag{1.1}$$

то атака на этот подкод полиномиально сводится к атаке на полный код. При этом для кода $\mathsf{RM}(r, m)$ уже известна полиномиальная структурная атака [33]. Таким образом, подкоды, удовлетворяющие условию (1.1), нельзя назвать стойкими и использовать на практике.

Предметом анализа настоящей главы является структура подкодов кода $\mathsf{RM}(r, m)$ таких, что построенная на них схема подписи CFS не будет подвержена упомянутой полиномиальной структурной атаке. Другим вопросом является доля подкодов, стойких к данному классу атак.

Глава содержит результаты, опубликованные в работе [64].

1.1. Электронная подпись на подкодах кодов $\mathsf{RM}(2, m)$

Начнем с анализа схемы CFS на подкоде частного случая кода Рида–Маллера с параметром $r = 2$.

Допустим, что код Рида–Маллера задан своим стандартным базисом. Будем искать минимальное число мономов $f_1, \ldots, f_{w(m,2)}$ степени 2 таких, что для подкода

$$\operatorname{span}\big(\mathsf{RM}(1, m) \cup \{f_1, \ldots, f_{w(m,2)}\}\big) \tag{1.2}$$

выполнено условие (1.1). Иначе говоря, для заданных $w(m, 2)$ мономов верно,

что

$$\big(\mathrm{span}\big(\mathsf{RM}(1,m)\cup\{f_1,\ldots,f_{w(m,2)}\}\big)\big)^2=\mathsf{RM}(4,m). \tag{1.3}$$

Подкод вида (1.2) будем называть *стабильным*.

Очевидно, что после нахождения минимального числа $w(m,2)$ мономов f_i, можно ответить на еще один вопрос: чему равно число $q(m,2)$ мономов степени 2, которые можно исключить из базиса кода $\mathsf{RM}(2,m)$ так, чтобы код

$$\mathrm{span}\big(\{1,x_1,x_2,\ldots,x_m,x_1x_2,\ldots,x_{m-1}x_m\}\setminus\{g_1,\ldots,g_{q(m,2)}\}\big)$$

остался стабильным. Соотношение между этими величинами может быть задано следующим уравнением:

$$q(m,2)=\binom{m}{2}-w(m,2). \tag{1.4}$$

Таким образом, после удаления $q(m,2)+1=\binom{m}{2}-w(m,2)+1$ базисных векторов, код становится *нестабильным*. Поэтому далее не будем останавливаться на этой задаче отдельно.

Перейдем к графовой интерпретации задачи. Сопоставим подкоду $\mathcal{A}\subset\mathsf{RM}(2,m)$ граф $G=(V,E)$ с множеством вершин $V=\{x_1,\ldots,x_m\}$ и множеством ребер E. Ребро $\{x_i,x_j\}\in E$ тогда и только тогда, когда моном $x_ix_j\in\mathcal{A}$.

Обозначим через $\deg(v)$ степень вершины v в графе. Будем говорить, что граф с m вершинами *обладает свойством* P, если

1. степень $\deg(v)$ любой вершины v не менее, чем $m-3$;
2. если $\deg(v)=m-3$ и $\{v,u_1\}\notin E,\{v,u_2\}\notin E$, то $\{u_1,u_2\}\in E$.

Случай $\deg(x_1)=m-3$ представлен на Рис. 1.1, где линиями показаны ребра графа.

Теорема 1. *Для любого $m\geqslant 4$ подкод кода $\mathsf{RM}(2,m)$ вида (1.2) стабилен тогда и только тогда, когда соответствующий граф обладает свойством P.*

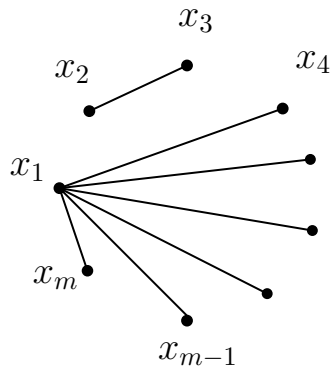


Рис. 1.1. Случай $\deg(x_1) = m - 3$

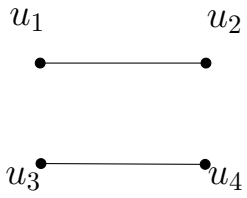


Рис. 1.2. Граф H

Доказательство. Обозначим через $G = (V, E)$ граф, соответствующий подкоду вида (1.2). Отметим, что условие (1.3) эквивалентно тому, что любой индуцированный подграф графа G на четырех вершинах содержит подграф, изоморфный графу H, изображенному на Рис. 2. Ребра $\{u_1, u_2\}$ и $\{u_3, u_4\}$ соответствуют мономам степени 2, используемым для получения монома $u_1u_2u_3u_4$. Также заметим, что для того, чтобы показать, что подкод (1.2) стабильный, достаточно доказать, что любой моном степени четыре может быть представлен как произведение двух мономов из кода. То же самое верно и для всех мономов степени 3. Действительно, для произвольного монома $u_1u_2u_3$ верно, что как минимум один из мономов u_1u_2, u_1u_3 или u_2u_3 лежит в коде. В противном случае моном $u_1u_2u_3v$ невозможно будет получить в результате операции возведения в квадрат. Мономы степени один лежат в коде по определению.

Для доказательства необходимости зафиксируем произвольную вершину v. Если отсутствуют любые три индуцированные ребра $\{v, u_j\}$ для $j = 1, 2, 3$, то индуцированный подграф на вершинах v, u_1, u_2, u_3 не будет содержать искомый подграф H. Противоречие доказывает, что $\deg(v) \geqslant m - 3$. Однако, если $\deg(v) = m - 3$ и $\{v, u_1\} \notin E$, $\{v, u_2\} \notin E$, то $\{u_1, u_2\} \in E$, т.к. иначе ни один из индуцированных подграфов на четырех вершинах, содержащий вершины v, u_1 и u_2, не будет иметь искомого подграфа. То есть выполнено свойство P.

Достаточность. Зафиксируем любой индуцированный подграф на четырех вершинах (назовем их v, u_1, u_2 и u_3). Отметим, что он удовлетворяет свойству P

для $m = 4$. Если вершина v имеет степень один, т.е. $\{v, u_1\} \in E$, но $\{v, u_2\} \notin E$, $\{v, u_3\} \notin E$, тогда из свойства P следует, что $\{u_2, u_3\} \in E$. Поэтому в подграфе, изоморфном графу H обязательно должны содержаться ребра $\{v, u_1\}$ и $\{u_2, u_3\}$.

Если все четыре вершины подграфа имеют степень как минимум два, то в нем существует простой цикл длины три или четыре. В случае, когда цикл имеет длину четыре, наличие подграфа, изоморфного H, очевидно. Иначе в графе есть треугольник $\{u_1, u_2, u_3\}$ и вершина v степени как минимум два. Предположим (без ограничения общности), что $\{v, u_1\} \in E$, тогда в искомый подграф войдут ребра $\{v, u_1\}$ и $\{u_2, u_3\}$. □

Из Теоремы 1 минимальное число ребер достигается в случае, когда граф обладает свойством P и степень каждой вершины есть $m-3$. Осталось описать такие графы.

Утверждение 18. *Пусть $m \geqslant 4$. Если некоторый граф G с m вершинами, степень каждой из которых есть $m - 3$, обладает свойством P, то дополнительный граф $\overline{G}$ представляет собой объединение циклов длины как минимум 4.*

Доказательство. Поскольку степень каждой вершины графа G равна $m - 3$, то степень каждой вершины графа $\overline{G}$ равна двум. Более того, из второго пункта свойства P следует, что если граф $\overline{G}$ содержит ребро $\{v, u_1\}$ и $\{v, u_2\}$, то он не содержит ребра $\{u_1, u_2\}$. Поэтому в графе $\overline{G}$ нет треугольников. Выберем произвольную вершину u_1. Она не изолированная, поэтому можно выбрать вершину, смежную с ней. Назовем ее u_2. Поскольку $\deg(u_2) = 2$, то существует смежная с ней вершина $u_3 \neq u_1$. Продолжаем рассуждение до тех пор, пока вершина u_j не совпадет с одной из вершин $u_1, \ldots, u_{j-1}$. Отметим, что u_j не может совпасть с u_i при $i > 1$, т.к. это бы означало, что $\deg(u_i) \geqslant 3$. Отсюда вершины $u_1, \ldots, u_{j-1}$ образуют простой цикл. Причем его длина не меньше четырех, поскольку в графе $\overline{G}$ нет треугольников. □

Таким образом, мы описали структуру графа, соответствующего минимальному стабильному подкоду вида (1.2). Теперь полностью опишем структуру кодов такого типа.

Утверждение 19. *Пусть $m \geqslant 4$. Если некоторый граф G с m вершинами, обладает свойством P, то дополнительный граф $\overline{G}$ представляет собой объединение циклов длины как минимум 4 или является простым путем.*

Доказательство. Действуем как в доказательстве Утверждения 18, пытаясь найти цикл в графе $\overline{G}$. Только в этот раз мы можем остановиться в вершине степени один, в результате чего образуется простой путь. Изолированные вершины являются простым путем по определению. □

Теорема 2. *Для любого $m \geqslant 4$ верно, что*

$$w(m, 2) = \frac{m(m-3)}{2}.$$

Доказательство. На основе замечания после Теоремы 1 для вычисления значения $w(m, 2)$ необходимо посчитать все подкоды, соответствующие графам, удовлетворяющим свойству P, степень каждой вершины которых равна $m - 3$. Из Утверждения 18 следует, что граф $\overline{G}$ имеет в точности m ребер. Отсюда граф G имеет не менее $\binom{m}{2} - m = m(m-3)/2$ ребер. □

Теорема 2 позволяет гарантировать стабильность при удалении из полного кода произвольных m мономов второй степени.

Следствие 3. *Удаление любых m мономов степени 2 из базиса кода $\mathsf{RM}(2, m)$ гарантировано дает стабильный подкод.*

Доказательство. Удаление m мономов из базиса полного кода Рида–Маллера $\mathsf{RM}(2, m)$ оставляет в этом базисе $m(m-3)/2$ мономов степени 2, что согласно Теореме 17 гарантирует выполнение свойства стабильности. □

Еще одним результатом Теоремы 2 является способ построения нестабильного подкода: требуется исключить из полного кода как минимум $m+1$ моном второй степени.

Следствие 4. *Удаление $m+1$ или более мономов степени 2 из базиса кода $\mathsf{RM}(2,m)$ гарантировано дает нестабильный подкод.*

Доказательство. По Теореме 17 минимальное число мономов степени 2 в подкоде кода $\mathsf{RM}(2,m)$ должно быть равно $m(m-3)/2$, однако удаление $m+1$ и более монома дает максимально $m(m-3)/2-1$ моном. □

1.2. Электронная подпись на подкодах кодов $\mathsf{RM}(r,m)$

Теперь перейдем к решению аналогичной задачи в общем случае, когда $r>2$. То есть будем искать минимальное число $w(m,r)$ такое, что код

$$\operatorname{span}\big(\mathsf{RM}(r-1,m)\cup\{f_1,\ldots,f_{w(m,r)}\}\big) \tag{1.5}$$

стабилен. Здесь через f_i обозначены уже мономы степени r.

Сопоставим подкоду $\mathcal{A}\subset\mathsf{RM}(r,m)$ гиперграф $G=(V,E)$ с набором вершин $V=\{x_1,\ldots,x_m\}$. r-ребро $\{x_{i_1},\ldots,x_{i_r}\}\in E$ тогда и только тогда, когда моном $x_{i_1}\ldots x_{i_r}\in\mathcal{A}$. Аналогом рассмотренного в предыдущей главе условия наличия в каждом индуцированном подграфе на 4 вершинах подграфа, изоморфного графу H, является требование коду (1.5) быть стабильным. А именно, каждый набор из $2r$ вершин должен быть покрыт двумя непересекающимися r-ребрами. Будем называть граф, удовлетворяющий этому условию *стабильным графом*. Замечания о покрытии мономов меньших степеней остаются теми же, что и в случае $r=2$.

Также можно обобщить соотношение (1.4) из Раздела 1.1 как:

$$q(m,r)=\binom{m}{r}-w(m,r).$$

Как и там, не будем останавливаться отдельно на поиске значения $q(m,r)$.

Далее будем использовать понятия «граф» и «гиперграф» взаимозаменяемо. Обозначим через $w(r,m)$ минимальное число мономов степени r, которое необходимо для того, чтобы подкод вида (1.5) был стабильным или, в графовой интерпретации, минимальное число ребер в стабильном r-гиперграфе на m вершинах.

Утверждение 20. *Для любого натурального r и $m \geqslant 2r$ выполнено*

$$w(m,r) \geqslant \frac{\binom{m}{2r}}{\binom{m-r}{r}}.$$

Доказательство. Отметим, что любое множство из $2r$ вершин в стабильном графе содержит как минимум одно ребро. Более того, любое ребро содержится в точности в $\binom{m-r}{r}$ таких множествах. Поэтому суммарное число ребер, умноженное на $\binom{m-r}{r}$, есть как минимум число всех множеств из $2r$ вершин, которых $\binom{m}{2r}$. Это дает искомую оценку. □

Следствие 5. *Любой стабильный граф содержит не менее $1/\binom{2r}{r}$ ребер полного графа.*

Доказательство. Суммарное число всех r-ребер в графе на m вершинах есть $\binom{m}{r}$. Тогда

$$\frac{w(m,r)}{\binom{m}{r}} = \frac{\binom{m}{2r}}{\binom{m-r}{r}\binom{m}{r}} = \frac{(r!)^2}{(2r)!} = \frac{1}{\binom{2r}{r}}.$$

□

Полученная в Утверждении 20 нижняя оценка числа $w(m,r)$ может быть уточнена. Улучшенный результат сформулирован в Теореме 3.

Теорема 3. *Для любого натурального r и $m \geqslant 2r$ выполнено*

$$w(m,r) \geqslant \frac{1}{2}\left(\sqrt{(\gamma+1)^2 + 8\cdot\binom{m}{2r}} + \gamma + 1\right), \text{ где } \gamma = \sqrt{\sum_{u=\max\{1,3r-m\}}^{r-1}\binom{r}{u}}.$$

Доказательство. Зафиксируем наименьшее множество ребер E такое, что каждые $2r$ вершины графа покрыты двумя непересекающимися ребрами из E. По определению $|E| = w(m,r)$.

Зафиксируем любое ребро $e \in E$. Обозначим через E_e множество ребер из E, пересекающихся с e, а через P_e — множество неупорядоченных пар $\{e', e''\}$, $e', e'' \in E_e$. Каждая пара $\{e', e''\}$ соответствует подмножеству $B \subset e$, $B = (e' \cup e'') \cap e$. Аналогично каждому ребру из E_e соответствует подмножество $B = e' \cap e$.

С другой стороны зафиксируем произвольное подмножество $B \subset e$ размера

$$\max\{1, 3r - m\} \leqslant |B| \leqslant r - 1. \tag{1.6}$$

Т.к. $|B| \geqslant 3r - m$, то $|V \setminus e| + |B| \geqslant 2r$ и существует множество S такое, что $|S| = 2r, S \cap e = B$. По предположению множество ребер E содержит пару ребер, покрывающих S. Обозначим эти ребра через e' и e''. Возможны два случая: либо оба ребра e' и e'' пересекаются с e, либо с e пересекается только одно из них. Таким образом, мы можем сопоставить подмножеству B элемент из $E_e \cup P_e$. Обратим внимание на то, что несмотря на то, что подмножество B может соответствовать нескольким элементам $E_e \cup P_e$, обратное отображение является однозначным. Таким образом, мы можем написать

$$|P_e| + |E_e| \geqslant \sum_{u=\max\{1,3r-m\}}^{r-1} \binom{r}{u} = \gamma^2,$$

где справа стоит число всех подмножеств $B \subset e$, удовлетворяющих условию (1.6).

Очевидно, что $|P_e| = \binom{|E_e|}{2}$. Тогда

$$\binom{|E_e|}{2} + |E_e| \geqslant \gamma^2 \;\Leftrightarrow\; |E_e|^2 + |E_e| \geqslant 2\gamma^2.$$

Из этого неравенства следует, что $|E_e| \geqslant \gamma$ (здесь используется тот факт, что γ не может лежать в интервале $(0, 1)$, поскольку по определению представляет собой квадратный корень из нуля или натурального числа).

Теперь мы можем оценить мощность множества P всех неупорядоченных пар $\{e', e''\}$ ребер из E. Обозначим через $\widehat{P}$ множество всех непересекающихся неупорядоченных пар ребер из E. Понятно, что

$$P = \widehat{P} \cup \bigcup_{e \in E} \big\{\{e', e\} : e' \in E_e\big\}$$

и, более того,

$$|P| = |\widehat{P}| + \frac{1}{2}\sum_{e\in E}|E_e|,$$

поскольку множество $\widehat{P}$ не пересекается со вторым множеством. и, проходя по всем $e \in E$, мы считаем каждую пересекающуюся неупорядоченную пару ровно дважды.

Из того, что ребра из E покрывают каждое множество размера $2r$, заключаем, что $|\widehat{P}| \geqslant \binom{m}{2r}$. Тогда

$$|P| - \frac{1}{2}\sum_{e\in E}|E_e| \geqslant \binom{m}{2r}.$$

Т.к. $|P| = \binom{|E|}{2} = \binom{w(m,r)}{2}$, можно переписать последнее неравенство как

$$\binom{w(m,r)}{2} - \frac{w(m,r)\gamma}{2} \geqslant \binom{m}{2r}.$$

Решая квадратное неравенство

$$w(m,r)^2 - w(m,r)(\gamma+1) - 2\cdot\binom{m}{2r} \geqslant 0,$$

получаем условие теоремы. □

Перейдем к доказательству верхней оценки. Зафиксируем наибольшее возможное множество $\mathcal{S}$, состоящее из множеств $S_i \subset V$ размера $2r$ таких, что

$$\max_{i,j}|S_i \cap S_j| \leqslant h.$$

Сначала докажем вспомогательную лемму.

Лемма 1. *Если $h < r/3$, то для любого множества $Q \notin \mathcal{S}, |Q| = 2r$ существует не более двух множеств из $\mathcal{S}$ таких, что их пересечение с Q имеет размер не менее r.*

Доказательство. Предположим, что множество Q пересекается как минимум с тремя множествами так, что размер каждого из пересечений больше или равен r. Без ограничения общности предположим, что это множества S_1, S_2 и S_3.

Обозначим $Q \cap S_1 = A_1$, $Q \cap S_2 = A_2$, $Q \cap S_3 = A_3$. Поскольку $|Q| = 2r$, то очевидно, что $|A_1 \cup A_2 \cup A_2| \leqslant 2r$. С другой стороны, по формуле включений-исключений

$$|A_1 \cup A_2 \cup A_2| \geqslant |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|.$$

Тогда

$$\sum_{i=1}^{3} |A_i| \leqslant 2r + 3h.$$

По условию $|A_i| \geqslant r$ для любого $i \in \{1, 2, 3\}$, следовательно

$$\sum_{i=1}^{3} |A_i| \geqslant 3r.$$

Откуда $3r \leqslant 2r + 3h$ и $h \geqslant r/3$, что противоречит условию леммы. □

Построение верхней оценки $w(m, r)$ будем выполнять через поиск максимально возможного числа ребер, которое может быть исключено из полного графа так, чтобы оставшийся граф сохранил свойство стабильности.

Теорема 4. *Для любого натурального $r \geqslant 2$, $m \geqslant 2r$ и $h < r/3$*

$$w(m, r) \leqslant \binom{m}{r} - T(r, m, h) \cdot \left(\binom{2r}{r} - 2 \right),$$

где

$$T(r, m, h) = \max \big\{ t : \exists S_1, \ldots, S_t \left(S_i \subset \{1, \ldots, m\} \ \& \right.$$
$$\left. \& \, |S_i| = 2r \ \& \ (i \neq j \Rightarrow |S_i \cap S_j| \leqslant h), \ i, j \in \{1, \ldots, t\} \right) \big\}.$$

Доказательство. Заметим, что двух непересекающихся r-ребер достаточно, чтобы покрыть набор из $2r$ вершин. Таким образом, можно удалить $\delta = \left(\binom{2r}{r} - 2 \right)$ r-ребер из полного графа на $2r$ вершинах и сохранить свойство стабильности. Очевидно, что больше ребер удалить нельзя.

Предположим, что из каждого множества, входящего в $\mathcal{S}$, удалено δ ребер так, что каждое из множеств покрыто не менее, чем двумя r-ребрами. Остается

проверить, что существует подобное покрытие для любого набора из $2r$ вершин. Поскольку по построению заведомо можно покрыть любое множество S_i, осталось показать что можно покрыть и любое множество $Q \notin S$, $|Q| = 2r$.

Заметим, что если мощность пересечения Q с некоторым S_i не превосходит $(r-1)$, то удаление ребер в S_i не влияет на количество ребер в Q. В то же время, согласно Лемме 1, при $h < r/3$ любое множество размера $2r$ может иметь пересечение размера не менее r не более чем с двумя множествами из $\mathcal{S}$. Если есть только один такой набор, скажем S_1, то возможны два случая:

1) $|Q \cap S_1| = 2r - 1$. В этом случае существует ребро $e_1 \in Q \cap S_1$, не содержащее вершину v, $\{v\} = S_1 \setminus Q$ (поскольку S_1 должно быть покрыто двумя непересекающимися ребрами). В качестве второго ребра можно взять $e_2 = Q \setminus e_1$ (отметим, что $e_2 \in E$, поскольку были удалены только ребра, содержащиеся во множествах S_i). Тогда пара непересекающихся ребер $\{e_1, e_2\}$ образует покрытие Q.

2) $|Q \cap S_1| < 2r - 1$. В этом случае во множестве $Q \setminus S_1$ лежит не менее двух вершин. Пусть это вершины v_1 и v_2. Тогда покрытие может быть получено двумя непересекающимися ребрами $e_1, e_2 \subset Q$ такими, что $v_1 \in e_1$, $v_2 \in e_2$.

Теперь рассмотрим случай, когда с Q по не менее чем r вершинам пресекаются два множества S_1 и S_2. Предположим, что $|A_1| > r + h$. Тогда по формуле включений-исключений верно, что $|A_1 \cap A_2| = |A_1| + |A_2| - |A_1 \cup A_2| > r+h+r-2r = h$, что противоречит условию $|S_1 \cap S_2| \leqslant h$. Отсюда $r \leqslant |A_i| \leqslant r+h$ для $i \in \{1, 2\}$. Поэтому из Q может быть исключено не более $2 \cdot \binom{r+h}{r}$ ребер. Отметим, что

$$\frac{\binom{2r}{r}}{2 \cdot \binom{r+h}{r}} = \frac{(2r)!\, r!\, h!}{2r!\, r!\, (r+h)!} = \frac{1}{2} \cdot \frac{2r}{r+h} \cdot \frac{2r-1}{r+h-1} \cdot \ldots \cdot \frac{r+1}{h+1}.$$

Последний множитель больше двух для $r > 3$. Для остальных множителей верно, что

$$\frac{2r-i}{r+h-i} > \frac{2r}{r+h} > \frac{6}{4}.$$

Отсюда для $r > 3$

$$\frac{\binom{2r}{r}}{2 \cdot \binom{r+h}{r}} > \frac{1}{2}\left(\frac{3}{2}\right)^{r-1} \cdot 2 > 2.$$

Для $r = 2$ и $r = 3$ аналогичное неравенство может быть проверено непосредственно. В Q входит $\binom{2r}{r}/2$ пар непересекающихся ребер, поэтому после удаления из него $2 \cdot \binom{r+h}{r} < \binom{2r}{r}/2$ ребер остается как минимум одна такая пара.

Таким образом, граф, полученный после удаления из полного графа δ ребер для каждого множества из $\mathcal{S}$, стабилен. Остается напомнить, что $|\mathcal{S}|$ есть число множеств размера $2r$, которые пересекаются по не более, чем h элементам, то есть $|\mathcal{S}| = T(r, m, h)$. □

Замечание 1. В работе [75] П. Эрдеша и Дж. Спенсера вводится величина $\mathbf{m}(n, k, t)$, которую будем выделять жирным шрифтом для того, чтобы отделить от величины m. Она обозначает размер наибольшего множества подмножеств $\{1, \ldots, n\}$ размера k таких, что любые два члена этого множества пересекаются менее, чем по t элементам. Позже В. Редль [76] доказал, что

$$\lim_{n\to\infty} \mathbf{m}(n, k, t) = \frac{\binom{n}{t}}{\binom{k}{t}}.$$

То есть, в нашем случае

$$\lim_{m\to\infty} T(r, m, h) = \lim_{m\to\infty} \mathbf{m}(m, 2r, \lfloor r/3 \rfloor) = \frac{\binom{m}{\lfloor r/3 \rfloor}}{\binom{2r}{\lfloor r/3 \rfloor}}.$$

Верхняя оценка может быть улучшена эмпирическим методом. Для этого построим Алгоритм 1, который получает на вход множество вершин V и возвращает множество ребер $E \subset V \times V$ такое, что в полученном графе каждое множество из $2r$ вершин покрыто двумя непересекающимися r-ребрами. Полная программная реализация Алгоритма 1 приведена в Приложении А.

Алгоритм 1 Жадный алгоритм для построения r-покрытия

Вход: V — множество вершин и r — мощность ребер

Выход: Множество r-ребер E, которое покрывает множество V

Функция `ChooseEdge`**:**

$e := \varnothing$;

цикл $i = 1, \ldots, r$ **выполнять**

$V' := \{v \in V :$ вершина v может быть добавлена к ребру $e\}$;

$v := \arg\min_{v \in V'} \deg(v)$;

$e := e \cup \{v\}$;

конец

вернуть e

Функция `Main`**:**

$E := \varnothing$;

до тех пор, пока E *не покрывает все вершины* V **выполнять**

$e :=$ `ChooseEdge`();

$E := E \cup \{e\}$;

конец

вернуть E

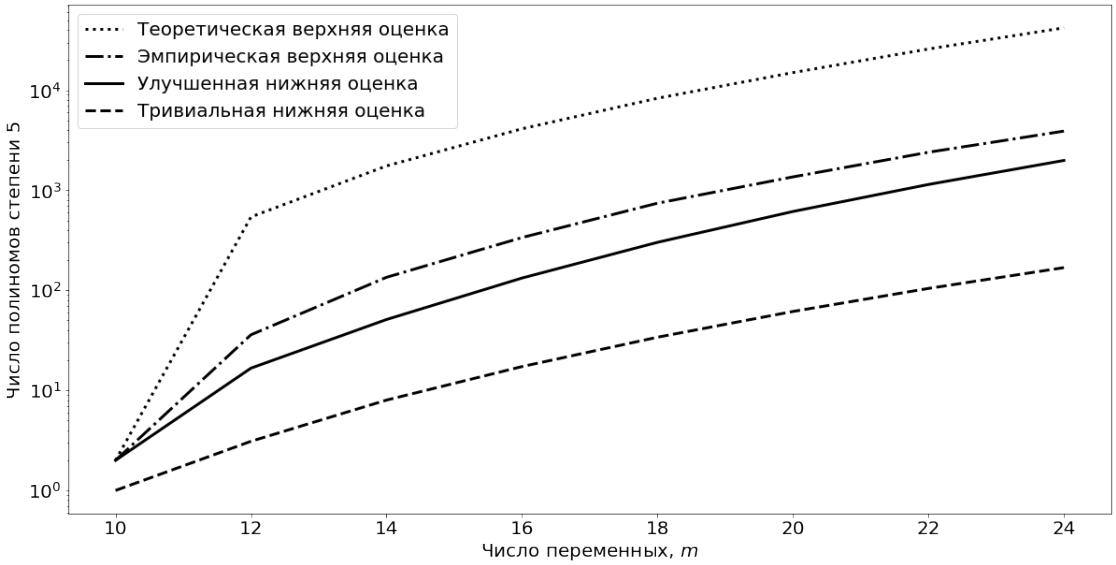
Точность результатов работы алгоритма может быть показана через сравнение с полученными выше теоретическими оценками. Так на Рис. 1.3 представлены две нижние и две верхние оценки, которые были получены в Утверждении 20, Теореме 3, Теореме 4 и в результате применения Алгоритма 1 для фиксированного параметра $r = 5$. По рисунку видно, что улучшенные оценки достаточно близки друг к другу.

1.3. Доля нестабильных подкодов кодов $\mathsf{RM}(r, m)$

В этом разделе будем рассматривать подкоды кодов Рида–Маллера, заданные стандартным базисом и имеющие коразмерность ℓ.

Для заданного параметра s и множества $I = \{i_j\}_{j=1}^{s}$ будем называть неупо-

Рис. 1.3. Сравнение оценок



рядоченные пары $\{A, B\}$ *критическим разбиением*, если выполнена следующая система условий:

$$\begin{cases} A \cap B = \varnothing, \\ A \cup B = I, \\ 1 \leqslant |A|, |B| \leqslant r. \end{cases}$$

Критические разбиения могут быть связаны с нестабильными подкодами $\mathsf{RM}(r, m)$ через следующее утверждение.

Утверждение 21. *Подкод кода* $\mathsf{RM}(r, m)$ *является нестабильным тогда и только тогда, когда из каждого критического разбиения для некоторого монома* $x_{i_1} \dots x_{i_s}$ *удален как минимум один элемент.*

Доказательство. Если моном $x_{i_1} \dots x_{i_s}$ входит в квадрат кода, то он должен быть образован парой $\{A, B\}$ из соответствующего критического разбиения. Но по условию либо A, либо B отсутствует. □

Утверждение 22. *Для заданного параметра* s *и произвольного множеств* I *размера* s *число критических разбиений этого множества есть*

$$v(s) = \frac{1}{2} \sum_{p=\max\{s-r,1\}}^{\min\{r,s-1\}} \binom{s}{p}.$$

Доказательство. С одной стороны, размеры подмножеств не должны превышать r. С другой стороны, разбиение должно быть нетривиальным, то есть разбиение на пустое множество и множество, совпадающее с I, недопустимо. Наконец, при рассмотрении всех разбиений каждая пара считается дважды. $\square$

Упорядочим каким-либо образом (скажем, лексикографически) элементы каждого критического разбиения, а затем и сами критические разбиения. Теперь рассмотрим любое множество M, состоящее из элементов критических разбиений и удовлетворяющее свойству, что для каждого критического разбиения M содержит хотя бы один его элемент. Множество M может быть закодировано строкой $\alpha \in \{1,2,3\}^{v(s)}$, где

$$\alpha_j = \begin{cases} 1 & \Leftrightarrow \text{ 1-ый элемент } j\text{-ой пары лежит в } M\text{, а 2-ый — нет,} \\ 2 & \Leftrightarrow \text{ 2-ый элемент } j\text{-ой пары лежит в } M\text{, а 1-ый — нет,} \\ 3 & \Leftrightarrow \text{ оба элемента } j\text{-ой пары лежат в } M. \end{cases}$$

Для того, чтобы обозначить множество, соответствующее заданной $\alpha \in \{1,2,3\}^{v(s)}$ будем писать $M(\alpha)$. Тогда

$$|M(\alpha)| = \#_1(\alpha) + \#_2(\alpha) + 2 \cdot \#_3(\alpha),$$

где $\#_c(\alpha)$ есть число символов c в строке α.

Используем множество M для построения верхней оценки числа θ нестабильных подкодов кода $\mathsf{RM}(r,m)$.

Теорема 5. *Число нестабильных подкодов кода* $\mathsf{RM}(r,m)$ *есть*

$$\theta \leqslant \sum_{s=2}^{2r} \tbinom{m}{s} \cdot \sum_{\alpha \in \{1,2,3\}^{v(s)}} \tbinom{k-1-2v(s)}{\ell-|M(\alpha)|} + \tbinom{k-1}{\ell-1}.$$

Доказательство. Существует ровно два вида нестабильных подкодов: содержащие моном 1 и не содержащие его. Число подкодов второго типа равно $\binom{k-1}{\ell-1}$, где k — размерность кода $\mathsf{RM}(r,m)$.

Зафиксируем параметр s, набор индексов I размера s и строку $\alpha \in \{1,2,3\}^{v(s)}$. Среди подкодов первого типа есть

$$\binom{k-1-2v(s)}{\ell-|M(\alpha)|},$$

обладающих свойством: среди мономов, составляющих критическое разбиение для I, отсутствуют все мономы из $M(\alpha)$. Дело в том, что нужно выбрать $\ell - |M(\alpha)|$ мономов из всех, имеющих степень больше нуля и не входящих ни в одно критическое разбиение (их $k-1-2v(s)$).

Для заданного s существуют $\binom{m}{s}$ вариантов выбрать I. Однако некоторые коды могут быть посчитаны несколько раз. Теорема доказана. □

Теорема 6. *Если $\ell = const$ и $r \geqslant 2\ell+1$, то доля нестабильных подкодов кодов $\mathsf{RM}(r,m)$ стремится к нулю при $m \to \infty$.*

Доказательство. Нашей целью является асимптотическая оценка вероятности того, что после удаления ℓ векторов из стандартного базиса кода $\mathsf{RM}(r,m)$ квадрат полученного кода будет отличаться от $\mathsf{RM}(2r,m)$. Верхняя оценка равна $\theta/\binom{k}{\ell}$. Разделим ее на две части и покажем стремление к нулю для каждой из них независимо. Для одного из них это сразу следует из того, что

$$\frac{\binom{k-1}{\ell-1}}{\binom{k}{\ell}} = \frac{\ell}{k} \xrightarrow[m\to\infty]{} 0,$$

поскольку $k \to \infty$ при $m \to \infty$.

Теперь рассмотрим первую часть и обозначим ее числитель через γ. Заметим, что

$$\#_\alpha(1) + \#_\alpha(2) + 2 \cdot \#_\alpha(3) = |M(\alpha)| \geqslant v(s) = \#_\alpha(1) + \#_\alpha(2) + \#_\alpha(3).$$

Тогда количество удаленных векторов, являющихся элементами критических разбиений для s, равно $|M(\alpha)| \geqslant v(s)$, а общее количество удаленных векторов равно ℓ. То есть $v(s) \leqslant \ell$ и можно рассматривать только параметры s, удовлетворяющие этому условию. Тогда

$$2v(s) = \sum_{p=\max\{s-r,1\}}^{\min\{r,s-1\}} \binom{s}{p} \leqslant 2\ell. \tag{1.7}$$

Рассмотрим отдельно два случая. Если $s \geqslant r+1$, то $\min\{r, s-1\} = r$ и в сумму (1.7) входит элемент $\binom{s}{r}$. Отсюда

$$2\ell \geqslant 2v(s) \geqslant \binom{s}{r} \geqslant s.$$

Последнее неравенство следует из того, что

$$\binom{s}{r} = \frac{(r+1)}{2} \cdot \frac{(r+2)}{3} \cdot \ldots \cdot \frac{(s-1)}{r} \cdot \frac{s}{1}.$$

Если, с другой стороны, $s < r+1$, то $\max\{s-r, 1\} = 1$ и в сумму (1.7) входит элемент $\binom{s}{1}$. Следовательно,

$$2\ell \geqslant 2v(s) \geqslant \binom{s}{1} = s.$$

Т.е. в любом случае выполняется неравенство $s \leqslant 2\ell$.

Упростим верхнюю оценку для γ, используя это неравенство и монотонность биномиального коэффициента $\binom{n}{k}$ относительно параметра k, что гарантирует рост величины $\binom{n}{k}$ с ростом k:

$$\sum_{s=2}^{2r} \binom{m}{s} \sum_{\alpha \in \{1,2,3\}^{v(s)}} \binom{k-1-2v(s)}{\ell - |M(\alpha)|} \leqslant \sum_{s=2}^{2\ell} \binom{m}{2\ell} \sum_{\alpha \in \{1,2,3\}^{v(s)}} \binom{k-1-2v(s)}{\ell - |M(\alpha)|} \leqslant$$
$$\leqslant 2\ell \cdot \binom{m}{2\ell} \max_{s \in [2, 2\ell]} \left\{ \binom{k-1-2v(s)}{\ell - z} \cdot 3^{v(s)} \right\},$$

где $z = \min_{\alpha \in \{1,2,3\}^{v(s)}} \{|M(\alpha)|\}$.

Отметим справедливость неравенства $v(s) < 2^s$, поскольку

$$2^s = (1+1)^s = \sum_{p=0}^{s} \binom{s}{p} > \frac{1}{2} \sum_{p=\max\{s-r,1\}}^{\min\{r,s-1\}} \binom{s}{p} = v(s).$$

Кроме того, поскольку $s \leqslant 2\ell$, то $3^{v(s)} \leqslant c$ для некоторой константы c. Эти рассуждения в совокупности с монотонностью биномиального коэффициента $\binom{n}{k}$ относительно n и неравенством $|M(\alpha)| \geqslant v(s)$ позволяют получить следующую верхнюю оценку:

$$2c\ell \cdot \binom{m}{2\ell} \binom{k}{\ell - v(s)} \leqslant 2c\ell \cdot \binom{m}{2\ell} \binom{k}{\ell - 1} = \psi.$$

Перейдем к оценку доли подкодов:

$$\frac{\gamma}{\binom{k}{\ell}} \leqslant \frac{\psi}{\binom{k}{\ell}} = \frac{2c\ell \cdot \binom{m}{2\ell}\binom{k}{\ell-1}}{\binom{k}{\ell}} = 2c\ell \cdot \binom{m}{2\ell} \cdot \ell/(k-\ell+1) = \\ = \frac{2c\ell \cdot \binom{m}{2\ell}}{k-\ell+1} \leqslant 2c\ell \cdot \frac{m^{2\ell}}{2k}.$$

Для достаточно большого m можно утверждать, что существует такое $p = 2\ell + 1$, что в представление (1) для k входит слагаемое $\binom{m}{p} \geqslant m^p$. Тогда

$$2c\ell \cdot \frac{m^{2\ell}}{2k} \leqslant 2c\ell \cdot \frac{m^{2\ell}}{m^{2\ell+1}} = 2c\ell \cdot \frac{1}{m} \xrightarrow[m\to\infty]{} 0.$$

Теорема доказана. □

1.4. Выводы к первой главе

Глава посвящена описанию подкодов кода Рида–Маллера, позволяющих построить вариант электронной подписи CFS, являющейся стойкой к полиномиальной атаке из работы [37]. Такие подкоды получили в диссертации название «нестабильные». В работе построен критерий для выявления таких кодов порядка 2. Помимо этого диссертация описывает структуру всех стабильных подкодов кода $\mathsf{RM}(2, m)$. На основе полученных результатов представлен метод построения нестабильного подкода, который может быть полезен для практических приложений.

Для кода Рида–Маллера $\mathsf{RM}(r, m)$ произвольного порядка построен ряд оценок, ограничивающих снизу и сверху число векторов степени r, подлежащих исключению из кода для того, чтобы квадрат результата перестал совпадать с квадратом полного кода. Полученные оценки также могут быть использованы для построения нестабильного подкода, однако без гарантии его оптимальности.

Тем не менее, построение нестабильного подкода случайным образом маловероятно: в настоящей диссертации показано, что доля таких подкодов стремится к нулю с увеличением параметра m. Из этого следует, что при случайном

выборе подкода кода Рида–Маллера вероятность построения стойкой схемы подписи на таких кодах также стремится к нулю.

Глава 2

Генерация ключей в электронной подписи CFS на основе квазициклических кодов

Алгоритм генерации ключей криптосистемы с открытым ключом LEDAcrypt, предложенной в рамках конкурса NIST на новый постквантовый механизм (см. [49]), требует нахождение невырожденной квадратной квазициклической матрицы Q. Идентичный алгоритм генерации ключей позднее был внедрен в схему подписи CFS [54]. Однако рекомендации по поиску такой матрицы в работе [54] отсутствуют. Авторы [49] предлагают представить матрицу Q как матрицу многочленов и по ней составить матрицу весов, заменив каждый многочлен на число, равное количеству его ненулевых коэффициентов. Такой подход позволяет вывести необходимое условие невырожденности матрицы Q через перманент матрицы весов. Это условие может быть применимо для построения ключей в LEDAcrypt, поскольку для любого уровня стойкости максимальный размер матрицы Q как блочной не превосходит 4×4. Но экспоненциальная сложность вычисления перманента делает невозможной проверку его значения, например, для матриц размера 63×63, которые предложены для схемы подписи CFS для уровня стойкости, равного 128 бит.

Подход авторов LEDAcrypt, заключающийся в представлении квазициклической матрицы как матрицы над факторкольцом кольца многочленов, позволяет свести задачу поиска невырожденной квадратной квазициклической матрицы Q к задаче построения случайной невырожденной матрицы над факторкольцом кольца многочленов. Этот вопрос давно изучен для конечных полей, но для колец представляет более сложную задачу. Сложным является даже вычисление определителя матрицы, ведь классический алгоритм Гаусса неприменим к кольцам, в которых есть делители нуля. Также нетривиальным является вопрос, чему равна доля невырожденных матриц над данным конечным кольцом,

в то время как в случае конечных полей этот вопрос также имеет простой ответ.

Для решения вопросов, поставленных в настоящей главе, используется алгоритм приведения матрицы над факторкольцом кольца многочленов к верхнетреугольному виду. В работе [77] для решения аналогичной задачи предложено два алгоритма. Первый с оценкой сложности $O(n^3)$ арифметических операций и применений расширенного алгоритма Евклида, а второй — со сложностью $O(n^\omega)$ операций того же типа, где ω — экспонента матричного умножения (т.е. минимальное ω, для которого сложность умножения двух матриц размера $n \times n$ есть $O(n^\omega)$). Несмотря на то, что формально второй алгоритм имеет меньшую сложность (известна оценка $\omega < 2.373$ [78]), на практике даже для достаточно больших матриц более целесообразно применение первого. Поэтому приведенный в диссертации алгоритм является адаптацией первого алгоритма из [77].

Результаты главы опубликованы в работе [65].

2.1. Дополнительные определения

Некоторая часть результатов главы получена относительно факторкольца $K_f = \mathbb{F}_2[x]/f(x)$ кольца многочленов над $\mathbb{F}_2[x]$. В некоторых случаях будет зафиксирован определенный вид этого многочлена.

Поставим кольцо циркулянтов порядка r во взаимно однозначное соответствие с факторкольцом $\mathbb{F}_2[x]/(x^r-1)$ (то есть кольцом многочленов по модулю x^r-1). Именно, циркулянту $A \in \mathbb{F}_2^{r\times r}$ с первым столбцом $\widehat{a}$ будет соответствовать многочлен $\widehat{a}_1 + \widehat{a}_2 x + \ldots + \widehat{a}_r x^{r-1}$. Несложно показать, что указанное отображение является изоморфизмом, то есть сохраняет операции сложения и умножения.

Определение 33. *Весом* многочлена $f(x) \in \mathbb{F}_2[x]$ назовем количество его ненулевых коэффициентов.

Очевидно, что вес многочлена степени не более $r-1$ и вес соответствующего ему циркулянта равны. Вес многочлена $f(x)$ будем обозначать $\mathrm{wt}\big(f(x)\big)$,

его четность (то есть остаток от деления на 2) — $\mathrm{wt}_2\big(f(x)\big) \in \mathbb{F}_2$.

Определение 34. Матрицу $M(Q) \in K_{x^r-1}^{n\times n}$, полученную заменой в некоторой квадратной квазициклической матрице Q порядка n каждого циркулянта Q_{ij} на многочлен m_{ij}, будем называть *матрицей многочленов*.

Определение 35. Матрицу $W \in \mathbb{F}_2^{n\times n}$, полученную из матрицы многочленов $M \in K_{x^r-1}^{n\times n}$ заменой $w_{ij} = \mathrm{wt}_2(m_{ij})$, будем называть *матрицей четности весов* матрицы M и будем обозначать $W = \mathrm{wt}_2(M)$.

Определение 36. Для произвольного коммутативного кольца K с единицей набор векторов $u_1, \ldots, u_k \in K^n$, $k, n \geqslant 1$ будем называть *линейно независимым*, если для любых элементов $\alpha_1, \ldots, \alpha_k \in K$, одновременно не равных нулю, верно

$$\alpha_1 u_1 + \ldots + \alpha_k u_k \neq 0.$$

Пустой набор векторов будем считать линейно независимым по определению.

Определение 37. Для произвольного коммутативного кольца K с единицей матрица $A \in K^{n\times n}$ называется *невырожденной*, если ее определитель является обратимым элементом кольца. Матрица A называется *обратимой*, если существует матрица B такая, что $AB = BA = I$.

Определение 38. Обозначать долю невырожденных матриц среди всех матриц из $K_f^{n\times n}$ через $\varrho(K_f, n)$.

Определение 39. Обозначим множество собственных делителей многочлена $f(x) \in \mathbb{F}_2[x]$ через $\eta(f(x))$. Множество неприводимых собственных делителей обозначим через $\overline{\eta}(f(x))$.

Определение 40. *Порядком* числа $g \in \mathbb{Z}$ по модулю $d \in \mathbb{N}$ такому, что $\mathrm{НОД}(g, d) = 1$, называется минимальное $k > 0$ такое, что $g^k = 1 \pmod d$. Будем обозначать его $\mathrm{ord}_d(g)$.

2.2. О связях матриц многочленов, квазициклических матриц и матриц весов

Представим в этом разделе некоторые свойства определителей квазициклических матриц, матриц многочленов и матриц весов, а также взаимосвязи между ними.

Утверждение 23. *Любой циркулянт $A \in \mathbb{F}_2^{r\times r}$ четного веса вырожден.*

Доказательство. Для доказательства достаточно сложить все строки матрицы A. Поскольку A — циркулянт, то в каждом столбце одинаковое число единиц. Более того, количество единиц в каждом столбце четно, поэтому сумма всех строк равна нулевому вектору. Полученное равенство $[1,\ldots,1]A = 0$ доказывает вырожденность матрицы A. □

Теорема 7. *Квазициклическая матрица Q вырождена тогда и только тогда, когда вырождена соответствующая ей матрица $M(Q)$.*

Доказательство. Достаточность. Пусть матрица $M = M(Q)$ вырождена. Тогда существует ненулевой вектор $y \in K^n_{x^r-1}$ такой, что $My = 0$. Представим вектор y в квазициклическом виде, заменив каждый многочлен на соответствующую ему циклическую подматрицу. Очевидно, любой столбец $y' \in \mathbb{F}_2^{nr}$ полученной матрицы является ненулевым решением уравнения $Qy' = 0$, что означает вырожденность матрицы Q.

Необходимость. Если матрица Q вырождена, то существует такой вектор $y' = [y'_1,\ldots,y'_n]^\top, y'_i \in \mathbb{F}_2^r$, что

$$Qy' = 0. \tag{2.1}$$

Выполнение условия (2.1) означает, что

$$Q_{i,1}y'_1 + \ldots + Q_{i,n}y'_n = 0,$$

где Q_{ij} — блок матрицы Q. Сформируем из каждого столбца y'_i циркулянт $Y'_i \in \mathbb{F}_2^{r\times r}$, приписав справа $(r-1)$ столбец, каждый из которых равен предыдущему,

циклически сдвинутому вниз на 1. Полученную в результате матрицу назовем матрицей Y'. Заметим теперь, что циклический сдвиг столбца из $\mathbb{F}_2^r$ на один элемент вниз задается матрицей перестановки $P \in \mathbb{F}_2^{r\times r}$:

$$P = \begin{pmatrix} 0 & 1 \\ I_{r-1} & 0 \end{pmatrix}.$$

Отсюда следует, что t-ый столбец матрицы Y' есть $[P^t y'_1, \ldots, P^t y'_n]^\top$. Поскольку P — циркулянт, а умножение циркулянтов коммутативно (это следует, например, из упомянутого изоморфизма кольца циркулянтов факторкольцу K_{x^r-1}), то для t-ого столбца можно записать

$$Q_{i,1}P^t y'_1 + \ldots + Q_{1,n}P^t y'_n = P^t(Q_{i,1}y'_1 + \ldots + Q_{i,n}y'_n) = P^t \cdot 0 = 0,$$

что означает, что столбец $y \in K^n_{x^r-1}$, соответствующий матрице Y', является ненулевым решением уравнения $My = 0$, что доказывает вырожденность матрицы $M = M(Q)$. □

Из Теоремы 7 следует, что для исследования невырожденности квазициклической матрицы Q достаточно исследовать невырожденность матрицы $M(Q)$.

Покажем далее, что при умножении и сложении циклических многочленов четности их весов умножаются и складываются соответственно.

Утверждение 24. *Пусть $f(x)$ и $g(x)$ — многочлены из K_{x^r-1}. Тогда*

$$\begin{aligned} \mathrm{wt}_2\big(f(x)+g(x)\big) &= \mathrm{wt}_2\big(f(x)\big) + \mathrm{wt}_2\big(g(x)\big), \\ \mathrm{wt}_2\big(f(x)g(x)\big) &= \mathrm{wt}_2\big(f(x)\big)\mathrm{wt}_2\big(g(x)\big). \end{aligned} \tag{2.2}$$

Доказательство. Часть утверждения про сумму $f(x)+g(x)$ верна в силу того, что равенство (2.2) эквивалентно равенству

$$(f_1+\ldots+f_r+g_1+\ldots+g_r) \bmod 2 = ((f_1+\ldots+f_r) \bmod 2)+((g_1+\ldots+g_r) \bmod 2).$$

Докажем часть про произведение $f(x)g(x)$. Коэффициент при x^i равен

$$\sum_{j=1}^{r} f_j \cdot g_{1+(i-j) \bmod r}.$$

Поэтому

$$\mathrm{wt}_2\big(f(x)g(x)\big) = \sum_{i=1}^{r}\sum_{j=1}^{r} f_j \cdot g_{1+(i-j) \bmod r} = \sum_{j=1}^{r} f_j \sum_{i=1}^{r} g_{1+(i-j) \bmod r}.$$

Заметим, что при фиксированном j индекс при g (то есть $1 + (i - j) \bmod r$) во внутренней сумме пробегает все числа от 1 до r ровно по одному разу. Отсюда

$$\mathrm{wt}_2\big(f(x)g(x)\big) = \sum_{j=1}^{r} f_j \sum_{i=1}^{r} g_i = \mathrm{wt}_2\big(f(x)\big)\mathrm{wt}_2\big(g(x)\big).$$

□

Теорема 8. *Четность веса определителя матрицы M равна определителю матрицы* $\mathrm{wt}_2(M)$: $\mathrm{wt}_2(\det M) = \det(\mathrm{wt}_2(M))$.

Доказательство. По определению определитель матрицы M может быть вычислен по формуле

$$\det M = \sum_{\alpha_1,\alpha_2,\ldots,\alpha_n} (-1)^{N(\alpha_1,\alpha_2,\ldots,\alpha_n)} \cdot m_{1\alpha_1} m_{2\alpha_2} \ldots m_{n\alpha_n},$$

где суммирование проводится по всем перестановкам $\alpha_1, \alpha_2, \ldots, \alpha_n$ чисел из множества $\{1, 2, \ldots, n\}$, а $N(\alpha_1, \alpha_2, \ldots, \alpha_n)$ обозначает число инверсий в перестановке $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Отсюда и по Утверждению 24

$$\begin{aligned}\mathrm{wt}_2\big(\det M\big) &= \sum_{\alpha_1,\alpha_2,\ldots,\alpha_n} \mathrm{wt}_2\big(m_{1\alpha_1}\big)\mathrm{wt}_2\big(m_{2\alpha_2}\big)\ldots\mathrm{wt}_2\big(m_{n\alpha_n}\big) = \\ &= \sum_{\alpha_1,\alpha_2,\ldots,\alpha_n} (-1)^{N(\alpha_1,\alpha_2,\ldots,\alpha_n)} \cdot w_{1\alpha_1} w_{2\alpha_2} \ldots w_{n\alpha_n} = \det(\mathrm{wt}_2(M)),\end{aligned}$$

где w_{ij} — элементы матрицы W и сложение и умножение производятся в поле $\mathbb{F}_2$. □

Следствие 6. *Для того, чтобы была вырождена матрица Q, необходимо, чтобы была вырождена матрица* $\mathrm{wt}_2(M(Q))$.

Доказательство. Справедливость утверждения следует непосредственно из Теорем 7 и 8. □

2.3. Оценка доли обратимых матриц

В этом разделе мы оценим величину $\varrho(K_f, n)$ для различных многочленов $f(x) \in \mathbb{F}_2[x]$.

Утверждение 25. *Для произвольного конечного коммутативного кольца K с единицей и матрицы $A \in K^{n\times n}$ следующие утверждения эквивалентны:*

1. *матрица A обратима,*
2. *матрица A невырождена,*
3. *столбцы матрицы A линейно независимы.*

Доказательство. Докажем сначала, что условия (1) и (2) эквивалентны. Действительно, т.к. определитель произведения матриц равен произведению определителей, то для обратимой матрицы A получаем

$$1 = \det(I) = \det(AA^{-1}) = \det A \det(A^{-1}),$$

значит, определитель является обратимым элементом K, т.е. матрица A невырождена. Напротив, если A невырождена, то обратной к ней является матрица

$$A^{-1} = (\det A)^{-1}\mathrm{adj}(A),$$

где $\mathrm{adj}(A)$ — присоединенная матрица.

Далее обоснуем эквивалентность условий (3) и (1), то есть покажем, что линейная независимость столбцов матрицы эквивалентна ее обратимости. Если A обратима, то из равенства $Ax = 0$ следует $x = 0$, поэтому не существует ненулевой линейной комбинации столбцов, равной нулю. Обратно, рассмотрим матрицу A, чьи столбцы $a_1, \ldots, a_n$ образуют линейно независимую систему. Линейная оболочка $\mathrm{Im}(A)$ ее столбцов содержит ровно $|K|^n$ векторов, т.к. для каждого набора коэффициентов $\alpha_1, \ldots, \alpha_n \in K$ получается уникальный столбец $v = \alpha_1 a_1 + \cdots + \alpha_n a_n$ (в силу линейной независимости разложение столбца

v по столбцам матрицы A единственно). Значит, $\mathrm{Im}(A) = K^n$, то есть система $Ax = v$ разрешима для любой правой части $v \in K^n$, в том числе для v, равных столбцам единичной матрицы. Поэтому матрица A обратима. □

В связи с доказанным утверждением далее термины «невырождена» и «обратима» будут использованы как синонимы.

Лемма 2. *Для заданного набора линейно независимых векторов $u_1, \ldots, u_k \in K_f^n$, $0 \leqslant k \leqslant n-1$, число векторов $v \in K_f^n$ таких, что система $\{u_1, \ldots, u_k, v\}$ линейно зависима, не превосходит*

$$\sum_{\alpha \in \overline{\eta}(f)} 2^{k \deg f} 2^{(n-k) \deg \alpha}.$$

Доказательство. Для начала рассмотрим случай $k > 0$. Необходимо оценить сверху количество векторов $v \in K_f^n$ таких, что существует набор одновременно не равных нулю коэффициентов $\alpha_1, \ldots, \alpha_k, \alpha \in K_f$ и

$$\alpha_1 u_1 + \ldots + \alpha_k u_k = \alpha v. \tag{2.3}$$

Введем множество V_α такое, что

$$V_\alpha = \{v : \alpha v \in \mathrm{span}(u_1, \ldots, u_k)\},\ \alpha \in K_f.$$

Заметим, что для любого обратимого $\beta \in K$ выполнено $V_\alpha = V_{\alpha\beta}$. Поэтому множество всех различных значений α разбивается на классы эквивалентности отношения эквивалентности $\alpha' \sim \alpha'' \Leftrightarrow$ (существует обратимый $\beta : \alpha' = \beta\alpha''$). Заметим, что все представители одного класса эквивалентности имеют одинаковый НОД с многочленом $f(x)$. Этот НОД является собственным делителем $f(x)$. Поэтому

$$\bigcup_{\alpha \in K_f} V_\alpha = \bigcup_{\alpha \in \eta(f)} V_\alpha.$$

Более того, пусть некоторый многочлен $\alpha' \in K_f$ делится на $\alpha'' \in K_f$, тогда из того, что $\alpha'' v \in \mathrm{span}(u_1, \ldots, u_k)$ следует, что $\alpha' v \in \mathrm{span}(u_1, \ldots, u_k)$. Отсюда

$V_{\alpha''} \subset V_{\alpha'}$, поэтому

$$\bigcup_{\alpha \in K_f} V_\alpha = \bigcup_{\substack{\alpha \text{ — максмальный} \\ \text{собственный} \\ \text{делитель } f}} V_\alpha = \sum_{\alpha \in \overline{\eta}(f)} V_{f/\alpha}.$$

Последнее равенство следует из того, что неприводимые делители $f(x)$ взаимно однозначно соответствуют его максимальным собственным делителям, то есть тем, что не делят ни один другой собственный делитель. Можно записать соответствующее неравенство на размеры множеств:

$$\left| \bigcup_{\alpha \in K_f} V_\alpha \right| \leqslant \sum_{\alpha \in \overline{\eta}(f)} \left| V_{f/\alpha} \right|.$$

Осталось оценить величину $|V_\alpha|$ для некоторого $\alpha \in \overline{\eta}(F)$. Домножим обе части равенства (2.3) на $\theta = f/\alpha$ и получим

$$\theta\alpha_1 u_1 + \ldots + \theta\alpha_k u_k = 0.$$

Поскольку вектора $u_1, \ldots, u_k$ линейно независимы, то из равенства $\alpha_i\theta = 0$ в факторкольце кольца K_f следует равенство $\alpha_i(x)\theta(x) = f(x)\gamma(x)$ в кольце многочленов для некоторого $\gamma(x) \in \mathbb{F}_2[x]$. Таким образом, $\alpha_i(x)$ делится на $\alpha(x)$ для любого i, и уравнение (2.3) можно переписать как

$$\frac{\alpha_1}{\alpha} u_1 + \ldots + \frac{\alpha_k}{\alpha} u_k = v \pmod{f/\alpha}.$$

Существует $\left|K_{f/\alpha}\right|^k$ линейных комбинаций векторов $u_1, \ldots, u_k$ с коэффициентами из $K_{f/\alpha}$. Каждая из них отвечает $(2^{\deg\alpha})^n$ векторам v из K_f^n. Поэтому

$$\begin{aligned} |V_\alpha| &\leqslant \left|K_{f/\alpha}\right|^k (2^{\deg\alpha})^n = 2^{k\deg(f/\alpha)} 2^{n\deg\alpha} = \\ &= 2^{k\deg f - k\deg\alpha} 2^{n\deg\alpha} = 2^{k\deg f} 2^{(n-k)\deg\alpha}. \end{aligned}$$

Отсюда получаем

$$\left| \bigcup_{\alpha \in K_f} V_\alpha \right| \leqslant \sum_{\alpha \in \overline{\eta}(f)} 2^{k\deg f} 2^{(n-k)(\deg f - \deg\alpha)}.$$

Для случая $k = 0$ рассуждение остается корректным. Стоит лишь заметить, что, вопреки интуиции, выработанной при работе с линейными пространствами над полями, ненулевой вектор v может образовывать линейно зависимую систему. □

Теорема 9. *Доля $\varrho(K_f, n)$ невырожденных матриц $A \in K_f^{n\times n}$ удовлетворяет неравенству*

$$\varrho(K_f, n) \geqslant \prod_{k=0}^{n-1} \left(1 - 2^{(k-n)\deg f} \sum_{\alpha\in\overline{\eta}(f)} 2^{(n-k)(\deg f - \deg\alpha)}\right). \tag{2.4}$$

Доказательство. Вычислим количество невырожденных матриц с элементами из кольца K_f. Будем строить такую матрицу итеративно, на каждом шаге добавляя по столбцу, линейно не зависящему от предыдущих, и посчитаем, сколькими способами можно это сделать. Для $0 \leqslant k < n$ количество векторов, линейно не зависящих от предыдущих, можно найти по Лемме 2. Общее количество векторов $x \in K_f^n$ есть $2^{n\deg f}$, поэтому общее количество невырожденных матриц можно оценить снизу как

$$\prod_{k=0}^{n-1} \left(2^{n\deg f} - 2^{k\deg f} \sum_{\alpha\in\overline{\eta}(f)} 2^{(n-k)(\deg f - \deg\alpha)}\right).$$

Так как общее число матриц из $K_f^{n\times n}$ есть $2^{n^2\deg f}$, получаем неравенство (2.4). □

Следствие 7. *Доля $\varrho(K_f, n)$ невырожденных матриц $A \in K_f^{n\times n}$ удовлетворяет неравенству*

$$\varrho(K_f, n) > e^{-2}\left(1 - \sum_{\alpha\in\overline{\eta}(f)} 2^{-\deg\alpha}\right).$$

Доказательство. Для краткости будем обозначать через r степень многочлена $f(x)$. Оценим величину из Теоремы 9. Поскольку $\overline{\eta}(f)$ состоит только из

неприводимых многочленов, можем записать

$$\sum_{\alpha\in\overline{\eta}(f)} 2^{(n-k)(r-\deg\alpha)} \leqslant 2^{r(n-k)} \sum_{\alpha-\text{неприв.}} 2^{-(n-k)\deg\alpha} = \\ = 2^{r(n-k)} \left(\sum_{d=1}^{\infty} 2^{-(n-k)d}\,\psi(d) \right) = \\ = 2^{r(n-k)} \left(2^{-(n-k)} + \sum_{d=2}^{\infty} 2^{-(n-k)d}\psi(d) \right), \tag{2.5}$$

где $\psi(d)$ обозначает количество неприводимых многочленов степени d.

В работе [79] в Лемме 1 было показано, что $\psi(d) \leqslant \frac{2^d-2}{d}$. Поэтому мы можем оценить сверху сумму в выражении (2.5) следующим образом

$$\sum_{d=2}^{\infty} 2^{-(n-k)d}\frac{2^d}{d} \leqslant \frac{1}{2}\sum_{d=2}^{\infty} 2^{-(n-k-1)d} \leqslant \frac{1}{2}\cdot 2^{-(n-k-1)\cdot 2}\sum_{d=0}^{\infty} 2^{-(n-k-1)d}. \tag{2.6}$$

Для $0 \leqslant k \leqslant n-2$ число $2^{-(n-k-1)}$ не превосходит $1/2$, поэтому и сумма геометрической прогрессии в правой части (2.6) не превосходит 2. Отсюда и из того, что $2^{-2(n-k-1)} \leqslant 2^{-(n-k)}$ для $0 \leqslant k \leqslant n-2$, получаем, что

$$\sum_{\alpha\in\overline{\eta}(f)} 2^{(n-k)(r-\deg\alpha)} \leqslant 2^{r(n-k)}(2^{-(n-k)} + 2^{-2(n-k-1)}) \leqslant 2^{(r-1)(n-k)+1}.$$

Оценим сразу часть произведения (2.4), отвечающую $0 \leqslant k \leqslant n-2$:

$$\prod_{k=0}^{n-2} \left(1 - 2^{r(k-n)} \sum_{\alpha\in\overline{\eta}(f)} 2^{(n-k)(r-\deg\alpha)} \right) \geqslant \prod_{k=0}^{n-2} \left(1 - 2^{k+1-n}\right).$$

Для оценки произведения оценим сначала логарифм одного сомножителя. Отметим тривиально проверяемое неравенство: для $0 < x < 1$

$$\ln(1-x) > -\frac{x}{1-x}.$$

Поэтому

$$\ln(1-2^{k+1-n}) > -\frac{2^{k+1-n}}{1-2^{k+1-n}} \geqslant -\frac{2^{k+1-n}}{1-2^{-1}} = -2^{k+2-n}.$$

Теперь уже тривиально оценивается сумма логарифмов:

$$\sum_{k=0}^{n-2} \ln\left(1 - 2^{1+k-n}\right) > -\sum_{k=0}^{n-2} 2^{k+2-n} > -2,$$

что доказывает неравенство

$$\prod_{k=0}^{n-2} \left(1 - 2^{k+1-n}\right) > e^{-2}.$$

Учитывая сомножитель для $k = n-1$, окончательно получаем:

$$\varrho(K_f, n) > e^{-2} \left(1 - 2^{-r} \sum_{\alpha \in \overline{\eta}(f)} 2^{r - \deg \alpha}\right) = e^{-2} \left(1 - \sum_{\alpha \in \overline{\eta}(f)} 2^{-\deg \alpha}\right).$$

□

Следствие 8. *Для любых натуральных r и n верно неравенство*

$$\varrho(K_{x^r-1}, n) > e^{-2} \left(1 - \sum_{\substack{d \mid r \\ d - \text{нечетное}}} 2^{-\mathrm{ord}_d(2)} \frac{\varphi(d)}{\mathrm{ord}_d(2)}\right),$$

где $\varphi(d)$ — количество взаимно простых с d чисел от 1 до $d-1$ (функция Эйлера).

Доказательство. Уточним оценку из Следствия 7 для многочлена $f(x) = x^r - 1$. Для этого необходимо найти $\overline{\eta}(f)$. Пусть $r = 2^k r'$, где r' — нечетное. Тогда в силу того, что поле $\mathbb{F}_2$ имеет характеристику 2, получаем

$$x^r - 1 = (x^{r'} - 1)^{2^k},$$

а поэтому $\overline{\eta}(x^r - 1) = \overline{\eta}(x^{r'} - 1)$. В связи с этим далее будем считать, что r нечетно.

Для нечетного r разложение $x^r - 1 \in \mathbb{F}_2[x]$ на неприводимые множители выглядит следующим образом (см. [80, Теорема 2.47(ii)]):

$$x^r - 1 = \prod_{d \mid r} \prod_{i=1}^{\varphi(d)/\mathrm{ord}_d(2)} P_{d,i}(x),$$

где $P_{d,i}(x)$ — некоторый неприводимый многочлен степени $\mathrm{ord}_d(2)$. Отсюда получаем, наконец, что

$$\sum_{\alpha\in\overline{\eta}(f)} 2^{-\deg\alpha} = \sum_{d|r} \sum_{i=1}^{\varphi(d)/\mathrm{ord}_d(2)} 2^{-\mathrm{ord}_d(2)} = \sum_{d|r} 2^{-\mathrm{ord}_d(2)} \cdot \frac{\varphi(d)}{\mathrm{ord}_d(2)}. \tag{2.7}$$

□

Теорема 10. *Для любого простого r и натурального n верно неравенство*

$$\varrho(K_{x^r-1}, n) > \frac{1}{4e^2}.$$

Доказательство. Обозначим величину из (2.7) для данного r через $\xi(r)$. Очевидно, что для всех натуральных d выполнено

$$\mathrm{ord}_d(2) \geqslant \lceil \log_2(d) \rceil,$$

где $\lceil x \rceil$ есть минимальное целое число, большее или равное x. Из этого вытекает следующая цепочка неравенств для $r > 1$:

$$\xi(r) = 2^{-1} + 2^{-\mathrm{ord}_r(2)} \cdot \frac{r-1}{\mathrm{ord}_r(2)} \leqslant 2^{-1} + (r-1)\frac{2^{-\log_2(r)}}{\log_2(r)} =$$
$$= 2^{-1} + \frac{r-1}{r} \cdot \frac{1}{\log_2(r)} < 2^{-1} + \frac{1}{\log_2(r)}.$$

Очевидно, что для $r \geqslant 16$ выполнено $\xi(r) \leqslant 3/4$. Случаи простых r от 2 до 16 рассмотрены в Таблице 2.1. Далее, очевидно, что $\xi(1) = 1/2$. Более того, $\xi(2)$

f	3	5	7	11	13
$\xi(f)$	$\frac{3}{4}$	$\frac{9}{16}$	$\frac{3}{4}$	$\frac{513}{1024}$	$\frac{2049}{4096}$

Таблица 2.1

также равно $1/2$. Это следует из того факта, что единственным неприводимым делителем многочлена $x^2 - 1$ является многочлен $x - 1$ степени 1.

В результате можно утверждать, что для любого простого r верно неравенство

$$\xi(r) \leqslant \frac{3}{4}.$$

Наконец, можно записать:

$$\varrho(K_{x^r-1}, n) > \frac{1-\xi(r)}{e^2} \geqslant \frac{1}{4e^2}.$$

□

2.4. Приведение матрицы к треугольной форме

Рассмотрим алгоритм приведения матрицы над кольцом K_f к треугольной форме с помощью преобразований строк. Данный алгоритм на самом деле применим к более широкому классу колец: достаточно, чтобы в кольце работал алгоритм Евклида. Отметим, что классический алгоритм гауссова исключения для матриц над полем в данном случае неприменим. Дело в том, что для выполнения гауссова исключения требуется найти в столбце обратимый элемент, что может быть невозможно, даже если матрица обратима. Рассмотрим, к примеру, матрицу

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \in \mathbb{Z}_6^{2\times 2}.$$

Ее определитель равен $-5 = 1 \pmod 6$, то есть матрица является невырожденной. Также непосредственной проверкой можно убедиться, что $A^{-1} = A$. При этом все элементы матрицы A не являются обратимыми элементами кольца $\mathbb{Z}_6$, то есть классический алгоритм гауссова исключения не будет работать для этой матрицы.

Предлагаемый алгоритм основан на преобразовании строк, напоминающем вращение Гивенса (см. [81]), которое применяется, в частности, для вычисления QR-разложения матриц. Предлагаемое преобразование заключается в умножении матрицы A слева на матрицу R, совпадающую с единичной за исключением подматрицы размера 2×2 на пересечении строк и столбцов с заданными номерами i_1 и i_2, где $i_1 < i_2$. Указанную подматрицу обозначим через $\widehat{R}$. Она выбирается таким образом, чтобы после применения преобразования обратился в ноль элемент в позиции (i_2, i_1). Покажем, что этого всегда можно добиться.

Обозначим $u_1 := a_{i_1,i_1}$, $u_2 := a_{i_2,i_1}$. Применим алгоритм Евклида для вычисления НОД(u_1, u_2), получим следующую последовательность равенств:

$$\begin{aligned} u_1 &= u_2 q_1 + u_3, \\ u_2 &= u_3 q_2 + u_4, \\ &\dots \\ u_s &= u_{s+1} q_s + u_{s+2}, \\ u_{s+1} &= \text{ НОД}(u_1, u_2), \\ u_{s+2} &= 0. \end{aligned} \tag{2.8}$$

Помимо этого, каждый из элементов u_k может быть записан как линейная комбинация u_1 и u_2: $u_k = \alpha_k u_1 + \beta_k u_2$. Именно, по индукции тривиально получается

$$\begin{aligned} u_1 &= 1 \cdot u_1 + 0 \cdot u_2, \\ u_2 &= 0 \cdot u_1 + 1 \cdot u_2, \\ u_3 &= u_1 - u_2 q_1 = 1 \cdot u_1 + (-q_1) u_2, \\ &\dots \\ u_k &= u_{k-2} - u_{k-1} q_{k-2} = \\ &= (\alpha_{k-2} - \alpha_{k-1} q_{k-2}) u_1 + (\beta_{k-2} - \beta_{k-1} q_{k-2}) u_2. \end{aligned}$$

Для коэффициентов α_k и β_k получаем, таким образом:

$$\begin{aligned} &\alpha_1 = 1, \ \beta_1 = 0, \\ &\alpha_2 = 0, \ \beta_2 = 1, \\ &\alpha_k = \alpha_{k-2} - \alpha_{k-1} q_{k-2}, \text{ если } k \geqslant 2, \\ &\beta_k = \beta_{k-2} - \beta_{k-1} q_{k-2}, \text{ если } k \geqslant 2. \end{aligned} \tag{2.9}$$

Алгоритм, который помимо НОД(u_1, u_2) вычисляет еще и коэффициенты α_k и β_k, называют расширенным алгоритмом Евклида.

В качестве $\widehat{R}$ возьмем

$$\widehat{R} := \begin{pmatrix} \alpha_s & \beta_s \\ \alpha_{s+1} & \beta_{s+1} \end{pmatrix}.$$

Для элементов a'_{i_1,i_1} и a'_{i_2,i_1} матрицы $A' = RA$ из (2.8) получаем равенство:

$$\begin{pmatrix} a'_{i_1,i_1} \\ a'_{i_2,i_1} \end{pmatrix} = \begin{pmatrix} \alpha_s & \beta_s \\ \alpha_{s+1} & \beta_{s+1} \end{pmatrix} \cdot \begin{pmatrix} a_{i_1,i_1} \\ a_{i_2,i_1} \end{pmatrix} = \begin{pmatrix} \text{НОД}(a_{i_1,i_1}, a_{i_2,i_1}) \\ 0 \end{pmatrix}. \tag{2.10}$$

Мы хотим показать, что матрица R обратима. Для этого обозначим для всех $k = 2, \ldots, s+1$

$$\widehat{R}_k := \begin{pmatrix} \alpha_{k-1} & \beta_{k-1} \\ \alpha_k & \beta_k \end{pmatrix}$$

и докажем следующее.

Лемма 3. *Для всех* $k = 2, \ldots, s+1$ *выполнено равенство* $\det \widehat{R}_k = 1$.

Доказательство. При $k = 2$ искомый определитель имеет вид

$$\det \widehat{R}_2 = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Далее, для всех $k > 2$ можно записать, воспользовавшись (2.9),

$$\det \widehat{R}_k = \det \begin{pmatrix} \alpha_{k-1} & \beta_{k-1} \\ \alpha_{k-2} - \alpha_{k-1} q_{k-2} & \beta_{k-2} - \beta_{k-1} q_{k-2} \end{pmatrix}.$$

Прибавим ко второй строке первую, домноженную на q_{k-2} (отчего определитель не поменяется). Тогда

$$\det \widehat{R}_k = \det \begin{pmatrix} \alpha_{k-1} & \beta_{k-1} \\ \alpha_{k-2} & \beta_{k-2} \end{pmatrix} = -\det A_{k-1},$$

и по индукции получаем утверждение леммы. Так как рассматривается кольцо многочленов над полем $\mathbb{F}_2$ характеристики 2, то $-1 = 1$ и $\det \widehat{R}_k = 1$. □

Теперь можно сформулировать алгоритм приведения квадратной матрицы над K_f к верхнетреугольному виду (Алгоритм 2, аналогичный алгоритму из замечания в начале Главы 3 работы [77]).

Алгоритм 2 Приведение матрицы $A \in K_f^{n\times n}$ к верхнетреугольному виду

Вход: Матрица $A \in K_f^{n\times n}$ со строками $a_1^\top, \ldots, a_n^\top$

цикл $j = 1, \ldots, n$ **выполнять**

  цикл $i = n-1, \ldots, j$ **выполнять**

    Шаг 1. Применить расширенный алгоритм Евклида для вычисления НОД$(a_{i,j}, a_{i+1,j})$ и найти числа $\alpha_s, \beta_s, \alpha_{s+1}, \beta_{s+1}$;

    Шаг 2. $a'_i := \alpha_s a_i + \beta_s a_{i+1}$;

    Шаг 3. $a'_{i+1} := \alpha_{s+1} a_i + \beta_{s+1} a_{i+1}$;

    Шаг 4. $a_i, a_{i+1} := a'_i, a'_{i+1}$;

  конец

конец

Теорема 11. *В результате работы Алгоритма 2, примененного к матрице $A \in K_f^{n\times n}$ получается верхнетреугольная матрица $A' = RA$, где $\det R = 1$. Алгоритм 2 имеет сложность $O(n^3)$ умножений и сложений элементов кольца K_f, а также $O(n^2)$ применений расширенного алгоритма Евклида в этом кольце.*

Доказательство. Из (2.10) следует, что после выполнения Шага 4 для данных i и j элемент в позиции $(i+1, j)$ занулится. Более того, элемент в этой позиции будет оставаться нулевым до конца работы алгоритма, потому что при всех последующих преобразованиях строк он будет заменяться на линейную комбинацию нулевых элементов. Отсюда получаем, что после выполнения алгоритма матрица действительно будет иметь верхнетреугольный вид. Выполнение Шага 4 эквивалентно умножению текущей матрицы слева на матрицу $R^{(\ell)}$, отличающуюся от единичной подматрицей $\widehat{R}^{(\ell)}$, которая находится на пересечении строк и столбцов с номерами i и $i+1$. Разложение определителя $\det R^{(\ell)}$ по строкам с номерами i и $i+1$ дает равенство $\det R^{(\ell)} = \det \widehat{R}^{(\ell)}$, а по Лемме 3 получаем, что $\det R^{(\ell)} = 1$.

После завершения работы алгоритма получается матрица $R^{(N)} \dots R^{(1)} A$, где N — общее количество внутренних итераций цикла. Введение обозначения $R = R^{(N)} \dots R^{(1)}$ дает первую часть утверждения теоремы.

Шаги 1–4, очевидно, суммарно выполняются $(n-1) + (n-2) + \dots + 1 = n(n-1)/2$ раз. На Шагах 2–3 выполняются умножения вектора из K_f^n на число и сложения векторов, что требует $O(n)$ сложений и умножений элементов кольца K_f. Суммарно получаем $O(n^3)$ сложений и умножений, а также $O(n^2)$ выполнений расширенного алгоритма Евклида при $n \to \infty$. □

2.5. Построение случайной обратимой матрицы

Алгоритмы построения случайной обратимой матрицы в этом разделе опираются на алгоритм приведения матрицы к треугольной форме (Алгоритм 2).

За основу анализа возьмем модель Random Access Machine [82, стр. 5–11] с модификацией, позволяющей моделировать генерацию случайных битов. В этом случае по аналогии со входной лентой машина имеет еще одну односторонне бесконечную ленту, в ячейках которой записаны биты. Считывание очередного бита с этой ленты производится с помощью инструкции «RAND x», аналогичной инструкции «READ x». Состояние выходной ленты после останова машины, а также сам факт останова теперь зависят от входа и случайной ленты. Распределение заполнений случайной ленты выберем исходя из бернуллиевского процесса (бесконечной последовательности бросков честной монеты). Тогда для фиксированного входа можно ставить вопросы: «Чему равна вероятность останова?» или «Каково математическое ожидание времени работы?»

Алгоритм 3 Построение случайной обратимой матрицы $A \in K_f^{n\times n}$

Вход: Кольцо K_f, параметр n

Выход: Обратимая матрица $A \in K_f^{n\times n}$

Шаг 1. Построить случайную матрицу $A \in K_f^{n\times n}$, выбрав каждый элемент равномерно и независимо из K_f;

Шаг 2. Вычислить верхнетреугольную форму T матрицы A;

Шаг 3. Вычислить $d := \prod_{i=1}^{n} t_{ii}$;

если *элемент d необратим* **тогда**

  Вернуться на Шаг 1;

иначе

  вернуть A;

конец

Теорема 12. *Пусть $f(x)$ — многочлен степени $r \geqslant 1$. Тогда Алгоритм 3, примененный к кольцу K_f, корректен (то есть возвращает обратимую матрицу) и завершается с вероятностью 1, причем каждую обратимую матрицу он возвращает с одинаковой вероятностью. В среднем (по внутреннему источнику случайности) он требует генерации $n^2 r[\varrho(K_f, n)]^{-1}$ случайных бит и выполнения $O\left(n^3 r^2 [\varrho(K_f, n)]^{-1}\right)$ битовых операций.*

Доказательство. Покажем вначале, что алгоритм завершается на очередной итерации тогда и только тогда, когда построенная матрица A является обратимой. Действительно, из Теоремы 11 следует, что $\det T = \det A$. С другой стороны, определитель треугольной матрицы T равен произведению диагональных элементов, т.е. d. Поэтому $\det A$ обратим тогда и только тогда, когда обратим элемент d.

Вероятность того, что случайно выбранная матрица окажется невырожденной, равна $\varrho(K_f, n)$. Это число в рассматриваемом случае кольца с единицей заведомо положительно для любого натурального n, т.к. единичная матрица

является невырожденной. Фиксируем произвольную невырожденную матрицу $B \in K_f^{n\times n}$ и вычислим вероятность $\Pr(\mathsf{returned} = B)$ того, что алгоритм вернул матрицу B. В силу независимости выбора матрицы A на каждой итерации алгоритма можно утверждать, что вероятность $\Pr(\mathsf{returned} = B \wedge \mathsf{steps} = k)$ события, что алгоритм завершится в точности после k шагов и вернет матрицу B, есть

$$\Pr(\mathsf{returned} = B \wedge \mathsf{steps} = k) = (1 - \varrho(K_f, n))^{k-1}|K_f|^{-n^2}. \tag{2.11}$$

Тогда для вероятности $\Pr(\mathsf{returned} = B)$ можно записать

$$\begin{aligned}\Pr(\mathsf{returned} = B) &= \sum_{k=1}^{\infty}(1 - \varrho(K_f, n))^{k-1}|K_f|^{-n^2} = \\ &= \frac{1}{1 - (1 - \varrho(K_f, n))}|K_f|^{-n^2} = \frac{1}{\varrho(K_f, n)|K_f|^{n^2}}.\end{aligned}$$

Поэтому вероятность получить каждую невырожденную матрицу на выходе алгоритма одинакова.

Вероятность того, что алгоритм завершится за конечное число шагов, есть

$$\sum_{B \text{ обратима}} \Pr(\mathsf{returned} = B) = \frac{1}{\varrho(K_f, n)|K_f|^{n^2}}\varrho(K_f, n)|K_f|^{n^2} = 1,$$

ведь количество обратимых матриц есть в точности $\varrho(K_f, n)|K_f|^{n^2}$.

Перейдем к оценке ожидаемой сложности. Если алгоритм завершится в точности после k шагов, то его сложность составит kn^2 генераций случайного элемента, $O\left(kn^3\right)$ сложений и умножений и $O\left(kn^2\right)$ применений расширенного алгоритма Евклида при $k \to \infty, n \to \infty$. Поэтому достаточно оценить математическое ожидание количества шагов k. Так как из (2.11) следует, что

$$\Pr(\mathsf{steps} = k) = (1 - \varrho(K_f, n))^{k-1}\varrho(K_f, n),$$

то по известной формуле для математического ожидания геометрического распределения получаем

$$\mathbb{E}k = \sum_{k'=1}^{\infty} k' \Pr(\mathsf{steps} = k') = \frac{1}{\varrho(K_f, n)}.$$

Сложность вычисления суммы двух элементов кольца K_f есть, очевидно, $O(r)$, а сложность вычисления произведения есть $O(r^2)$ при $r \to \infty$. Также можно показать, что сложность расширенного алгоритма Евклида есть $O(r^2)$. Именно, рассмотрим k-й шаг алгоритма (2.8). На нем выполняется деление с остатком многочлена u_k на u_{k+1}. При применении стандартного метода деления «в столбик» для этого требуется $O(\deg u_k - \deg u_{k+1})$ шагов, сложность каждого из которых есть $O(\deg u_{k+1})$ битовых операций. Оценив последнюю величину сверху как $O(r)$, получим в итоге, что весь алгоритм Евклида требует

$$O\big(r(\deg u_1 - \deg u_2) + r(\deg u_2 - \deg u_3) + \ldots + r(\deg u_s - \deg u_{s+1})\big) \quad (2.12)$$

битовых операций. Эта сумма после перегруппировки слагаемых дает $O(r(\deg u_1 - \deg u_{s+1})) = O(r^2)$.

При выполнении расширенного алгоритма Евклида, однако, на каждом шаге вычисляются многочлены α_k и β_k. Покажем, что суммарная сложность вычисления всех этих многочленов есть также $O(r^2)$. Действительно, из (2.9) следует, что сложность вычисления α_k есть

$$O(\deg \alpha_{k-1} \deg q_{k-2}) = O(r \deg q_{k-2}).$$

Из (2.8) же следует, что $\deg q_k = \deg u_k - \deg u_{k+1}$. Вместе это позволяет получить оценку сложности вычисления всех многочленов α_k, аналогичную (2.12). Для многочленов β_k рассуждения аналогичны. □

Мы видим, что основную сложность в Алгоритме 3 составляет Шаг 2, то есть приведение матрицы к треугольной форме. Оказывается, в случае матриц над кольцом K_{x^r-1} есть возможность уменьшить требуемое число таких приведений. Для этого в Алгоритме 4 предварительно строится и проверяется невырожденность матрицы четности весов $\mathrm{wt}_2(A) \in \mathbb{F}_2^{n \times n}$.

Теорема 13. *Алгоритм 4 корректен и завершается с вероятностью 1, причем каждую обратимую матрицу он возвращает с одинаковой вероятностью.*

Алгоритм 4 Построение случайной обратимой матрицы $A \in K_{x^r-1}^{n\times n}$

Вход: Натуральные числа n и r

Выход: Обратимая матрица $A \in K_{x^r-1}^{n\times n}$

Шаг 1. Построить случайную матрицу $W \in \mathbb{F}_2^{n\times n}$;

Шаг 2. Проверить вырожденность матрицы W;

если *матрица W вырождена* **тогда**
  вернуться на Шаг 1

конец

Шаг 3. Построить матрицу $A \in K_{x^r-1}^{n\times n}$ так, что элемент a_{ij} выбирается независимо и равновероятно среди всех многочленов веса w_{ij};

Шаг 4. Вычислить верхнетреугольную форму T матрицы A;

Шаг 5. Вычислить $d := \prod_{i=1}^{n} t_{ii}$;

если *элемент d необратим* **тогда**
  Вернуться на Шаг 1;

иначе
  вернуть A;

конец

В среднем (по внутреннему источнику случайности) он требует выработки

$$\frac{n^2 + n^2 r\varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}$$

случайных бит и выполнения

$$O\left(n^3 r^2 \frac{\varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}\right)$$

битовых операций.

Доказательство. Корректность алгоритма при условии завершения следует из Теоремы 12. Для доказательства завершимости с вероятностью 1 воспользуемся теорией цепей Маркова. Именно, представим работу алгоритма в виде блуждания по цепи Маркова, изображенной на Рис. 2.1.

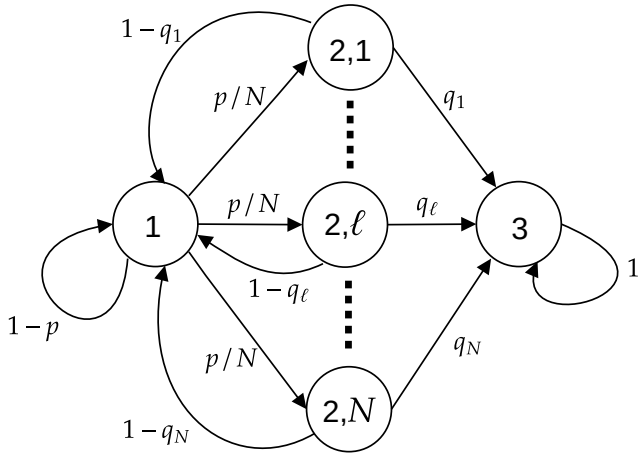


Рис. 2.1. Цепь Маркова, моделирующая возможные исполнения Алгоритма 4 (вертикальные многоточия обозначают остальные состояния $(2, \ell')$, $\ell' \notin \{1, \ell, N\}$)

Состояния условно соответствуют шагам алгоритма. Начальное состояние 1 соответствует первым двум шагам, то есть построению и проверке вырожденности матрицы W. Для каждой невырожденной матрицы $W_\ell \in \mathbb{F}_2^{n\times n}$ есть отдельное состояние $(2,1), \ldots, (2,N)$, которое соответствует Шагам $3-5$. Здесь через N обозначено общее количество невырожденных матриц $W \in \mathbb{F}_2^{n\times n}$. Наконец, состояние 3 соответствует завершению алгоритма, то есть нахождению невырожденной матрицы A.

Переходы из состояния 1 в состояния $(2,i)$ соответствуют невырожденным матрицам W_ℓ и имеют, очевидно, одинаковые вероятности $\varrho(\mathbb{F}_2, n)/N$, а переход $1 \to 1$ имеет вероятность $1 - \varrho(\mathbb{F}_2, n)$. На рисунке через p обозначена величина $\varrho(\mathbb{F}_2, n)$, этим же обозначением для краткости мы будем пользоваться дальше.

Вероятность перехода $(2,\ell) \to 3$ обозначена через q_ℓ. Соответственно, вероятность возврата в состояние 1 есть $1 - q_\ell$. Рассмотрим матрицы $M \in K_{x^r-1}^{n\times n}$ такие, что $\mathrm{wt}_2(M) = W_\ell$. Обозначим через $\varphi_{\text{обр}}(W_\ell)$ число обратимых, а через $\varphi(W_\ell)$ — общее число матриц такого вида. Несложно видеть, что

$$q_\ell = \frac{\varphi_{\text{обр}}(W_\ell)}{\varphi(W_\ell)}.$$

Также очевидно, что $\varphi(W_\ell) = 2^{n^2(r-1)}$. Состояние 3 является поглощающим (absorbing), то есть переход из него возможен только в него же (этот переход не

соответствует шагам работы алгоритма и нужен лишь для того, чтобы построенная модель действительно являлась цепью Маркова). Ясно, что построенная цепь Маркова корректно моделирует работу Алгоритма 4.

Получим некоторые соотношения для q_ℓ. Например, можно вычислить

$$\sum_{\ell=1}^{N} q_\ell = \frac{1}{2^{n^2(r-1)}} \sum_{\ell=1}^{N} \varphi_{\text{обр}}(W_\ell).$$

Из Теоремы 8 следует, что для любой обратимой матрицы M обратима также матрица $\mathrm{wt}_2(M)$, то есть $\sum_{\ell=1}^{N} \varphi_{\text{обр}}(W_\ell)$ дает общее число обратимых матриц M. Таким образом приходим к равенству

$$\sum_{\ell=1}^{N} q_\ell = \frac{\varrho(K_{x^r-1}, n) 2^{n^2 r}}{2^{n^2(r-1)}} = \varrho(K_{x^r-1}, n) \cdot 2^{n^2}$$

или, иначе,

$$\sum_{\ell=1}^{N} q_\ell = \frac{N}{p} \varrho(K_{x^r-1}, n). \tag{2.13}$$

Так как все $q_\ell > 0$ (в силу того, что как минимум матрица $W_\ell \in K_{x^r-1}^{n\times n}$ является невырожденной), то из каждого состояния существует путь с ненулевой вероятностью до состояния 3. Поэтому, согласно определению из [83], построенная цепь Маркова является поглощающей (absorbing). Значит, по [83, Теорема 11.3] вероятность оказаться в поглощающем состоянии равна 1, что доказывает завершимость Алгоритма 4 с вероятностью 1.

Теперь посчитаем ожидаемое количество прохождений через состояния 1 и $(2, \ell)$ в рассматриваемой цепи. Для этого построим матрицу переходов цепи, причем запишем ее сразу в каноническом виде [83, Раздел 11.2]:

$$T = \begin{array}{c} \\ 1 \\ (2,1) \\ \\ (2,N) \\ 3 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & (2,1) & & (2,N) & 3 \end{array} \\ \begin{pmatrix} 1-p & p/N & \dots & p/N & 0 \\ 1-q_1 & 0 & \dots & 0 & q_1 \\ \vdots & & \ddots & & \vdots \\ 1-q_N & 0 & \dots & 0 & q_N \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \end{array}$$

Соответственно, левый верхний блок размера $(N+1)\times(N+1)$ обозначим P. Воспользуемся Теоремой 11.4 из [83] для вычисления математического ожидания количества прохождений через каждое состояние. Указанная теорема утверждает, что матрица $I-P$ обратима, а ее элемент с индексами s, s' матрицы $(I-P)^{-1}$ есть математическое ожидание количества прохождений состояния s' среди всех путей, начинающихся в состоянии s. Нас интересуют лишь пути, начинающиеся в состоянии 1, а значит, достаточно вычислить только первую строку матрицы $(I-P)^{-1}$. Тривиально проверяется, что ею является строка

$$\left(\frac{N}{p\sum_{\ell=1}^{N} q_\ell}, \frac{1}{\sum_{\ell=1}^{N} q_\ell}, \ldots, \frac{1}{\sum_{\ell=1}^{N} q_\ell}\right). \tag{2.14}$$

Учитывая равенство (2.13), получаем, что математическое ожидание числа выполнений Шагов 1 и 2 алгоритма есть $[\varrho(K_{x^r-1}, n)]^{-1}$, а числа выполнений Шагов 3–5 есть $[\varrho(K_{x^r-1}, n)]^{-1}p$.

Таким образом, ожидаемое количество случайных бит, выработанных на Шагах 1 и 3, есть

$$\frac{n^2}{\varrho(K_{x^r-1}, n)} \text{ и } \frac{n^2 r\varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}$$

соответственно, а ожидаемая сложность Шагов 2 и 4 есть

$$O\left(n^3\frac{1}{\varrho(K_{x^r-1}, n)}\right) \text{ и } O\left(n^3 r^2\frac{\varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}\right)$$

битовых операций соответственно при $n\to\infty$.

Вычислим теперь вероятность того, что алгоритм вернет конкретную невырожденную матрицу $B\in K_{x^r-1}^{n\times n}$. Рассмотрим все пути из состояния 1 в состояние 3, для которых возвращается матрица B. Предпоследнее состояние на каждом таком пути есть $(2,\ell)$, где $W_\ell = \mathrm{wt}_2(B)$, а переход в состояние 3 по матрице B происходит с вероятностью

$$\left(\frac{|K_{x^r-1}|}{2}\right)^{-n^2}.$$

Для вычисления искомой вероятности применим формулу полной вероятности, разбив множество всех путей из 1 в 3 на непересекающиеся (возможно,

пустые) подмножества π_k, $k \geqslant 2$, где в π_k содержатся все пути длины k. Получим:

$$\Pr(\mathsf{returned} = B) = \sum_{k=2}^{\infty} \Pr(\text{перейти из 1 в } (2, \ell) \text{ за } k-1 \text{ шаг}) \left(\frac{|K_{x^r-1}|}{2} \right)^{-n^2},$$

где $\mathsf{returned}$ — матрица, которую вернул алгоритм. Очевидно, что первый сомножитель в каждом слагаемом есть соответствующий элемент матрицы P^{k-1}. Так как $P + P^2 + \ldots = (I - P)^{-1} - I$, то из (2.14) получаем:

$$\Pr(\mathsf{returned} = B) = \left(\frac{1}{\sum_{\ell=1}^{N} q_\ell} - 1 \right) \left(\frac{|K_{x^r-1}|}{2} \right)^{-n^2},$$

то есть не зависит от B. □

2.6. Выводы ко второй главе

В настоящей главе исследовалась возможность построения электронной подписи CFS на основе квазициклических кодов в случае, когда ключевая пара генерируется по алгоритму, предложенному в схеме LEDAcrypt, который требует построение невырожденной квазициклической матрицы.

В диссертации эта задача сведена к задаче построения невырожденной матрицы над факторкольцом кольца многочленов от одной переменной над полем из двух элементов. Описан алгоритм приведения такой матрицы к верхнетреугольному виду для последующей проверки невырожденности. Найдены нижние оценки доли невырожденных матриц среди всех матриц многочленов заданного размера. На основе этих результатов предложено и проанализировано два эффективных алгоритма построения случайной невырожденной квазициклической матрицы (в соответствии с равномерным распределением на множестве всех таких матриц). Первый из них также может использоваться в общем случае для построения невырожденной матрицы многочленов. Второй имеет бóльшую эффективность за счет того, что специализирован для квазициклических матриц. Его обоснование использует связь между невырожденностью

матрицы такого типа и матрицы четности весов, построенной для соответствующей матрицы многочленов.

Глава 3

Структура ключей электронной подписи CFS на основе конструкции Сидельникова

Схемы с открытым ключом, сформированным на основе конструкции Сидельникова, известны своей нестойкостью к структурным атакам. Так, например, в работе [44] описан алгоритм восстановления секретного ключа по открытому, построенному на основе кода Рида–Маллера. Схемы типа Сидельникова, использующие комбинацию кода Рида–Маллера и случайного линейного кода, были атакованы в работах [45] и [46]. Также известен анализ стойкости криптосистемы, построенной полностью на случайных кодах [69]. Обобщение результатов перечисленных исследований показало, что рассматриваемые схемы показывают нестойкость в одном и том же предположении о структуре кода, задаваемого открытым ключом.

В настоящей главе вводится понятие кодов с разложимым квадратом, что позволяет формализовать семейство кодов, подвергающих схему описанным ранее структурным атакам. Одной из ключевых задач работы является описание структуры пространства секретных ключей кодов, порождающих уязвимость к данным атакам. Другой задачей является описание кодов, не удовлетворяющих введенному определению. Этот вопрос особенно важен в свете результата работы [47], где показано, что с вероятностью близкой к 1 случайный линейный код обладает разложимым квадратом. Тогда поиск кодов, не обладающих этим свойством, является базой разработки стойких криптографических схем.

Основные результаты главы представлены в работе [66].

3.1. Дополнительные определения

Для проведения ряда доказательств в настоящей главе потребуется понятие укорочения кода.

Определение 41. Для произвольного вектора $c \in \mathbb{F}_{q^m}^n$ и ненулевого вектора $v \in \mathbb{F}_2^n \subseteq \mathbb{F}_{q^m}^n$ можно построить вектор $c(v) = (c_{i_1}, \ldots, c_{i_s})$, где $1 \leqslant i_1 < \ldots < i_s \leqslant n$ — индексы всех ненулевых элементов вектора v. Тогда *укорочением* кода $\mathcal{C}$ называется код, задаваемый как $\mathcal{C}_v = \{c(v) \,|\, c \in \mathcal{C}\}$. Вектор v в этом случае называется *вектором инцидентности* укорочения $\mathcal{C}_v$.

Структура укорочения кода задает структуру полного кода. В частности, верно следующее утверждение.

Утверждение 26. *Пусть для некоторого линейного кода $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ и некоторого ненулевого вектора $b \in \mathbb{F}_2^n \subseteq \mathbb{F}_{q^m}^n$ верно вложение $\mathcal{C}_b \subseteq (\mathcal{C}_b)^\perp$. Тогда $b \in (\mathcal{C}^2)^\perp$.*

Доказательство. Так как $\mathcal{C}_b \subseteq (\mathcal{C}_b)^\perp$, то для любых $c' \in \mathcal{C}$ и $c'' \in \mathcal{C}$ верно, что $(c'(b), c''(b)) = 0$. Отсюда

$$0 = \sum_{j:\, b_j \neq 0} c'_j c''_j = \sum_{j=1}^{n} c'_j c''_j b_j = (c' \circ c'', b),$$

откуда сразу следует условие утверждения. □

3.2. Пространство ключей подписи CFS на основе конструкции Сидельникова на линейных кодах общего вида

Будем говорить, что схема подписи CFS обладает *эквивалентными* секретными ключами, если существует пара несовпадающих ключей (M'_1, M'_2, Γ') и (M''_1, M''_2, Γ''), которым соответствует один и тот же открытый ключ

$$(M'_1 R \,\|\, M'_2 R) \cdot \Gamma' = (M''_1 R \,\|\, M''_2 R) \cdot \Gamma''.$$

Таким образом, множество секретных ключей криптосистемы естественным образом разбивается на классы эквивалентности. Каждый класс может быть задан порождающей матрицей кода и одним своим представителем. Введем для него обозначение $[(M_1, M_2, \Gamma)]_R$.

Описание структуры классов эквивалентности в явном виде выглядит сложной задачей, однако оно может быть получено через эквивалентное представление. Для этого рассмотрим перестановочную матрицу Γ такую, что существуют невырожденные матрицы M_1', M_2', обладающие свойством:

$$(M_1 R \parallel M_2 R)\Gamma = M_1' R \parallel M_2' R.$$

Обозначим через $\mathcal{G}_R(M_1, M_2)$ множество всех таких матриц Γ.

Теорема 14. *Для произвольной матрицы R полного ранга существует взаимно однозначное соответствие между классом эквивалентности $[(M_1, M_2, \Gamma)]_R$ секретных ключей и множеством $\mathcal{G}_R(M_1, M_2)$.*

Доказательство. Введем отображение f, отображающее произвольный секретный ключ в некоторую подстановку:

$$f(M_1', M_2', \Gamma') = \Gamma\Gamma'^{-1}.$$

Тогда f — инъективно, так как если ключи (M_1', M_2', Γ'), (M_1'', M_2'', Γ'') эквивалентны и $f(M_1', M_2', \Gamma') = f(M_1'', M_2'', \Gamma'')$, то $\Gamma' = \Gamma''$, а, значит, из

$$(M_1' R \parallel M_2' R)\Gamma' = (M_1'' R \parallel M_2'' R)\Gamma''$$

следует, что $M_i' R = M_i'' R$. Откуда, учитывая линейную независимость строк порождающей матрицы, получаем $M_i' = M_i''$.

Покажем, что f — сюръективно. Выберем подстановку $\Gamma_g \in \mathcal{G}_R(M_1, M_2)$ и найдем такой секретный ключ (M_1', M_2', Γ'), что $f(M_1', M_2', \Gamma') = \Gamma_g$. По определению множества $\mathcal{G}_R(M_1, M_2)$ существуют невырожденные матрицы M_1', M_2' такие, что

$$(M_1 R \parallel M_2 R)\Gamma_g = (M_1' R \parallel M_2' R).$$

Следовательно,

$$(M_1R \,\|\, M_2R)\Gamma = (M_1'R \,\|\, M_2'R)\Gamma_g^{-1}\Gamma,$$

то есть $(M_1', M_2', \Gamma_g^{-1}\Gamma) \in [(M_1, M_2, \Gamma)]_R$. Наконец, $f(M_1', M_2', \Gamma_g^{-1}\Gamma) = \Gamma(\Gamma_g^{-1}\Gamma)^{-1} = \Gamma\Gamma^{-1}\Gamma_g = \Gamma_g$.

Итак, отображение f инъективно и сюръективно, а значит f — взаимно однозначное отображение класса эквивалентности с представителем (M_1, M_2, Γ) во множество $\mathcal{G}_R(M_1, M_2)$. □

Стоит отменить, что доказательство теоремы повторяет доказательство аналога для частного случая, в котором R — порождающая матрица кода Рида–Маллера (его можно найти в [70, Теорема 1]).

Следующие два утверждения являются непосредственными следствиями Теоремы 14.

Следствие 9. *Класс эквивалентности $[(M_1, M_2, \Gamma)]_R$ состоит из ключей вида $(M_1', M_2', \Gamma_g^{-1}\Gamma)$, где $\Gamma_g \in \mathcal{G}_R(M_1, M_2)$ и*

$$(M_1'R \,\|\, M_2'R) = (M_1R \,\|\, M_2R)\Gamma_g.$$

Следствие 10. *Справедлива формула для мощности класса эквивалентности*

$$\left|[(M_1, M_2, \Gamma)]_R\right| = |\mathcal{G}_R(M_1, M_2)|.$$

Утверждение 27. *Пусть R — порождающая матрица произвольного кода $\mathcal{C}$, все столбцы которой различны. Тогда для любой подстановки Γ выполнено*

$$\left|[(E, E, \Gamma)]_R\right| = 2^n|\mathrm{Aut}(\mathcal{C})|^2.$$

Доказательство. В силу Следствия 10 вместо мощности класса эквивалентности $[(E, E, \Gamma)]_R$ можем искать мощность множества $\mathcal{G}_R(E, E)$.

Определим структуру этого множества. Возьмем подстановку $\Gamma' \in \mathcal{G}_R(E, E)$. Тогда по определению $(R \,\|\, R)\Gamma' = M_1R \,\|\, M_2R$. Поскольку по условию в матрице R нет одинаковых столбцов, то и в матрице M_iR, $i \in \{1, 2\}$ все столбцы

также различны. Значит, существует подстановка $P \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})$ такая, что $(R \,\|\, R)\Gamma' = (R \,\|\, R)P$.

Обозначив $\Gamma'' = \Gamma' P^{-1}$, получаем, что $\Gamma' = \Gamma'' P$, причем для Γ'' выполнено соотношение $(R \,\|\, R)\Gamma'' = R \,\|\, R$. Таким образом установлено, что множество $\mathcal{G}_R(E, E)$ совпадает со множеством $\{\Gamma'' P \,|\, \Gamma'' = \Gamma' P^{-1}, P \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})\}$. То есть для нахождения мощности множества $\mathcal{G}_R(E, E)$ достаточно найти число таких подстановок.

Поскольку $|\mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})| = \big|\mathrm{Aut}(\mathcal{C})\big|^2$, то этому же числу равно количество различных подстановок P. Подстановка Γ'' переставляет одинаковые столбцы матрицы $R \,\|\, R$. Таким образом, число подстановок Γ'' равно 2^n. Следовательно, подстановок вида $\Gamma'' \cdot P$ есть в точности $2^n \big|\mathrm{Aut}(\mathcal{C}))\big|^2$. □

Теорема 15. *Справедлива оценка снизу на мощность Ψ множества открытых ключей схемы подписи CFS на основе конструкции Сидельникова:*

$$\frac{(2n)! h_k}{2^n |\mathrm{Aut}(\mathcal{C})|} \leqslant \Psi,$$

где $\mathcal{C}$ — произвольный код с порождающей матрицей R, все столбцы которой различны, а h_k — число невырожденных $(k \times k)$-матриц над полем $\mathbb{F}_{q^m}$.

Доказательство. Определим подмножество секретных ключей схемы подписи CFS: $\mathcal{H} = \{(MD_1, MD_2, \Gamma)\}$, где M — невырожденная $(k \times k)$-матрица над полем $\mathbb{F}_{q^m}$, матрицы D_i размера $k \times k$ задают автоморфизм $\mathcal{C}$, а $\Gamma \in S_{2n}$.

Покажем, что если ключ $(MD_1, MD_2, \Gamma) \in \mathcal{H}$, а ключи (MD_1, MD_2, Γ) и (M_1, M_2, Γ') эквивалентны, то $(M_1, M_2, \Gamma') \in \mathcal{H}$. Действительно, из эквивалентности ключей следует, что

$$(MD_1 R \,\|\, MD_2 R)\Gamma = (M_1 R \,\|\, M_2 R)\Gamma'.$$

Домножим равенство слева на невырожденную матрицу M^{-1} и получим

$$(D_1 R \,\|\, D_2 R)\Gamma = (M_1' R \,\|\, M_2' R)\Gamma',$$

где $M'_1 = M^{-1}M_1, M'_2 = M^{-1}M_2$. Теперь домножим его справа на перестановочную матрицу $(\Gamma')^{-1}$. Имеем

$$(D_1R \,\|\, D_2R)\Gamma'' = M'_1R \,\|\, M'_2R,$$

где $\Gamma'' = \Gamma(\Gamma')^{-1}$. В силу невырожденности матриц M'_1 и M'_2 аналогично доказательству Утверждения 27 можно показать существование такой подстановки $P \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})$, что $(D_1R \,\|\, D_2R)\Gamma' = (D_1R \,\|\, D_2R)P$. Тогда открытый ключ $(D_1R \,\|\, D_2R)\Gamma''$ представим в виде $D'_1R \,\|\, D'_2R$ для некоторых $D'_1 \in \mathrm{Aut}(C), D'_2 \in \mathrm{Aut}(C)$. Из полученного равенства матриц $D'_1R \,\|\, D'_2R = M'_1R \,\|\, M'_2R$ и того факта, что R имеет полный ранг, следуют равенства

$$\begin{cases} M'_1 = D'_1, \\ M'_2 = D'_2. \end{cases}$$

Поскольку $M_1 = MM'_1, M_2 = MM'_2$, то $(M_1, M_2, \Gamma') = (MD'_1, MD'_2, \Gamma')$, причем $D'_1 \in \mathrm{Aut}(C)$, $D'_2 \in \mathrm{Aut}(C)$. Следовательно, $(M_1, M_2, \Gamma') \in \mathcal{H}$.

Теперь заметим, что в силу Теоремы 14 множества $[(MD_1, MD_2, \Gamma)]_R$ и $\mathcal{G}_R(MD_1, MD_2)$ эквивалентны. По определению, множество $\mathcal{G}_R(MD_1, MD_2)$ состоит из таких подстановок Γ, что существуют невырожденные матрицы M_1, M_2, такие что

$$(MD_1R \,\|\, MD_2R)\Gamma = M_1R \,\|\, M_2R.$$

В результате домножения на невырожденную матрицу M^{-1} получаем

$$(D_1R \,\|\, D_2R)\Gamma = (M'_1R \,\|\, M'_2R),$$

где $M'_1 = M^{-1}M_1, M'_2 = M^{-1}M_2$. Представим подстановку Γ как произведение подстановок $\Gamma = \tilde{\Gamma}\tilde{\Gamma}^{-1}\Gamma$, где $\tilde{\Gamma}$ — подстановка, действующая таким образом, что $(M_1R \,\|\, M_2R)\tilde{\Gamma} = R \,\|\, R$. Таким образом мы перешли к рассмотрению подстановок Γ, для которых существуют невырожденные матрицы M'_1, M'_2 такие, что

$$(R \,\|\, R)\tilde{\Gamma}^{-1}\Gamma = M'_1R \,\|\, M'_2R,$$

то есть к рассмотрению множества $\mathcal{G}_R(E,E)$. То есть доказали равенство мощностей множеств $[(MD_1, MD_2, \Gamma)]_R$ и $\mathcal{G}_R(E,E)$. Отсюда следует, что число открытых ключей, порождаемых множеством секретных ключей, равно отношению числа секретных ключей к мощности множества $\mathcal{G}_R(E,E)$.

Найдем размер множества $\mathcal{H}$. Для этого рассмотрим множество матриц вида (M, D_1, D_2, Γ). Введем на этом множестве отношение эквивалентности следующим образом: два элемента (M, D_1, D_2, Γ) и $(M', D_1', D_2', \Gamma')$ эквивалентны, если им соответствует один и тот же элемент множества $\mathcal{H}$, то есть

$$(MD_1, MD_2, \Gamma) = (M'D_1', M'D_2', \Gamma').$$

Заметим, что если в таком классе эквивалентности лежала четверка (M, D_1, D_2, Γ), то будет лежать и четверка $(MA^{-1}, AD_1, AD_2, \Gamma)$, если $A \in \mathrm{Aut}(\mathcal{C})$.

Пусть тройки $(MD_1, MD_2, \Gamma) \in \mathcal{H}$ и $(M'D_1', M'D_2', \Gamma') \in \mathcal{H}$ эквивалентны. Запишем это условие как $(MD_1, MD_2, \Gamma) = (M'D_1', M'D_2', \Gamma')$ и будем искать решения системы:

$$\begin{cases} MD_1 = M'D_1', \\ MD_2 = M'D_2', \\ \Gamma = \Gamma'. \end{cases}$$

Тогда $M = M'D_1'D_1^{-1}, M = M'D_2'D_2^{-1}$. И из того, что $D_1 \in \mathrm{Aut}(\mathcal{C}), D_1' \in \mathrm{Aut}(\mathcal{C})$ следует, что $A = D_1'D_1^{-1} \in \mathrm{Aut}(\mathcal{C})$. Это дает возможность переписать систему в следующем виде:

$$\begin{cases} M = M'A, \\ D_1 = A^{-1}D_1', \\ D_2 = A^{-1}D_2', \\ \Gamma = \Gamma'. \end{cases}$$

Или, эквивалентно:

$$\begin{cases} M' = MA^{-1}, \\ D'_1 = AD_1, \\ D'_2 = AD_2, \\ \Gamma' = \Gamma. \end{cases}$$

То есть все элементы рассматриваемого класса эквивалентности имеют вид $(MA^{-1}, AD_1, AD_2, \Gamma)$, а его мощность равна $\mathrm{Aut}(\mathcal{C})$. Отсюда следует, что каждый ключ (MD_1, MD_2, Γ) будет встречаться во множестве $\mathcal{H}$ ровно $|\mathrm{Aut}(\mathcal{C})|$ раз.

Автоморфизм D_i можно выбрать $|\mathrm{Aut}(\mathcal{C})|$ способами, а подстановку Γ — $(2n)!$ способами. При этом, как было оказано выше, одинаковые ключи будут встречаться $|\mathrm{Aut}(\mathcal{C})|$ раз.

Число открытых ключей $\Psi_{\mathcal{H}}$, которое можно получить из множества $\mathcal{H}$, равно

$$\Psi_{\mathcal{H}} = \frac{|\mathcal{H}|}{|\mathcal{G}_R(E,E)|} = \frac{h_k|\mathrm{Aut}(\mathcal{C})|^2(2n)!}{|\mathcal{G}_R(E,E)||\mathrm{Aut}(\mathcal{C})|} = \frac{h_k|\mathrm{Aut}(\mathcal{C})|^2(2n)!}{2^n|\mathrm{Aut}(\mathcal{C})|^2|\mathrm{Aut}(\mathcal{C})|} = \frac{(2n)!h_k}{2^n|\mathrm{Aut}(\mathcal{C})|}.$$

Осталось вспомнить, что $\mathcal{H}$ — подмножество секретных ключей, поэтому число классов эквивалентности, а значит и число открытых ключей, будет не меньше, чем число классов в множестве $\mathcal{H}$, то есть

$$\frac{(2n)!h_k}{2^n|\mathrm{Aut}(\mathcal{C})|} \leqslant \Psi.$$

Это и требовалось доказать. □

Доказательство теоремы является обобщением результата для кодов Рида-Маллера (см. [84, Теорема 2]). Для его получения необходимо взять $u = 2$. При этом отсутствие одинаковых столбцов явно прописано в условии теоремы, а не следует из свойств кода.

Обозначим через $\mathcal{C}[M]$ линейный код с порождающей матрицей $R \parallel MR$, где R — порождающая матрица произвольного линейного кода $\mathcal{C}$ размера $k \times n$,

а M — невырожденная матрица размера $k \times k$. Несложно проверить, что

$$\mathcal{G}_R(M_1, M_2) = \mathcal{G}_R(I, M_1^{-1}M_2) = \mathcal{G}_R(I, M)$$

для $M = M_1^{-1}M_2$. Далее покажем, что структура множества $\mathcal{G}_R(I, M)$, а, значит, и множества $\mathcal{G}_R(M_1, M_2)$, зависит от вида кода $\mathcal{C}[M]$. Для этого нам понадобится следующее определение.

Определение 42. Код $\mathcal{C}[M]$ будем называть

1. *кодом с разложимым квадратом*, если $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$;
2. *кодом с неразложимым квадратом*, если $(\mathcal{C}[M])^2 \subsetneq \mathcal{C}^2 \times \mathcal{C}^2$.

Покажем, что для любого линейного кода $\mathcal{C}$ код $\mathcal{C}[M]$ обязан быть либо с разложимым квадратом, либо с неразложимым.

Теорема 16. $(\mathcal{C}[M])^2 \subseteq \mathcal{C}^2 \times \mathcal{C}^2$ *для всех невырожденных матриц* M.

Доказательство. Пусть строки матрицы M составляют вектора $\{m_i \,|\, 1 \leqslant i \leqslant k\}$, а строки матрицы R — вектора $\{r_i \,|\, 1 \leqslant i \leqslant k\}$. Тогда код $\mathcal{C}[M]$, заданный относительно матрицы M, представляет собой линейную оболочку векторов $(r_1 \,\|\, m_1R), \ldots, (r_k \,\|\, m_kR)$. При этом код $(\mathcal{C}[M])^2$ состоит из векторов

$$\left(\sum_{i=1}^{k} \alpha_i (r_i \,\|\, m_iR)\right) \circ \left(\sum_{j=1}^{k} \beta_j (r_j \,\|\, m_jR)\right) =$$
$$= \left(\sum_{i=1}^{k}\sum_{j=1}^{k} \alpha_i\beta_j (r_i \circ r_j) \,\Big\|\, \sum_{i=1}^{k}\sum_{j=1}^{k} \alpha_i\beta_j ((m_iR) \circ (m_jR))\right),$$

где α_i и β_j — элементы поля $\mathrm{GF}(q^m)$ для $1 \leqslant i, j \leqslant k$.

Докажем, что $u \in \mathcal{C}^2 \times \mathcal{C}^2$ в предположении, что $u \in (\mathcal{C}[M])^2$. Поскольку код $\mathcal{C}^2$ линейный, для этого достаточно показать, что $(r_i \circ r_j) \in \mathcal{C}^2$ и $((m_iR) \circ (m_jR)) \in \mathcal{C}^2$. Первое вложение следует из определения операции возведения в

квадрат Адамара, а второе можно представить как

$$(m_{i1}r_1 + \cdots + m_{ik}r_k) \circ (m_{j1}r_1 + \cdots + m_{jk}r_k) =$$
$$= \sum_{s,t=1}^{k} (m_{is}r_s \circ m_{jt}r_t) = \sum_{s,t=1}^{k} (m_{is} \cdot m_{jt})(r_s \circ r_t),$$

где последнее выражение есть линейная комбинация векторов $r_s \circ r_t$. Таким образом, снова пользуясь линейностью $\mathcal{C}^2$, можно утверждать, что оно также лежит в этом коде.

□

Далее будем изучать множество $\mathcal{G}_R(I, M)$ в случае, когда код $\mathcal{C}[M]$ имеет разложимый квадрат.

Утверждение 28. *Если* $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$, *то* $\mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.

Доказательство. Согласно определению, если $\Gamma \in \mathcal{G}_R(I, M)$, то $\mathcal{C}[M]\Gamma$ представляет собой линейную оболочку строк матрицы $M_1'R \parallel M_2'R$, где M_1', M_2' — невырожденные, то есть $\mathcal{C}[M]\Gamma \subseteq \mathcal{C} \times \mathcal{C}$. Возведение в квадрат обеих частей вложения позволяет утверждать также, что $(\mathcal{C}[M]\Gamma)^2 \subseteq (\mathcal{C} \times \mathcal{C})^2$.

Заметим, что операции возведения в квадрат и применения подстановки коммутируют. То есть, в частности, верно, что $(\mathcal{C}[M]\Gamma)^2 = (\mathcal{C}[M])^2\Gamma$. Кроме того,

$$(\mathcal{C} \times \mathcal{C})^2 = \left\{ (a \parallel b) \circ (c \parallel d) \;\middle|\; a, b, c, d \in \mathcal{C} \right\} =$$
$$= \left\{ (a \circ c \parallel b \circ d) \;\middle|\; a, b, c, d \in \mathcal{C} \right\} = \mathcal{C}^2 \times \mathcal{C}^2.$$

Отсюда, $(\mathcal{C}[M])^2\Gamma \subseteq \mathcal{C}^2 \times \mathcal{C}^2$.

Тогда из равенства $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$ следует вложение $(\mathcal{C}^2 \times \mathcal{C}^2)\Gamma \subseteq \mathcal{C}^2 \times \mathcal{C}^2$. Применение подстановки не меняет размерность кода. То есть, более того, имеет место равенство $(\mathcal{C}^2 \times \mathcal{C}^2)\Gamma = \mathcal{C}^2 \times \mathcal{C}^2$. Другими словами, $\Gamma \in \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.

□

Пусть Γ_b — подстановка, которая меняет местами левую и правую части матрицы по правилу $\Gamma_b(k) = ((k-1+n) \bmod 2n) + 1$ для $1 \leqslant k \leqslant 2n$. Определим тогда новое множество перестановок

$$\mathcal{A}(\mathcal{C}) = \bigcup_{\Gamma \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})} \{\Gamma, \Gamma\Gamma_b, \Gamma_b\Gamma\}.$$

Утверждение 29. $\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M)$.

Доказательство. Матрица, задающая подстановку $\Gamma \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})$, имеет вид

$$\Gamma = \left(\begin{array}{c|c} \Gamma_1 & 0 \\ \hline 0 & \Gamma_2 \end{array}\right).$$

Тогда $(R \parallel MR)\Gamma = (R\Gamma_1 \parallel MR\Gamma_2)$. Поскольку Γ_i является автоморфизмом, то $R\Gamma_i = A_i R$ для некоторых невырожденных матриц A_i, $i \in \{1, 2\}$. Отсюда $(R \parallel MR)\Gamma = (A_1 R \parallel MA_2 R)$ и, после введения обозначений $M_1' = A_1, M_2' = MA_2$, получаем $\Gamma \in \mathcal{G}_R(I, M)$.

Очевидно, что $\Gamma_b \in \mathcal{G}_R(I, M)$. Кроме того, если $\Gamma \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})$, то

$$(R \parallel MR)\Gamma\Gamma_b = (M_1 R \parallel M_2 R)\Gamma_b = (M_2 R \parallel M_1 R),$$

а также

$$(R \parallel MR)\Gamma_b\Gamma = (MR \parallel R)\Gamma = (A_1 MR \parallel A_2 R) = (M_1' R \parallel M_2' R),$$

то есть $\Gamma\Gamma_b \in \mathcal{G}_R(I, M)$ и $\Gamma_b\Gamma \in \mathcal{G}_R(I, M)$. □

3.3. Пространство ключей подписи CFS на основе конструкции Сидельникова на кодах, основанных на ОРС и имеющих разложимый квадрат

В этом разделе покажем, как результаты Раздела 3.2 могут быть улучшены для кодов Рида–Соломона. Будем считать здесь, что код $\mathsf{GRS}_k(\alpha, v)$ задан порождающей матрицей вида (2).

Утверждение 30. $\mathrm{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v)) = \mathcal{A}(\mathsf{GRS}_k(\alpha, v))$.

Доказательство. Покажем, что для любой подстановки $\Gamma' \in \mathrm{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$ верно, что $\Gamma' \in \mathcal{A}(\mathsf{GRS}_k(\alpha, v))$. Обозначим через G следующую порождающую матрицу кода $\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v)$:

$$G = \left(\begin{array}{c||c} R & 0 \\ \hline\hline 0 & R \end{array}\right).$$

Если Γ' не переставляет столбцы между половинами $(2k \times 2n)$-матрицы G (т.е. все столбцы остаются в своих половинах), то $\Gamma' \in \mathrm{Aut}(\mathsf{GRS}_k(\alpha, v)) \times \mathrm{Aut}(\mathsf{GRS}_k(\alpha, v))$ и $\Gamma' \in \mathcal{A}(\mathsf{GRS}_k(\alpha, v))$. Иначе, без ограничения общности, будем считать, что переставленные столбцы имеют номера

$$1, 2, \ldots, t \quad \text{и}$$

$$n+1, n+2, \ldots, n+t,\ 1 \leqslant t \leqslant n.$$

То есть:

$$\left(\begin{array}{c||c} R & 0 \\ \hline\hline 0 & R \end{array}\right) \Gamma' = \left(\begin{array}{c|c||c|c} 0 & R'_2 & R'_1 & 0 \\ \hline\hline R''_1 & 0 & 0 & R''_2 \end{array}\right),$$

где $R = (R'_1 \parallel R'_2) = (R''_1 \parallel R''_2)$, матрицы R'_1 и R''_1 имеют размеры $k \times (n-t)$, а матрицы R'_2, R''_2 — размеры $k \times t$.

Докажем от противного, что $t = n$. Пусть это не так, и $1 \leqslant t \leqslant n-1$. Тогда из условия $\Gamma' \in \mathrm{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$ следует, что любая линейная комбинация строк матрицы

$$G_1 = \left(\begin{array}{c|c} 0 & R'_2 \\ \hline R''_1 & 0 \end{array}\right)$$

принадлежит коду $\mathsf{GRS}_k(\alpha, v)$. Заметим, что первые $1 \leqslant \ell \leqslant k$ строк матрицы (2) образуют порождающую матрицу $[n, \ell]$-обобщенного кода Рида–Соломона. Соответственно, каждая квадратная подматрица матрицы (2), включающая

строки с номерами из множества $\{1, 2, \dots \ell\}$, где $1 \leqslant \ell \leqslant k$, невырождена. Отсюда следует, в частности, что матрицы R'_1, R'_2, R''_1 и R''_2 имеют полный ранг.

В силу того, что матрица G_1 имеет блочную структуру, выполнено

$$\operatorname{rank}(R'_2) + \operatorname{rank}(R''_1) = \min(k, n-t) + \min(k, t).$$

Если $1 \leqslant t \leqslant n-1$, то $\min(k, n-t) \geqslant 1$ и $\min(k, t) \geqslant 1$. Если при этом дополнительно $t < k$ и $n - t < k$, то

$$\operatorname{rank}(R'_2) + \operatorname{rank}(R''_1) = (n-t) + t = n > k.$$

Иначе $t \geqslant k$ или $n - t \geqslant k$, откуда $\min(k, n-t) + \min(k, t) > k$. То есть в любом случае $\dim(\mathsf{GRS}_k(\alpha, v)) > k$, что невозможно, ведь $\dim(\mathsf{GRS}_k(\alpha, v)) = k$. Полученное противоречие доказывает, что $t = n$. В этом случае $\Gamma' = \Gamma_b$ и $\Gamma' \in \mathcal{A}(\mathsf{GRS}_k(\alpha, v))$.

Вложение $\mathcal{A}(\mathsf{GRS}_k(\alpha, v)) \subseteq \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$ очевидно, поскольку $\Gamma_b \in \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$. Одновременно любая подстановка $\Gamma \in \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v)) \times \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v))$ также является подстановкой из $\operatorname{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$, не переставляющей столбцы между подматрицами. Следовательно, аналогичное верно и для их суперпозиций, т.е. $\Gamma\Gamma_b \in \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$ и $\Gamma_b\Gamma \in \operatorname{Aut}(\mathsf{GRS}_k(\alpha, v) \times \mathsf{GRS}_k(\alpha, v))$.

Это завершает доказательство. □

Теорема 17. *Если* $(\mathsf{GRS}_k(\alpha, v)[M])^2 = \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$, *то*

$$\mathcal{A}(\mathsf{GRS}_k(\alpha, v)) \subseteq \mathcal{G}_R(I, M) \subseteq \mathcal{A}(\mathsf{GRS}_{2k-1}(\alpha, v^2)).$$

Доказательство. Справедливость теоремы следует из Утверждений 28, 29 и 30, а также из свойств операции возведения в квадрат кода Рида-Соломона. □

3.4. Неразложимость квадратов кодов на основе ОРС

Для практических применений интерес представляют коды с неразложимым квадратом, поскольку для них множество $\mathcal{G}_R(I, M)$ имеет более сложную

структуру, что может затруднить построение атаки на всю схему. Далее мы приведем три класса матриц M, для которых код $\mathsf{GRS}_k(\alpha, v)[M]$ будет иметь неразложимый квадрат.

Итак, пусть i_1 и i_2 — пара натуральных чисел, таких, что $1 \leqslant i_1 < i_2 \leqslant k$. Пусть также $a, b \in \mathbb{F}_{q^m}^k$ и матрица

$$B = \begin{pmatrix} a_{i_1} & a_{i_2} \\ b_{i_1} & b_{i_2} \end{pmatrix}$$

невырождена. Определим на основе этих параметров $(k \times k)$-матрицу $T_{a,b}^{i_1,i_2}$ следующим образом:

$$T_{a,b}^{i_1,i_2} = \begin{array}{c} \\ \\ \\ i_1\to \\ \\ i_2\to \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ i_1\downarrow \\ \\ \\ i_2\downarrow \\ \\ \\ \end{array} \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \dots & \vdots \\ a_1 & a_2 & \dots & a_{i_1} & \dots & a_{i_2} & \dots & a_k \\ \vdots & \vdots & \dots & \vdots & \ddots & \vdots & \dots & \vdots \\ b_1 & b_2 & \dots & b_{i_1} & \dots & b_{i_2} & \dots & b_k \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix}.$$

Отметим, что невырожденность матрицы B гарантирует невырожденность матрицы $T_{a,b}^{i_1,i_2}$.

Частный случай, когда одна из строк, образованных наборами a и b, совпадает с соответствующей строкой единичной матрицы, будем обозначать через T_w^i, выделяя только нетривиальную строку.

Теорема 18. *Если* $\{i_1, i_2\} \cap \{1, k\} \neq \varnothing$, *то*

$$\left(\mathsf{GRS}_k(\alpha, v)\left[T_{a,b}^{i_1,i_2}\right]\right)^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2).$$

Доказательство. Обозначим строки порождающей матрицы кода Рида–Соломона R через r_i для $1 \leqslant i \leqslant k$. Тогда в порождающей матрице кода $\left(\mathsf{GRS}_k(\alpha, v)\left[T_{a,b}^{i_1,i_2}\right]\right)^2$ есть строки следующих типов:

1. $r_s \circ r_t \,\|\, r_s \circ r_t$, где $s, t \notin \{i_1, i_2\}$;
2. а. $r_{i_1} \circ r_s \,\|\, aR \circ r_s$,
   б. $r_{i_2} \circ r_s \,\|\, bR \circ r_s$,
   где $s \notin \{i_1, i_2\}$;
3. а. $r_{i_1} \circ r_{i_2} \,\|\, aR \circ bR$,
   б. $r_{i_1} \circ r_{i_1} \,\|\, aR \circ aR$,
   в. $r_{i_2} \circ r_{i_2} \,\|\, bR \circ bR$.

Строки первого типа суть конкатенации строк значений многочленов степени $\ell : 0 \leqslant \ell \leqslant 2k-2$, т.е. имеют вид $v^2 \circ x^\ell \,\|\, v^2 \circ x^\ell$. Отметим, что из-за дополнительного условия на номера i_1 и i_2 невозможно получить все x^ℓ в указанном диапазоне. Так, для $j \in \{1, 2\}$ при $i_j = 1$ не удастся получить многочлен первой степени, а при $i_j = k$ — многочлен степени $2k-2$. Тогда число различных строк такого типа можно оценить сверху числом $2k-2$.

Так как число номеров s таких, что $s \notin \{i_1, i_2\}$, равно $k-2$, то максимальное число линейно независимых строк второго типа равно $k-2$. Строк третьего типа три.

В итоге получаем

$$\dim\left(\left(\mathsf{GRS}_k(\alpha, v)\left[T_{a,b}^{i_1,i_2}\right]\right)^2\right) \leqslant (2k-2) + 2 \cdot (k-2) + 3 = 4k-3,$$

а искомое вложение следует из Теоремы 16 и равенства (4). □

Следствие 11. $\left(\mathsf{GRS}_k(\alpha, v)\left[T_w^i\right]\right)^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$.

Доказательство. Определим $e^{(s)} \in \mathbb{F}_2^n$ следующим образом: $e_j^{(s)} = 1 \Leftrightarrow j = s$. Тогда при $i \neq 1$ требуемое утверждение получается из Теоремы 18 при выборе

$i_1 = 1$, $i_2 = i$ и $a = e^{(1)}$, $b = w$. При $i = 1$ выберем $i_1 = i = 1$, $i_2 = 2$ и $a = w$, $b = e^{(2)}$. □

Утверждение 31. *Если* $k \leqslant \frac{n+1}{2}$, *то* $\dim((\mathsf{GRS}_k(\alpha, v)[M])^2) \geqslant 2k-1$ *для любой невырожденной матрицы* M.

Доказательство. Справедливость условия следует из того, что

$$\dim((\mathsf{GRS}_k(\alpha, v)[M])^2) \geqslant \dim((\mathsf{GRS}_k(\alpha, v))^2) = 2k - 1.$$

□

Обозначим через D диагональную матрицу с ненулевыми диагональными элементами d_i. Тогда следующее утверждение очевидно.

Утверждение 32. $\dim\big((\mathsf{GRS}_1(\alpha, v)[D])^2\big) = 1$.

Утверждение 33. $\dim((\mathsf{GRS}_2(\alpha, v)[D])^2) = 3, n \geqslant 4$.

Доказательство. Порождающая матрица кода $(\mathsf{GRS}_2(\alpha, v)[D])^2$ вложена в матрицу G вида

$$G = \left(\begin{array}{c|c} v^2 \circ x^0 & (v^2 \circ x^0)d_0d_0 \\ v^2 \circ x^1 & (v^2 \circ x^1)d_0d_1 \\ v^2 \circ x^1 & (v^2 \circ x^1)d_1d_0 \\ v^2 \circ x^2 & (v^2 \circ x^2)d_1d_1 \end{array}\right).$$

Первая, вторая и четвертая строки этой матрицы линейно независимы, поскольку содержат в левой половине порождающую матрицу кода $\mathsf{GRS}_3(\alpha, v)$. Таким образом, эти строки образуют порождающую матрицу кода $(\mathsf{GRS}_2(\alpha, v)[D])^2$ и его размерность равна 3.

□

Теорема 19. *Если* $3 < k \leqslant \frac{n+1}{2}$, *то* $2k - 1 \leqslant \dim((\mathsf{GRS}_k(\alpha, v)[D])^2) \leqslant 4k - 6$, *причем и верхняя, и нижняя оценки достижимы.*

Доказательство. Сначала покажем, что $2k-1 \leqslant \dim((\mathsf{GRS}_k(\alpha,v)[D])^2) \leqslant 4k-6$. Нижняя оценка верна в силу Утверждения 31.

Перейдем к верхней оценке. Порождающая матрица кода $(\mathsf{GRS}_k(\alpha,v)[D])^2$ является подматрицей матрицы G следующего вида:

$$G = \left(\begin{array}{c|c} v^2 \circ x^0 & (v^2 \circ x^0)d_0d_0 \\ v^2 \circ x^1 & (v^2 \circ x^1)d_0d_1 \\ v^2 \circ x^2 & (v^2 \circ x^2)d_0d_2 \\ v^2 \circ x^2 & (v^2 \circ x^2)d_1d_1 \\ \dots & \dots \\ v^2 \circ x^{2k-2} & (v^2 \circ x^{2k-2})d_{k-1}d_{k-1} \end{array}\right).$$

Матрица G может быть разбита на блоки по степеням x, стоящим в ее левой части. Элементарными преобразованиями строк каждый блок может быть приведен к виду

$$\left(\begin{array}{c|c} v^2 \circ x^p & (v^2 \circ x^p)d_{i_1}d_{j_1} \\ 0 & (v^2 \circ x^p)\left(d_{i_2}d_{j_2} - d_{i_1}d_{j_1}\right) \\ \dots & \dots \\ 0 & (v^2 \circ x^p)\left(d_{i_t}d_{j_t} - d_{i_1}d_{j_1}\right) \end{array}\right).$$

Для того, чтобы размерность кода достигала верхней границы кода, необходимо потребовать, чтобы ранг каждого блока был максимален. Заметим, что при $p \in \{0,1,2k-3,2k-2\}$ ранг блока не может отличаться от единицы, поскольку соответствующие многочлены могут быть получены единственным образом: $x^0 = x^0x^0$, $x^1 = x^0x^1$, $x^{2k-3} = x^{k-2}x^{k-1}$ и $x^{2k-2} = x^{k-1}x^{k-1}$. Отсюда $\operatorname{rank}(G) \leqslant 2\cdot(2k-1) - \left|\{0,1,2k-3,2k-2\}\right| = (4k-2)-4 = 4k-6$.

Перейдем к вопросам достижимости. Так нижняя оценка достигается, например, при $d_0 = d_1 = \ldots = d_{k-1}$.

Для доказательства достижимости верхней оценки отметим, что при выполнении следующего условия:

$$\forall p \in \{2,\ldots,2k-4\}\ \exists i',j',i'',j'' : i'+j' = i''+j'' = p,\ d_{i'}d_{j'} \neq d_{i''}d_{j''} \qquad (3.1)$$

	0	1	2	3	4	5	6	7	8	9	10
0			•	•							
1		•	•	•	•						
2			•	•	•	•					
3				•	•	•	•				
4					•	•	•	•			
5						•	•	•	•		
6							•	•	•	•	
7								•	•	•	•
8									•	•	•
9										•	
10											

Таблица 3.1 Точки стоят в пересечении i-ой строки и j-го столбца для пар (i, j), участвующих в неравенствах (для $k = 11$)

ранг блоков, заданных многочленами степеней отличных от $\{0, 1, 2k-3, 2k-2\}$, будет строго равен двум. Одним из вариантов достижения верхней границы является выполнения следующих условий (первое гарантирует выполнение условия (3.1) для всех четных значений p, а второе — для нечетных):

$$\begin{cases} d_i d_i \neq d_{i-1} d_{i+1} & \text{для } i = 1, \ldots, k-2; \\ d_i d_{i+1} \neq d_{i-1} d_{i+2} & \text{для } i = 1, \ldots, k-3. \end{cases}$$

Для наглядности отметим в Таблице 3.1 элементы с индексами (i, j), которые участвуют в рассматриваемых неравенствах. Такой набор индексов выбран не случайно. Дело в том, что здесь для каждого $p = 2, \ldots, 2k-4$ на диагонали $\{(i, j) \mid i + j = p\}$ есть ровно две рассматриваемые пары, т.е. минимальное возможное количество.

Пусть g — порождающий элемент $\mathbb{F}_2(q^m)$. Тогда $d_i = g^{\gamma_i}$, и систему можно переписать как

$$\begin{cases} g^{2\gamma_i} \neq g^{\gamma_{i-1}+\gamma_{i+1}} & \text{для } i = 1, \ldots, k-2; \\ g^{\gamma_i+\gamma_{i+1}} \neq g^{\gamma_{i-1}+\gamma_{i+2}} & \text{для } i = 1, \ldots, k-3. \end{cases}$$

Откуда

$$\begin{cases} 2\gamma_i \neq \gamma_{i-1} + \gamma_{i+1} & \text{для } i = 1, \ldots, k-2; \\ \gamma_i + \gamma_{i+1} \neq \gamma_{i-1} + \gamma_{i+2} & \text{для } i = 1, \ldots, k-3. \end{cases}$$

Значения γ_i, удовлетворяющие условию (3.1), можно выбрать, например, в соответствии с Таблицами 3.2 и 3.3. Тогда $2k-5$ блоков будут иметь ранг 2, а

Таблица 3.2 Выбор значений γ_i в случае, когда k — нечетное

i	0	1	2	3	...	$k-3$	$k-2$	$k-1$
γ_i	0	$k-1$	1	$k-2$	...	$\frac{k-3}{2}$	$\frac{k+1}{2}$	$\frac{k-1}{2}$

Таблица 3.3 Выбор значений γ_i в случае, когда k — четное

i	0	1	2	3	...	$k-3$	$k-2$	$k-1$
γ_i	0	$k-1$	1	$k-2$	...	$\frac{k+2}{2}$	$\frac{k-2}{2}$	$\frac{k}{2}$

блоки, соответствующие $p \in \{0, 1, 2k-3, 2k-2\}$, будут иметь ранг 1.

Покажем, что из матрицы G можно выбрать $4k-6$ линейно независимых строк: первую строку из 4 блоков ранга 1 и первые две строки из $2k-5$ блоков ранга 2. Обозначим через χ_p и ψ_p соответственно коэффициенты $d_{i_1}d_{j_1}$ и $(d_{i_2}d_{j_2} - d_{i_1}d_{j_1})$ из p-ого блока, $2 \leqslant p \leqslant 2k-4$. Предположим противное: пусть существует некоторая нетривиальная линейная комбинация этих строк, равная нулю. То есть

$$a_{01}\big(v^2 \circ x^0 \parallel (v^2 \circ x^0)\chi_0\big) + a_{11}\big(v^2 \circ x^1 \parallel (v^2 \circ x^1)\chi_1\big) + a_{21}\big(v^2 \circ x^2 \parallel \big(v^2 \circ x^2)\chi_2\big) + \\ + a_{22}\big(0 \parallel (v^2 \circ x^2)\psi_2\big) + a_{31}\big(v^2 \circ x^3 \parallel (v^2 \circ x^3)\chi_3\big) + a_{32}\big(0 \parallel (v^2 \circ x^3)\psi_3\big) + \ldots = 0.$$

Отсюда, в частности, должно быть выполнено условие:

$$a_{01}(v^2 \circ x^0) + a_{11}(v^2 \circ x^1) + a_{21}(v^2 \circ x^2) + a_{31}(v^2 \circ x^3) + \ldots = 0. \tag{3.2}$$

Но эта сумма есть линейная комбинация строк порождающей матрицы обобщенного кода Рида–Соломона, которые линейно независимы по определению. Поэтому сумма (3.2) может быть равна нулю лишь при условии, что

$$a_{01} = a_{11} = a_{21} = a_{31} = \ldots = 0. \tag{3.3}$$

Также необходимо, чтобы было верно равенство

$$a_{01}(v^2 \circ x^0)\chi_0 + a_{11}(v^2 \circ x^1)\chi_1 + a_{21}(v^2 \circ x^2)\chi_2 + a_{22}(v^2 \circ x^2)\psi_2 + \\ + a_{31}(v^2 \circ x^3)\chi_3 + a_{32}(v^2 \circ x^3)\psi_3 + \ldots = 0.$$

Или, в силу условия (3.3), что

$$a_{22}(v^2 \circ x^2)\psi_2 + a_{32}(v^2 \circ x^3)\psi_3 + \ldots = 0.$$

Но поскольку значения d_i выбирались таким образом, чтобы ни одна из разностей ψ_p не обращалась в ноль, то $a_{22} = a_{32} = \ldots = 0$. Из последнего равенства следует, что только тривиальная линейная комбинация выбранных нами строк равна нулю.

□

Следствие 12. $(\mathsf{GRS}_k(\alpha, v)[D])^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$ *для* $k \leqslant \frac{n+1}{2}$.

Доказательство. Справедливость вложения непосредственно следует из Утверждений 32 и 33, Теорем 16 и 19, а также равенства (4). □

В заключение рассмотрим задание кода $\mathsf{GRS}_k(\alpha, v)$ систематической порождающей матрицей над $\mathbb{F}_{2^m}$, то есть матрицей вида:

$$R = \left(\, I_k \, \middle| \, \ldots\ldots \, \right),$$

где I_k — единичная матрица размера $k \times k$. Это возможно в силу невырожденности главной $(k \times k)$-подматрицы порождающей матрицы кода $\mathsf{GRS}_k(\alpha, v)$, что следует из того, что определитель такой матрицы отличается от определителя матрицы Вандермонда лишь умножением на ненулевой скаляр.

Напомним, что матрица A размера $\ell \times \ell$ называется *ортогональной*, если $AA^T = I_\ell$.

Теорема 20. *Для любой матрицы H' вида*

$$H' = \left(\begin{array}{c|c} \hat{H} & H_1 \\ \hline 0 & H_2 \end{array}\right),$$

где $\hat{H}$ — ортогональная подматрица, выполнено

$$(\mathsf{GRS}_k(\alpha, v)[H'])^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2).$$

Доказательство. Согласно Утверждениям 5 и 6 условие

$$\mathsf{GRS}_k^2(\alpha, v)[H'] \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$$

эквивалентно условию

$$(\mathsf{GRS}_k^2(\alpha, v)[H'])^\perp \supsetneq (\mathsf{GRS}_{2k-1}(\alpha, v^2))^\perp \times (\mathsf{GRS}_{2k-1}(\alpha, v^2))^\perp.$$

Согласно Утверждению 16 найдется вектор v' такой, что $(\mathsf{GRS}_{2k-1}(\alpha, v^2))^\perp = \mathsf{GRS}_{n-2k+1}(\alpha, v')$. Поэтому будем доказывать вложение

$$(\mathsf{GRS}_k^2(\alpha, v)[H'])^\perp \supsetneq \mathsf{GRS}_{n-2k+1}(\alpha, v') \times \mathsf{GRS}_{n-2k+1}(\alpha, v').$$

Заметим, что если матрица $\hat{H}$ имеет размер $\ell \times \ell$, то верно, что

$$(R \parallel H'R) = \left(\begin{array}{c|ccc||c|ccc} I_\ell & \dots & \dots & & \hat{H} & \dots & \dots & \\ \hline 0 & \dots & \dots & & 0 & \dots & \dots & \end{array}\right). \tag{3.4}$$

Рассмотрим вектор $u = (u_L \parallel u_R)$ вида

$$u = (\underbrace{111\ldots1}_{\ell}\underbrace{000\ldots0}_{n-\ell}\underbrace{111\ldots1}_{\ell}\underbrace{000\ldots0}_{n-\ell})^{\mathrm{T}}.$$

Покажем, что для укорочения $(\mathsf{GRS}_k^2(\alpha, v)[H'])_u$ выполнено условие Утверждения 26. Действительно, для его порождающей матрицы $\left(\begin{array}{c|c} I_\ell & \hat{H} \\ \hline 0 & 0 \end{array}\right)$ выполнено условие

$$\left(\begin{array}{c|c} I_\ell & \hat{H} \\ \hline 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c|c} I_\ell^T & 0 \\ \hline \hat{H}^T & 0 \end{array}\right) = \left(\begin{array}{c|c} I_\ell + \hat{H}\hat{H}^T & 0 \\ \hline 0 & 0 \end{array}\right) = 0.$$

Отсюда из Утверждения 26 получаем $u \in (\mathsf{GRS}_k^2(\alpha, v)[H'])^{\perp}$.

Предположим, что $u_L \in \mathsf{GRS}_{n-2k+1}(\alpha, v')$. Но, согласно соотношениям (3) и (5) $\mathsf{GRS}_{n-2k+1}(\alpha, v') \subseteq \mathsf{GRS}_{n-k}(\alpha, v') = \mathsf{GRS}_k^{\perp}(\alpha, v^2)$, где последнее равенство следует из Утверждения 16. Тогда можно заключить, что $u_L \in \mathsf{GRS}_k^{\perp}(\alpha, v^2)$. Однако в этом случае для порождающей матрицы $\tilde{R}$ вида (2) кода $\mathsf{GRS}_k(\alpha, v^2)$ должно быть выполнено равенство $\tilde{R}u_L^T = 0$, что невозможно в силу Утверждения 17. Полученное противоречие опровергает предположение о том, что $u_L \in \mathsf{GRS}_{n-2k+1}(\alpha, v')$. Аналогичное замечание для вектора u_R завершает доказательство. □

3.5. Выводы к третьей главе

Глава посвящена исследованию классов эквивалентности секретных ключей электронных подписей типа CFS, построенных на основе конструкции Сидельникова при использовании линейных кодов общего вида или обобщенных кодов Рида–Соломона. Предложен механизм исследования структуры множества секретных ключей в схемах такого вида путем перехода к исследованию множеств, однозначно соответствующих классам эквивалентности секретных ключей. Подход позволил получить нижнюю оценку мощности открытых ключей исследуемой схемы подписи. Описаны классы эквивалентности секретных

ключей электронной подписи CFS, построенной на конкатенации произвольных линейных кодов, при условии разложимости квадрата кода, задаваемого открытым ключом. Структура классов эквивалентности уточнена для частного случая, когда схема строится на обобщенных кодах Рида–Соломона. Наконец, приведены три частных случая кодов на основе обобщенных кодов Рида–Соломона, квадрат которых неразложимым.

Глава 4

Построение стойкой схемы подписи на основе кодов общего типа

Результаты первых глав диссертации показали, что схема электронной подписи CFS может быть подвергнута структурным атакам, которые возможны за счет факта использования кодов из фиксированного класса. Поэтому целью настоящей главы является построение новой схемы электронной подписи, стойкость которой не зависела бы от структуры используемого кода. При этом необходимо отказаться от конструкции CFS, которая в алгоритме генерации подписи явно использует алгоритм декодирования кода.

Одним из возможных подходов к решению поставленной задачи является применение преобразования А. Фиата и А. Шамира [56] к одной из известных схем идентификации. В качестве такой схемы можно выбрать, например, протокол Я. Штерна [57]. Это позволит отказаться от использования кодов с известной структурой, делающих подпись потенциально уязвимой к структурным атакам, а также свести стойкость схемы к стойкости задачи синдромного декодирования, которая является NP-трудной.

В настоящей главе приведем описание схемы подписи, полученной на основе протокола идентификации Штерна, и исследуем стойкость построенной конструкции. Эти исследования проводились автором в рамках процесса стандартизации постквантовых криптографических механизмов в России при Техническом комитете 26 по стандартизации [18].

Для вывода стойкости схемы подписи в настоящем разделе потребуется обращение к задаче, определенной для хэш-функций.

Задача $\mathsf{Coll}(h)$. **Поиск коллизии**

Дано: хэш-функция $h : \mathbb{F}_2^* \to \mathbb{F}_2^\ell$.

Найти: вектора $x', x'' \in \mathbb{F}_2^*, x' \neq x''$ такие, что $h(x') = h(x'')$.

Сложность этой задачи зависит от структуры функции h. В общем случае сложность решения такой задачи с использованием парадокса дней рождения можно оценить как $\mathcal{O}\left(2^{\frac{\ell}{2}}\right)$.

Глава содержит результаты статьи [67].

4.1. Синтез схемы подписи

Ниже приведем описание схемы электронной подписи, которая является результатом применения преобразования Фиата–Шамира [56] к схеме идентификации Штерна. Преобразование состоит в замене случайного значения b, сгенерированного проверяющим, на некоторую функцию f от сообщения и значений, полученных от доказывающего. Важно, чтобы f зависела сразу от всех этих значений.

Параметры подписи такие же, как и в исходном протоколе идентификации, описанном выше. Дополнительно схема использует хэш-функцию $f(\cdot) : \mathbb{F}_2^* \to \{0,1,2\}^\delta$. Длина подписи зависит от параметра δ, который определяется параметром безопасности λ.

Stern.KGen(1^λ)

$s \xleftarrow{\mathcal{U}} \{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = \omega\}$

$y \leftarrow Hs^T$

return (y, s)

Stern.SigGen(s, m)

foreach $0 \leqslant i < \delta$:

  $u_i \xleftarrow{\mathcal{U}} \mathbb{F}_2^n, \sigma_i \xleftarrow{\mathcal{U}} \mathcal{S}_n$

  $c_{i,0} \leftarrow h(\sigma_i \| Hu_i^T)$

  $c_{i,1} \leftarrow h(\sigma_i(u_i))$

  $c_{i,2} \leftarrow h(\sigma_i(u_i \oplus s))$

  $c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$

$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$

$b \leftarrow f(m \| c)$

foreach $0 \leqslant i < \delta$:

  if $b_i = 0 : r_i \leftarrow \sigma_i \| u_i$

  if $b_i = 1 : r_i \leftarrow \sigma_i \| (u_i \oplus s)$

  if $b_i = 2 : r_i \leftarrow \sigma_i(u_i) \| \sigma_i(s)$

$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$

return $c \| r$

Stern.SigVer$(y, m, (c \| r))$

$b \leftarrow f(m \| c)$

foreach $0 \leqslant i < \delta$:

  if $\big[b_i = 0\big] \wedge \Big[\big[c_{i,0} \neq h(r_{i,0} \| Hr_{i,1}^T)\big] \vee \big[c_{i,1} \neq h(r_{i,0}(r_{i,1}))\big]\Big]$:

    return 0

  if $\big[b_i = 1\big] \wedge \Big[\big[c_{i,0} \neq h(r_{i,0} \| (Hr_{i,1}^T \oplus y))\big] \vee \big[c_{i,2} \neq h(r_{i,0}(r_{i,1}))\big]\Big]$:

    return 0

  if $\big[b_i = 2\big] \wedge \Big[\big[c_{i,1} \neq h(r_{i,0})\big] \vee \big[c_{i,2} \neq h(r_{i,0} \oplus r_{i,1})\big] \vee \big[\mathrm{wt}(r_{i,1}) \neq \omega\big]\Big]$:

    return 0

return 1

Для оценки стойкости схемы подписи построим серию экспериментов, в которых нарушитель представлен вероятностной полиномиальной машиной Тьюринга. Выражение $\mathbf{Exp} \Rightarrow b$ следует трактовать как «значение b стало выходом

эксперимента **Exp**». После наступления события **abort** в псевдокоде оракула соответствующий эксперимент останавливается и возвращает 0. Для того, чтобы подчеркнуть, что значение x — результат вероятностного алгоритма A, будем писать $x \leftarrow\!\!\$\ A(\dots)$. Как и ранее запись $s \xleftarrow{\mathcal{U}} S$ означает, что s выбрано из множества S случайно равновероятно. А выражение $x \leftarrow v$ означает присваивание значения v переменной x.

Будем моделировать случайный оракул $\mathrm{F} : \mathbb{F}_2^* \to \{0,1,2\}^\delta$, используя технику «ленивое семплирование». Для этого введем множество Π^{F}, содержащее пары вида $(\alpha, \mathrm{F}(\alpha))$. Запись $(\alpha, \cdot) \in \Pi^{\mathrm{F}}$ для некоторого $\alpha \in \mathbb{F}_2^*$ означает существование такого $\beta \in \{0,1,2\}^\delta$, что $(\alpha, \beta) \in \Pi^{\mathrm{F}}$. Поскольку множество Π^{F} содержит не более одной пары (α, β) для каждого значения α, то $\Pi^{\mathrm{F}}(\alpha)$ представляет собой либо β, если $(\alpha, \beta) \in \Pi^{\mathrm{F}}$, либо специальное значение $\perp$, если такая пара отсутствует.

Определение 43. Для схемы подписи Stern.Σ *преимущество нарушителя* $\mathcal{A}$ *в модели* EUF-NMA *с доступом к случайному оракулу* обозначим через

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) \Rightarrow 1],$$

где эксперимент $\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A})$ определен следующим образом:

$\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A})$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow\!\!\$\ \mathsf{Stern.KGen}()$
2 : $\Pi^{\mathrm{F}} \leftarrow \varnothing$
3 : $(m, \zeta) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{F}}(\mathsf{pk})$
4 : **return** $\mathsf{Stern.SigVer}(\mathsf{pk}, m, \zeta)$

Oracle $\mathrm{F}(\alpha)$

1 : **if** $\alpha \in \Pi^{\mathrm{F}} : \beta \leftarrow \Pi^{\mathrm{F}}(\alpha)$
2 : **else**
3 : $\quad \beta \xleftarrow{\mathcal{U}} \{0,1,2\}^\delta$
4 : $\quad \Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
5 : **return** β

Определение 44. Для схемы подписи Stern.Σ *преимущество нарушителя* $\mathcal{A}$ *в модели* EUF-CMA *с доступом к случайному оракулу* обозначим через

$$\mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) \Rightarrow 1],$$

где эксперимент $\mathbf{Exp}^{\text{EUF-CMA}}_{\text{Stern}}$ определен следующим образом:

$\mathbf{Exp}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A})$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow\!\!\$\ \mathsf{Stern.KGen}()$
2 : $\mathcal{L} \leftarrow \varnothing$
3 : $\Pi^{\mathrm{F}} \leftarrow \varnothing$
4 : $(m, \zeta) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Sign},\mathrm{F}}(\mathsf{pk})$
5 : **if** $m \in \mathcal{L}$: **return** 0
6 : **return** $\mathsf{Stern.SigVer}(\mathsf{pk}, m, \zeta)$

Oracle $\mathrm{F}(\alpha)$

1 : **if** $\alpha \in \Pi^{\mathrm{F}} : \beta \leftarrow \Pi^{\mathrm{F}}(\alpha)$
2 : **else**
3 : $\quad \beta \xleftarrow{\mathcal{U}} \{0,1,2\}^{\delta}$
4 : $\quad \Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
5 : **return** β

Oracle $\mathrm{Sign}(m)$

1 : $\zeta \leftarrow\!\!\$\ \mathsf{Stern.SigGen}(\mathsf{sk}, m)$
2 : $\mathcal{L} \leftarrow \mathcal{L} \cup \{m\}$
3 : **return** ζ

4.2. Обоснование стойкости новой схемы подписи

Для проведения дальнейших рассуждений нам необходимо ввести несколько дополнительных определений.

Определение 45. *Плотностью* троичного дерева T глубины δ с N листьями назовем величину $N/3^{\delta}$.

Определение 46. Назовем дерево *ρ-плотным деревом*, если его плотность не меньше, чем ρ.

Определение 47. Назовем дерево *равномерно ρ-плотностным деревом*, если каждое его поддерево, не считая листьев, является ρ-плотным деревом.

Утверждение 34. *Если рассматривать ρ-плотное дерево T, все листья которого имеют глубину δ, как граф, то в нем существует подграф, который является равномерно $\frac{\rho}{\delta}$-плотным деревом с тем же корнем.*

Доказательство. Приведем алгоритм построения такого поддерева. Будем идти от яруса $\delta - 1$ к корню (ярусу 0) и исключать из дерева вершины, которые

являются корнями поддеревьев плотности меньшей, чем $\theta = \frac{\rho}{\delta}$. Отметим, что пока алгоритм не остановится, т.е. не дойдет до корня, структура дерева может быть отличной от исходной (а именно ветви могут иметь глубину отличную от δ). Однако после завершения алгоритма каждый из оставшихся листьев будет иметь глубину равную δ.

Покажем, что на каждом шаге этого алгоритма плотность корня уменьшается не более, чем на θ. Для этого рассмотрим ярус с номером i. Пусть на этом ярусе в исходном дереве T расположено κ вершин. Плотности образованных ими поддеревьев есть $\rho_{i,1}, \ldots, \rho_{i,\kappa}$. Если t означает количество листьев дерева T, то

$$\rho_{i,1} + \ldots + \rho_{i,\kappa} = \frac{t}{3^{\delta - i}} = 3^i \rho.$$

После окончания работы алгоритма на i-ом ярусе из дерева исключены вершины плотности меньше, чем θ. Отсюда новая плотность дерева $\rho'_{i,j}$ равна либо $\rho_{i,j}$, либо 0, если $\rho_{i,j} < \theta$. Тогда

$$\rho'_{i,1} + \ldots + \rho'_{i,\kappa} \geqslant \rho_{i,1} + \ldots + \rho_{i,\kappa} - \kappa\theta \geqslant 3^i \rho - \kappa\theta.$$

Для новой плотности корня ρ' выполнено $3^i \rho' \geqslant 3^i \rho - \kappa\theta$ и

$$\rho' \geqslant \rho - \frac{\kappa}{3^i}\theta \geqslant \rho - \theta.$$

В результате всех удалений ρ уменьшилась максимально на $(\delta - 1)\theta$. Так как $\theta = \frac{\rho}{\delta}$, то

$$\rho - (\delta - 1)\frac{\rho}{\delta} = \frac{\rho\delta - (\delta - 1)\rho}{\delta} = \frac{\rho}{\delta} = \theta.$$

То есть полученное дерево является равномерно θ-плотным. □

Теорема 21. *Пусть $\mathcal{A}$ — нарушитель, решающий задачу* EUF-NMA *для подписи на основе схемы идентификации Штерна, делая не более одного запроса к оракулу хэширования* F. *Тогда*

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \max\left\{15 \cdot \sqrt[3]{\frac{\delta^2 T}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \left(\frac{2}{3}\right)^{\delta}, \left(\frac{2}{3}\right)^{\delta}\left(1 + 2\delta \cdot 1.1^{\delta}\right)\right\},$$

где T_{SD} *и* T_{Coll} *— сложности оптимальных алгоритмов решения задачи* $\mathsf{SD}(H, y, \omega)$ *и* $\mathsf{Coll}(h)$ *с вероятностями успеха не менее* $1 - \frac{1}{e}$.

Доказательство. Обозначим

$$\varepsilon = \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) - \left(\frac{2}{3}\right)^{\delta}. \tag{4.1}$$

В случае $\varepsilon \leqslant 0$ доказательство завершено. Поэтому далее будем рассматривать случай

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) = \left(\frac{2}{3}\right)^{\delta} + \varepsilon,\ \varepsilon > 0.$$

Будем представлять работу нарушителя $\mathcal{A}$ на всех выходах случайного оракула F как неполное троичное дерево $T(x)$, в котором каждый лист имеет глубину δ. Оно задается случайной лентой x нарушителя $\mathcal{A}$. Каждый выход b_i случайного оракула соответствует определенному пути в дереве. Если значение b_i равно 0, то у вершины есть левый сын, если $b_i = 1$, то у вершины есть средний сын, и если $b_i = 2$, то у вершины есть правый сын. Если нарушитель не смог корректно построить подпись для некоторого случайного оракула, то соответствующая ему ветвь удаляется из дерева. Отметим, что фиксация ленты нарушителя гарантирует, что на каждом ярусе дерева проверяется часть подписи, соответствующая одному и тому же набору $(c_{i,0}, c_{i,1}, c_{i,2})$.

Покажем, что если в дереве найден ярус i на котором есть хотя бы три вершины $v_{i,0}, v_{i,1}$ и $v_{i,2}$ такие, что у вершины $v_{i,0}$ есть левый сын, у вершины $v_{i,1}$ есть средний сын и у вершины $v_{i,2}$ есть правый сын, то может быть решена одна из задач $\mathsf{SD}(H, y, \omega)$ и $\mathsf{Coll}(h)$. Здесь некоторые из этих вершин $v_{i,0}, v_{i,1}$ и $v_{i,2}$ могут совпадать. Далее представим алгоритм, который позволит нарушителю $\mathcal{A}$ найти эти вершины в дереве $T(x)$ с вероятностью $1 - \frac{1}{e}$.

Пусть в дереве есть такие вершины. Этот случай соответствует ситуации, когда нарушитель сгенерировал три корректные подписи в случае, когда на i-м шаге оракул выдал разные значения: $b_i = 0, b_i = 1$ и $b_i = 2$. Заметим, что из этого следует, что нарушитель построил по каждому из этих b_i ответ r_i, который прошел проверку, т.е. выли корректно восстановлены значения $c_{i,0}, c_{i,1}, c_{i,2}$.

Пусть на запрос $b_i = 0$ были получены значения $r_{i,0} = \sigma_0$ и $r_{i,1} = u_0$, на запрос $b_i = 1$ — значения $r_{i,0} = \sigma_1$ и $r_{i,1} = w_1$ (соответствующее $u_i \oplus s$) и σ_1 и, наконец, результатом запроса $b_i = 2$ стали $r_{i,0} = z_2$ (соответствующее $\sigma_i(u_i)$) и $r_{i,1} = t_2$ (соответствующее $\sigma_i(s)$). Поскольку c_0 может быть получено в двух случаях ($b_i = 0$ и $b_i = 1$), то

$$c_{i,0} = h(\sigma_0 \| H u_0^T) = h(\sigma_1 \| H w_1^T \oplus y).$$

Из этого следует, что либо у хэш-функции может быть найдена коллизия, либо $\sigma_0 = \sigma_1$ и $Hu_0^T = Hw_1^T \oplus y$. Аналогичные рассуждения позволяют показать, что если коллизия не была найдена, то $z_2 = \sigma_0(u_0)$ и $z_2 \oplus t_2 = \sigma_1(w_1)$. Отметим, что поскольку третий ответ был принят, то t_2 удовлетворяет ограничению на вес. Обозначая $\sigma = \sigma_0 = \sigma_1$, имеем

$$t_2 = z_2 \oplus (t_2 \oplus z_2) = \sigma(u_0 \oplus w_1).$$

Отсюда $u_0 \oplus w_1$ также имеет нужный вес. Теперь

$$H(u_0 \oplus w_1)^T = Hu_0^T \oplus Hw_1^T = y$$

и $u_0 \oplus w_1$ — это приемлемый секретный ключ.

Обозначим $\theta = \frac{\varepsilon}{2\delta}$. Теперь опишем теперь вероятностный алгоритм поиска дерева с вершинами $v_{i,0}, v_{i,1}$ и $v_{i,2}$.

Алгоритм 1

- Случайным образом выбрать значение x случайной ленты нарушителя (т.е. определить дерево $T(x)$);
- Задать $\frac{60}{\theta^2}$ выходов случайного оракула (т.е. определить столько ветвей этого дерева);
- Просмотреть дерево по ярусам в поиске вершин $v_{i,0}, v_{i,1}$ и $v_{i,2}$. Если они найдены, то решить одну из задач $\mathsf{SD}(H, y, \omega)$ и $\mathsf{Coll}(h)$. Иначе вернуться на Шаг 1.

Лемма 4. *В предположениях Теоремы 21 вероятность успеха каждого запуска Алгоритма 1 не менее, чем* $\frac{\varepsilon}{4}$*, где* ε *определено как в* (4.1).

Доказательство. Определим множество X как

$$X = \{x \mid \text{в } T(x) \text{ не менее } 2^\delta + \frac{\varepsilon}{2} \cdot 3^\delta \text{ веток} T(x)\}.$$

Тогда $\Pr[x \in X] \geqslant \varepsilon/2$.

Иначе пусть $\Pr[x \in X] < \varepsilon/2$. Обозначим количество листьев в дереве $T(x)$ через t. Тогда $\Pr[\mathcal{A} \Rightarrow 1 \wedge x \notin X] = t/3^\delta < (2/3)^\delta + \varepsilon/2$. Следовательно, вероятность успеха нарушителя $\mathcal{A}$ есть

$$\Pr[\mathcal{A} \Rightarrow 1] = \Pr[\mathcal{A} \Rightarrow 1 \wedge x \in X] + \Pr[\mathcal{A} \Rightarrow 1 \wedge x \notin X] \leqslant \Pr[x \in X] + \\ + \Pr[\mathcal{A} \Rightarrow 1 \wedge x \notin X] < \varepsilon/2 + \big((2/3)^\delta + \varepsilon/2\big) = (2/3)^\delta + \varepsilon.$$

Однако это противоречит предположению Теоремы 21.

Рассмотрим отдельно случай $x \in X$. Заметим, что X задает множество $\varepsilon/2$-плотных деревьев. Поэтому по Предложению 34 из каждого такого дерева можно выделить поддерево, которое будет равномерно θ-плотным с листьями глубины δ. Назовем такое дерево $T_1(x)$.

Для любого индекса $i, 0 \leqslant i \leqslant \delta$ обозначим через $n_{i,1}, n_{i,2}$ и $n_{i,3}$ количество вершин на уровне i в $T_1(x)$. Общее число вершин на уровне i обозначим через n_i. Тогда для $0 \leqslant i < \delta$ выполнено, что

$$n_{i+1} = n_{i,1} + 2n_{i,2} + 3n_{i,3} = n_i + n_{i,2} + 2n_{i,3}. \tag{4.2}$$

Пусть $q = \max_i n_{i,3}/n_i$. Тогда $n_{i,3} \leqslant q n_i$. Из (4.2) следует, что

$$n_{i+1} \leqslant n_i + n_{i,2} + 2qn_i \leqslant 2n_i + 2qn_i = 2n_i(1+q).$$

Из определения равномерной θ-плотности дерева для каждого $i : 0 \leqslant i \leqslant \delta$ выполнено неравенство:

$$n_i \geqslant 3^i \theta.$$

Тогда

$$3^\delta\theta \leqslant n_\delta \leqslant 2^\delta n_0(1+q)^\delta.$$

Поскольку $n_0 = 1$ ($i = 0$ соответствует корню дерева), имеем

$$\delta\ln(1+q) + \delta\ln 2 \geqslant \ln\theta + \delta\ln 3.$$

Разделив на δ, мы наконец получаем

$$q \geqslant \frac{3}{2}\cdot\theta^{\frac{1}{\delta}} - 1.$$

Теперь зафиксируем $\alpha := \log_{\frac{3}{2}}\left(1.1\cdot(2\delta)^{\frac{1}{\delta}}\right)$ и рассмотрим отдельно два случая.

Если $\varepsilon \leqslant \left(\frac{2}{3}\right)^{\delta(1-\alpha)}$ то

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \left(\frac{2}{3}\right)^\delta\left(1+\left(\frac{2}{3}\right)^{-\alpha\delta}\right) = \left(\frac{2}{3}\right)^\delta\left(1+2\delta\cdot 1.1^\delta\right).$$

Иначе, если $\varepsilon > \left(\frac{2}{3}\right)^{\delta(1-\alpha)}$ то верно, что

$$\theta^{\frac{1}{\delta}} = \left(\frac{\varepsilon}{2\delta}\right)^{\frac{1}{\delta}} < \left(\frac{\left(\frac{2}{3}\right)^{\delta(1-\alpha)}}{2\delta}\right)^{\frac{1}{\delta}} = \frac{\left(\frac{2}{3}\right)^{(1-\alpha)}}{\sqrt[\delta]{2\delta}}.$$

Можно проверить, что для α, определенного так, как это было сделано выше, выполняется неравенство $q \geqslant 0.1$. Отметим, что q на самом деле не зависит от θ.

Пусть j есть номер уровня, на котором достигается максимальное значение q. Тогда $n_{j,3} = qn_j$. Обозначим через $L_j(\pi)$ предикат: путь π лежит в $T_1(x)$ и проходит через левого сына некоторой вершины уровня j. Аналогично можно определить предикаты $C_j(\pi)$ и $R_j(\pi)$. Через L_j обозначим предикат $(\exists\pi : L_j(\pi))$.

Тогда справедливо следующее неравенство:

$$\begin{aligned}\Pr[L_j] &\geqslant \Pr[\exists\pi : (v_1\in\pi \vee v_2\in\pi \vee \ldots \vee v_{n_{j,3}}\in\pi)\wedge L_j(\pi)] = \\ &= \sum_{i=1}^{n_{j,3}}\Pr[\exists\pi : (v_i\in\pi)\wedge L_j(\pi)].\end{aligned}$$

Здесь v_i — это вершина j-го уровня, имеющая трех сыновей. Для такой вершины гарантировано существование левого сына.

Вероятность $\Pr[\exists\pi : (v_i \in \pi) \wedge L_j(\pi)]$ для $1 \leqslant i \leqslant n_{j,3}$ равна числу S путей в $T_1(x)$, проходящих через левого сына v_i, деленному на 3^δ. В поддереве с корнем v_i существует не более $3^{\delta-j-1}$ листьев. Но, поскольку $T_1(x)$ — это равномерно θ-плотное дерево, то

$$S \geqslant 3^{\delta-j-1}\theta \Rightarrow \Pr[\exists\pi : (v_i \in \pi) \wedge L_j(\pi)] \geqslant \frac{3^{\delta-j-1}\theta}{3^\delta}.$$

Отсюда можем заключить, что

$$\Pr[L_j] \geqslant n_{j,3} \cdot \frac{3^{\delta-j-1}\theta}{3^\delta} = \frac{n_{j,3}}{3^j} \cdot \frac{\theta}{3} = \frac{n_{j,3}}{n_j} \cdot \frac{n_j}{3^j} \cdot \frac{\theta}{3} \geqslant q \cdot \theta \cdot \frac{\theta}{3} \geqslant \frac{\theta^2}{30}.$$

Теперь найдем вероятность P того, что, выбирая $\frac{60}{\theta^2}$ ветвей π_j, на j-ом уровне дерева $T_1(x)$ мы найдем вершины $v_{j,0}, v_{j,1}$ и $v_{j,2}$.

$$\begin{aligned}
P &= \Pr[\exists j_0, j_1, j_2 : L_j(\pi_{j_0}) \wedge C_j(\pi_{j_1}) \wedge R_j(\pi_{j_2})] = \\
&= 1 - \Pr[\nexists j_0 : L_j(\pi_{j_0}) \vee \nexists j_1 : C_j(\pi_{j_1}) \vee \nexists j_2 : R_i(\pi_{j_2})] \geqslant \\
&\geqslant 1 - \Pr[\nexists j_0 : L_j(\pi_{j_0})] - \Pr[\nexists j_1 : C_j(\pi_{j_1})] - \Pr[\nexists j_2 : R_j(\pi_{j_2})] = \\
&= 1 - 3\Pr[\nexists j_0 : L_j(\pi_{j_0})] = 1 - 3\Pr[\overline{L}_j]^{\frac{60}{\theta^2}} = 1 - 3(1 - \Pr[L_j])^{\frac{60}{\theta^2}} \geqslant \\
&\geqslant 1 - 3\left(1 - \frac{\theta^2}{30}\right)^{\frac{60}{\theta^2}} \geqslant 1 - \frac{3}{e^2}.
\end{aligned}$$

Таким образом, вероятность успеха Алгоритма 1 поиска вершин $v_{i,0}, v_{i,1}$ и $v_{i,2}$ складывается из вероятностей выбора плотного дерева $T(x)$ и вероятности P. Она равна $p := \frac{\varepsilon}{2} \cdot (1 - \frac{3}{e^2}) > \frac{\varepsilon}{4}$. □

Алгоритм 1 запускается некоторым нарушителем $\mathcal{B}$ $1/p$ раз. Сложность одного запуска равна $T' := \frac{60T}{\theta^2}$. Вероятность того, что за $1/p$ попытку не случится ни одного успеха есть $(1-p)^{\frac{1}{p}}$. Тогда вероятность $\mathcal{B}$ есть $1 - (1-p)^{\frac{1}{p}}$. Покажем, что

$$1 - (1-p)^{\frac{1}{p}} > 1 - \frac{1}{e}.$$

В самом деле, разложения в ряд Маклорена функций $\frac{1}{1-p}$ и e^p имеют вид:

$$\frac{1}{1-p} = 1 + p + p^2 + \ldots, \quad e^p = 1 + \frac{p}{1!} + \frac{p^2}{2!} + \ldots,$$

поэтому для всех $p \in (0,1)$ выполнено

$$\frac{1}{1-p} > e^p \Rightarrow (1-p) < \frac{1}{e^p} \Rightarrow (1-p)^{\frac{1}{p}} < \frac{1}{e}.$$

Итоговая сложность нарушителя $\mathcal{B}$ есть $T'' := \frac{T'}{p} < \frac{240T}{\theta^2\varepsilon}$. Пусть $\mathcal{B}$ решает задачу $\mathsf{SD}(H, y, \omega)$ с вероятностью p_1, а $\mathsf{Coll}(h)$ — с вероятностью p_2. Тогда

$$p_1 + p_2 = 1 - \frac{1}{e}.$$

Назовем $T_{\mathsf{SD},\left(1-\frac{1}{e}\right)}$ — сложность оптимального алгоритма решения задачи синдромного декодирования с вероятностью успеха $1 - \frac{1}{e}$, а $T_{\mathsf{Coll},\left(1-\frac{1}{e}\right)}$ — сложность оптимального алгоритма поиска коллизии хэш-функции с вероятностью успеха $1 - \frac{1}{e}$. Тогда

$$T_{\mathsf{SD},\left(1-\frac{1}{e}\right)} \leqslant \frac{1}{p_1} T_{\mathsf{SD},p_1} \leqslant \frac{1}{p_1} T'',$$
$$T_{\mathsf{Coll},\left(1-\frac{1}{e}\right)} \leqslant \frac{1}{p_2} T_{\mathsf{Coll},p_2} \leqslant \frac{1}{p_2} T''.$$

Первые неравенства следуют из того, что повторение $\frac{1}{p_1}$ раза алгоритма с вероятностью успеха p_1 дает алгоритм с вероятностью успеха $1 - \frac{1}{e}$, однако, возможно, неоптимальный по сложности. Второе неравенство следует из того, что $\mathcal{B}$ решает одну из двух задач, соответственно, имеет сложность не менее сложности алгоритма, решающего одну из них.

Отсюда

$$T'' \geqslant p_1 T_{\mathsf{SD},\left(1-\frac{1}{e}\right)} \quad \text{и} \quad T'' \geqslant p_2 T_{\mathsf{Coll},\left(1-\frac{1}{e}\right)}.$$

Следовательно, обозначая $\widetilde{T} = \min\left\{T_{\mathsf{SD},\left(1-\frac{1}{e}\right)}, T_{\mathsf{Coll},\left(1-\frac{1}{e}\right)}\right\}$, можно переписать

$$T'' \geqslant \frac{1}{2}\left(p_1 T_{\mathsf{SD},\left(1-\frac{1}{e}\right)} + p_2 T_{\mathsf{Coll},\left(1-\frac{1}{e}\right)}\right) \geqslant \frac{1}{2}(p_1 + p_2)\widetilde{T} \geqslant \frac{1-\frac{1}{e}}{2}\,\widetilde{T}.$$

Эквивалентно,

$$\frac{960\delta^2 T}{\varepsilon^3} \geqslant \frac{1-\frac{1}{e}}{2}\,\widetilde{T}.$$

Выражая из последнего неравенства ε и замечая, что $\sqrt[3]{\frac{1920}{1-\frac{1}{e}}} \leqslant 15$, получаем:

$$\varepsilon \leqslant 15 \cdot \sqrt[3]{\frac{\delta^2 T}{\widetilde{T}}}.$$

Наконец для $\varepsilon > \left(\frac{2}{3}\right)^{\delta(1-\alpha)}$ получаем

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) \leqslant 15 \cdot \sqrt[3]{\frac{\delta^2 T}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \left(\frac{2}{3}\right)^{\delta}.$$

А для произвольного ε выполнено, что

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \max\left\{15 \cdot \sqrt[3]{\frac{\delta^2 T}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \left(\frac{2}{3}\right)^{\delta}, \left(\frac{2}{3}\right)^{\delta}\left(1 + 2\delta \cdot 1.1^{\delta}\right)\right\}.$$

□

Теорема 22. *Пусть $\mathcal{A}$ — нарушитель, решающий задачу* EUF-NMA *для подписи на основе схемы идентификации Штерна, делая не более q_f запросов к оракулу хэширования* F. *Тогда существует такой нарушитель $\mathcal{B}$, который решает задачу* EUF-NMA *для этой подписи, делая не более одного запроса к оракулу хэширования и*

$$q_f \cdot \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \geqslant \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) - 3^{-\delta}.$$

Причем, если сложность нарушителя $\mathcal{A}$ равна T, то сложность нарушителя $\mathcal{B}$ есть $T + c' q_f$, где c' — константа, зависящая от модели вычисления.

Доказательство. Пусть оригинальному эксперименту в модели EUF-NMA с q_f запросами к оракулу хэширования F соответствует эксперимент $\mathbf{Exp}^0$. В этом эксперименте $\mathcal{A}$ — нарушитель, строящий экзистенциальную подделку для подписи на основе схемы идентификации Штерна с использованием случайного оракула F. Следовательно,

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) := \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1].$$

$\mathbf{Exp}^0(\mathcal{A})$

1 : $s \xleftarrow{\mathcal{U}} \{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = \omega\}$
2 : $y \leftarrow Hs^T$
3 : $\Pi^{\mathrm{F}} \leftarrow \varnothing$
4 : $(m, c\|r) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{F}}(y)$
5 : **return** $\mathsf{Stern.SigVer}(y, m, c\|r)$

Oracle $\mathrm{F}(\alpha)$

1 : **if** $\alpha \in \Pi^{\mathrm{F}} : \beta \leftarrow \Pi^{\mathrm{F}}(\alpha)$
2 : **else**
3 : $\quad \beta \xleftarrow{\mathcal{U}} \{0,1,2\}^{\delta}$
4 : $\quad \Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
5 : **return** β

Построим теперь по $\mathcal{A}$ нарушителя $\mathcal{B}$, строящего экзистенциальную подделку в модели с одним запросом к случайному оракулу. $\mathcal{B}$ симулирует оракул F, который способный выдать q_f ответов, при помощи алгоритма SimF_t. Здесь $\mathcal{A}^{\mathrm{SimF}_t}$ означает, что единственный запрос, который $\mathcal{B}$ делает к своему случайному оракулу F^* совпадает с t-ым запросом нарушителя $\mathcal{A}$ к оракулу F. Отметим, что выход оракула F^* имеет равномерное распределение, т.е. значения β, полученные на строках 3 и 4 оракула SimF_t невозможно различить.

$\mathcal{B}^{\mathrm{F}^*}(y)$

1 : $\Pi^{\mathrm{F}} \leftarrow \varnothing$
2 : $j \leftarrow 0$
3 : $t \xleftarrow{\mathcal{U}} \{1, \ldots, q_f\}$
4 : $(m, c\|r) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{SimF}_t}(y)$
5 : **return** $(m, c\|r)$

$\mathrm{SimF}_t(\alpha)$

1 : $j \leftarrow j + 1$
2 : **if** $(\alpha, \cdot) \in \Pi^{\mathrm{F}} : \beta \leftarrow \Pi^{\mathrm{F}}(\alpha)$
3 : **elseif** $j = t : \beta \leftarrow \mathrm{F}^*(\alpha)$
4 : **else** $: \beta \xleftarrow{\mathcal{U}} \{0,1,2\}^{\delta}$
5 : $\Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
6 : **return** β

Для генерации подписи нарушитель $\mathcal{A}$ может либо существенно использовать один запрос к оракулу F, либо не использовать ни одного из них. Пусть I — это случайная величина, которая соответствует числу запросов нарушителя $\mathcal{A}$ к оракулу F для создания подделки. В случае, если $\mathcal{A}$ не использует ни одного, положим $I = 0$. Отсюда

$$\begin{aligned}
&\Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1] \geqslant \\
&\geqslant \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge t = I] \geqslant \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge t = I \wedge I \geqslant 1] = \\
&= \Pr[t = I] \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge I \geqslant 1] \geqslant \frac{1}{q_f} \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge I \geqslant 1].
\end{aligned}$$

Отметим, что в случае, когда нарушитель $\mathcal{A}$ не использует ни одного запроса к случайному оракулу F, его вероятность успеха не превосходит $3^{-\delta}$, поскольку ему необходимо полностью угадать выход $b = \mathrm{F}(\alpha)$. Отсюда и из определения условной вероятности выполнено, что

$$\Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1] \leqslant \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge I \geqslant 1] + \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge I = 0] \leqslant$$
$$\leqslant \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1 \wedge I \geqslant 1] + 3^{-\delta}.$$

Следовательно,

$$\Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1] - 3^{-\delta} \leqslant q_f \cdot \Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1].$$

Объединяя приведенные выше рассуждения, получаем итоговое неравенство:

$$q_f \cdot \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) = q_f \cdot \Pr[\mathbf{Exp}(\mathcal{B}) \Rightarrow 1] \geqslant \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1] - 3^{-\delta} =$$
$$= \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{A}) - 3^{-\delta}.$$

$\mathcal{B}$ запускает $\mathcal{A}$ и симулирует q_f запросов к оракулу F. Таким образом, если сложность нарушителя $\mathcal{A}$ есть T, то сложность нарушителя $\mathcal{B}$ не превышает $T + c'q_f$ для некоторой константы c'. □

Теорема 23. *Пусть $\mathcal{A}$ — нарушитель, решающий задачу* EUF-CMA *для подписи на основе схемы идентификации Штерна, делая не более q_f запросов к оракулу хэширования* F *и не более q_s запросов к оракулу подписи* Sign. *Тогда существует такой нарушитель $\mathcal{B}$, который решает задачу* EUF-NMA *для этой подписи, делая не более q_f запросов к оракулу хэширования и*

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \geqslant \mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) - q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{Coll}}\right)^{\delta},$$

где T_{Coll} — сложность оптимального алгоритма решения задачи $\mathsf{Coll}(h)$ с вероятностью успехане менее $1 - \frac{1}{e}$, а $\tilde{c}$ — константа, зависящая от модели вычислений.

Причем, если сложность нарушителя $\mathcal{A}$ равна T, то сложность нарушителя $\mathcal{B}$ ограничена сверху значением $T + c''(q_f + q_s T_{\text{Stern}}^{Sig})$, где T_{Stern}^{Sig} — сложность алгоритма генерации подписи, а c'' — константа, зависящая от модели вычислений.

Доказательство. Пусть оригинальному эксперименту в модели EUF-CMA соответствует эксперимент $\mathbf{Exp}^0$. В этом эксперименте $\mathcal{A}$ — нарушитель, строящий экзистенциальную подделку для подписи на основе схемы идентификации Штерна с использованием случайного оракула F и оракула подписи Sign. Мы предполагаем, что $\mathcal{A}$ может сделать не более q_f запросов к оракулу F и не более q_s запросов к оракулу Sign.

$$\mathsf{Adv}_{\text{Stern}}^{\text{EUF-CMA}}(\mathcal{A}) := \Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1].$$

Эксперимент $\mathbf{Exp}^1$ представляет собой модификацию $\mathbf{Exp}^0$ в которой используются множества $\Pi^S, \Pi \subset \mathbb{F}_2^* \times \{0,1,2\}^\delta$. Множество Π^S заполняется в процессе взаимодействия с оракулом Sign, а $\Pi = \Pi^{\text{F}} \cup \Pi^S$.

Модификации алгоритмов F и Sign не влияют на распределения их выходов, откуда

$$\Pr[\mathbf{Exp}^0(\mathcal{A}) \Rightarrow 1] = \Pr[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1].$$

$\mathbf{Exp}^{0}(\mathcal{A}) = \mathbf{Exp}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A})$

$s \xleftarrow{\mathcal{U}} \{x \in \mathbb{F}_2^n : \text{wt}(x) = \omega\}$
$y \leftarrow Hs^T$
$\mathcal{L} \leftarrow \varnothing$
$\Pi^{\text{F}} \leftarrow \varnothing$
$(m, c\|r) \leftarrow\!\!\$\ \mathcal{A}^{\text{Sign,F}}(y)$
if $m \in \mathcal{L}$: **return** 0
return $\mathsf{Stern.SigVer}(y, m, c\|r)$

Oracle $\text{F}(\alpha)$

if $\alpha \in \Pi^{\text{F}}$: $\beta \leftarrow \Pi^{\text{F}}(\alpha)$
else
  $\beta \xleftarrow{\mathcal{U}} \{0,1,2\}^{\delta}$
  $\Pi^{\text{F}} \leftarrow \Pi^{\text{F}} \cup \{(\alpha, \beta)\}$
return β

Oracle $\text{Sign}(s, m)$

foreach $0 \leqslant i < \delta$:
  $u_i \xleftarrow{\mathcal{U}} \mathbb{F}_2^n, \sigma_i \xleftarrow{\mathcal{U}} \mathcal{S}_n$
  $c_{i,0} \leftarrow h(\sigma_i \| H u_i^T)$
  $c_{i,1} \leftarrow h(\sigma_i(u_i))$
  $c_{i,2} \leftarrow h(\sigma_i(u_i \oplus s))$
  $c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$
$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$
$b \leftarrow \text{F}(m\|c)$
foreach $0 \leqslant i < \delta$:
  if $b_i = 0 : r_i \leftarrow \sigma_i \| u_i$
  if $b_i = 1 : r_i \leftarrow \sigma_i \| (u_i \oplus s)$
  if $b_i = 2 : r_i \leftarrow \sigma_i(u_i) \| \sigma_i(s)$
$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$
$\mathcal{L} \leftarrow \mathcal{L} \cup \{m\}$
return $c\|r$

$\mathbf{Exp}^1(\mathcal{A})$

1: $s \xleftarrow{\mathcal{U}} \{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = \omega\}$
2: $y \leftarrow Hs^T$
3: $\mathcal{L} \leftarrow \varnothing$
4: $(\Pi^{\mathrm{F}}, \Pi^S) \leftarrow (\varnothing, \varnothing)$
5: $\Pi \leftarrow \Pi^{\mathrm{F}} \cup \Pi^S$
6: $(m, c\|r) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{Sign,F}}(y)$
7: **if** $m \in \mathcal{L}$: **return** 0
8: **return** $\mathsf{Stern.SigVer}(y, m, c\|r)$

Oracle $\mathrm{F}(\alpha)$

1: **if** $(\alpha, \cdot) \in \Pi$: **return** $\Pi(\alpha)$
2: $\beta \xleftarrow{\mathcal{U}} \{0,1,2\}^\delta$
3: $\Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
4: $\Pi \leftarrow \Pi^{\mathrm{F}} \cup \Pi^S$
5: **return** β

Oracle $\mathrm{Sign}(s, m)$ $(\mathbf{Exp}^1)$

1: **foreach** $0 \leqslant i < \delta$:
2: $\quad u_i \xleftarrow{\mathcal{U}} \mathbb{F}_2^n, \sigma_i \xleftarrow{\mathcal{U}} \mathcal{S}_n$
3: $\quad c_{i,0} \leftarrow h(\sigma_i \| H u_i^T)$
4: $\quad c_{i,1} \leftarrow h(\sigma_i(u_i))$
5: $\quad c_{i,2} \leftarrow h(\sigma_i(u_i \oplus s))$
6: $\quad c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$
7: $c \leftarrow c_0 \| \ldots \| c_{\delta-1}$
8: **if** $(m\|c, \cdot) \in \Pi : b \leftarrow \Pi(m\|c)$
9: **else**
10: $\quad b \xleftarrow{\mathcal{U}} \{0,1,2\}^\delta$
11: $\quad \Pi^S \leftarrow \Pi^S \cup \{(m\|c, b)\}$
12: $\quad \Pi \leftarrow \Pi^{\mathrm{F}} \cup \Pi^S$
13: **foreach** $0 \leqslant i < \delta$:
14: $\quad$ **if** $b_i = 0 : r_i \leftarrow \sigma_i \| u_i$
15: $\quad$ **if** $b_i = 1 : r_i \leftarrow \sigma_i \| (u_i \oplus s)$
16: $\quad$ **if** $b_i = 2 : r_i \leftarrow \sigma_i(u_i) \| \sigma_i(s)$
17: $r \leftarrow r_0 \| \ldots \| r_{\delta-1}$
18: $\mathcal{L} \leftarrow \mathcal{L} \cup \{m\}$
19: **return** $c\|r$

Эксперимент $\mathbf{Exp}^2$ отличается от эксперимента $\mathbf{Exp}^1$ только алгоритмом Sign. В нем больше не используется секретный ключ. Вместо этого результат формируется по случайному вектору b.

Покажем, что распределения выходов $c\|r$ алгоритма Sign в экспериментах $\mathbf{Exp}^1$ и $\mathbf{Exp}^2$ неразличимы в случае, когда не выполнено условие со строки 23. Для этого достаточно показать, что распределения каждой части подписи вида $c_i\|r_i = c_{i,0}\|c_{i,1}\|c_{i,2}\|r_{i,0}\|r_{i,1}$ для $i = 0, \ldots, \delta - 1$ из эксперимента $\mathbf{Exp}^2$ совпадает с распределением соответствующей части подписи из $\mathbf{Exp}^1$.

Oracle Sign(m) ($\mathbf{Exp}^2$)

$s' \xleftarrow{\mathcal{U}} \{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = \omega\}$
foreach $0 \leqslant i < \delta$:
  $b_i \xleftarrow{\mathcal{U}} \{0, 1, 2\}$
  $u'_i \xleftarrow{\mathcal{U}} \mathbb{F}_2^n, \sigma'_i \xleftarrow{\mathcal{U}} \mathcal{S}_n,$
  if $b_i = 0$:
    $c_{i,0} \leftarrow h(\sigma'_i \| H u_i'^T)$
    $c_{i,1} \leftarrow h(\sigma'_i(u'_i))$
    $c_{i,2} \leftarrow h(\sigma'_i(u'_i \oplus s'))$
    $r_i \leftarrow \sigma'_i \| u'_i$
  if $b_i = 1$:
    $c_{i,0} \leftarrow h(\sigma'_i \| (H u_i'^T \oplus y))$
    $c_{i,1} \leftarrow h(\sigma'_i(s'))$
    $c_{i,2} \leftarrow h(\sigma'_i(u'_i))$
    $r_i \leftarrow \sigma'_i \| u'_i$
  if $b_i = 2$:
    $c_{i,0} \leftarrow h(\sigma'_i \| H(u'_i \oplus s')^T)$
    $c_{i,1} \leftarrow h(\sigma'_i(u'_i \oplus s'))$
    $c_{i,2} \leftarrow h(\sigma'_i(u'_i))$
    $r_i \leftarrow \sigma'_i(u'_i \oplus s') \| \sigma'_i(s')$
  $c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$
$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$
$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$
if $(m \| c, \cdot) \in \Pi^{\mathrm{F}}$: **abort**
$\Pi^S \leftarrow \Pi^S \cup \{(m \| c, b)\}$
$\Pi \leftarrow \Pi^{\mathrm{F}} \cup \Pi^S$
$\mathcal{L} \leftarrow \mathcal{L} \cup \{m\}$
return $c \| r$

Далее будем рассматривать аргументы хэш-функции h, соответствующие хэш-значениям $c_{i,j}$ вместо них самих. Это решение обусловлено тем фактом, что при совпадении распределений величин ξ и η также совпадают и распределения величин $h(\xi)$ и $h(\eta)$. В самом деле,

$$\Pr[h(\xi) = a] = \Pr[\xi \in h^{-1}(a)] = \Pr[\eta \in h^{-1}(a)] = \Pr[h(\eta) = a].$$

В случае, когда $b_i = 0$, для стороннего наблюдателя секретный ключ s является случайной величиной. Остальные значения выбираются случайно, также как это делалось в оригинальном протоколе. Таким образом, распределения, очевидно, совпадают.

Если $b_i = 1$, то вероятность того, что в эксперименте $\mathbf{Exp}^1$ строка $c_i \| r_i$

равна $a_1\|a_2\|a_3\|a_4\|a_5\|a_6$ есть

$$
\begin{aligned}
&P_{a_1,a_2,a_3,a_4,a_5,a_6} = \\
&= \Pr\left[\sigma_i = a_1, Hu_i^T = a_2, \sigma_i(u_i) = a_3, \sigma_i(u_i \oplus s) = a_4, \sigma_i = a_5, u_i \oplus s = a_6\right] = \\
&\qquad = \mathbb{I}\big[a_1 = a_5,\ H(a_6 \oplus s)^T = a_2, a_1(a_6) = a_4\big] \times \\
&\qquad\qquad \times \Pr\left[\sigma_i = a_1, s = a_1^{-1}(a_3) \oplus a_6, u_i = a_1^{-1}(a_3)\right],
\end{aligned}
$$

где $\mathbb{I}\big[\theta\big]$ означает индикатор выражения θ. В эксперименте $\mathbf{Exp}^2$ эта вероятность равна

$$
\begin{aligned}
&\widehat{P}_{a_1,a_2,a_3,a_4,a_5,a_6} = \\
&= \Pr\left[\sigma'_i = a_1, Hu_i'^T \oplus y = a_2, \sigma'_i(s') = a_3, \sigma'_i(u'_i) = a_4, \sigma'_i = a_5, u'_i = a_6\right] = \\
&= \mathbb{I}\big[a_1 = a_5, Ha_6^T \oplus y = a_2, a_1(a_6) = a_4\big] \Pr\left[\sigma'_i = a_1, s' = a_1^{-1}(a_3), u'_i = a_6\right].
\end{aligned}
$$

Поскольку $H(a_6 \oplus s)^T = Ha_6^T \oplus y$, индикаторы этих двух выражений совпадают.

Теперь вычислим вероятности. Отметим, что поскольку все случайные величины выбраны независимо, то вероятность пересечения событий равна произведению их вероятностей. Поэтому можем искать их независимо.

$$
\begin{aligned}
&\Pr[\sigma_i = a_1] = \Pr[\sigma'_i = a_1] = \frac{1}{n!}, \\
&\Pr[s = a_1^{-1}(a_3) \oplus a_6 = a'] = \frac{1}{2^n}, \\
&\Pr[u_i = a_1^{-1}(a_3) = a''] = \frac{1}{2^n}, \\
&\Pr[s' = a_1^{-1}(a_3) = a'''] = \frac{1}{2^n}, \\
&\Pr[u'_i = a_6] = \frac{1}{2^n}
\end{aligned}
$$

для любых констант a', a'' и a'''. Тогда

$$
\Pr\left[\sigma_i = a_1, s = a_1^{-1}(a_3) \oplus a_6, u_i = a_1^{-1}(a_3)\right] = \Pr\left[\sigma'_i = a_1, s' = a_3, u'_i = a_6\right] = \frac{1}{n!2^{2n}}
$$

и распределения неразличимы.

Наконец, если $b_i = 2$, то аналогичная рассмотренному выше случаю вероятность в эксперименте $\mathbf{Exp}^1$ есть

$$P_{a_1,a_2,a_3,a_4,a_5,a_6} =$$
$$= \Pr\left[\sigma_i = a_1, Hu_i^T = a_2, \sigma_i(u_i) = a_3, \sigma_i(u_i \oplus s) = a_4, \sigma_i(u_i) = a_5, \sigma_i(s) = a_6\right] =$$
$$= \mathbb{I}\big[a_3 = a_5, a_3 \oplus a_6 = a_4, H(a_1^{-1}(a_3))^T = a_2\big] \times$$
$$\times \Pr\left[\sigma_i = a_1, u_i = a_1^{-1}(a_3), s = a_1^{-1}(a_6)\right]$$

а в эксперименте $\mathbf{Exp}^2$ она равна

$$\widehat{P}_{a_1,a_2,a_3,a_4,a_5,a_6} = \Pr\left[\sigma'_i = a_1, H(u'_i \oplus s')^T = a_2, \sigma'_i(u'_i \oplus s') = a_3, \sigma'_i(u'_i) = a_4,\right.$$
$$\left.\sigma'_i(u'_i \oplus s') = a_5, \sigma'_i(s') = a_6\right) = \mathbb{I}\big[a_3 = a_5, a_4 \oplus a_6 = a_3, H(a_1^{-1}(a_3))^T = a_2\big] \times$$
$$\times \Pr\left[\sigma'_i = a_1, u'_i = a_1^{-1}(a_4), s' = a_1^{-1}(a_6)\right].$$

Применяя рассуждения, аналогичные сделанным выше, получаем, что

$$\Pr\left[\sigma_i = a_1, u_i = a_1^{-1}(a_3), s = a_1^{-1}(a_6)\right] =$$
$$= \Pr\left[\sigma'_i = a_1, u'_i = a_1^{-1}(a_4), s' = a_1^{-1}(a_6)\right] = \frac{1}{n!2^{2n}}$$

и распределения совпадают.

Проверка на строке 23 соответствует случаю, когда значение c, сгенерированное в процессе создания подписи под сообщением m, уже лежало в множестве Π^{F}. Будем рассматривать худший случай, в котором нарушитель $\mathcal{A}$ сначала делает все q_f запросов к оракулу хэширования F. Обозначим через p вероятность того, что условие было выполнено для некоторого сообщения на одном из q_s запросов:

$$p := \Pr\left[c \in \Pi_c^F\right],$$

где

$$\Pi_c^{\mathrm{F}} = \{c \in \mathbb{F}_2^{3\delta\ell} \mid \exists m \in \mathbb{F}_2^*, \exists \beta \in \{0,1,2\}^\delta : (m\|c, \beta) \in \Pi^{\mathrm{F}}\}.$$

Для строки c и множества $\Pi \subset \mathbb{F}_2^* \times \mathbb{F}_2^{3\delta\ell} \times \{0,1,2\}^\delta$ введем проекцию этого множества на часть строки как

$$\Pi_{c,(0,1)} = \{c_{0,1} \mid \exists m \in \mathbb{F}_2^*, \exists c \in \mathbb{F}_2^{3\delta\ell}, \exists \beta \in \{0,1,2\}^\delta : (m\|c, \beta) \in \Pi\}.$$

Аналогично для кортежа $c_{*,1} = (c_{0,1}, \ldots, c_{\delta-1,1})$ определим множество

$$\Pi_{c,(*,1)} = \{c_{*,1} \mid \exists m \in \mathbb{F}_2^*, \exists c \in \mathbb{F}_2^{3\delta\ell}, \exists \beta \in \{0,1,2\}^\delta : (m\|c,\beta) \in \Pi\}.$$

Тогда для множества $\Pi \subset \mathbb{F}_2^* \times \mathbb{F}_2^{3\delta\ell} \times \{0,1,2\}^\delta$ верно неравенство

$$p \leqslant \sum_{\Pi} \Pr[\Pi^{\mathrm{F}} = \Pi \wedge c_{*,1} \in \Pi_{c,(*,1)}].$$

Отметим, что первое событие задано случайным оракулом нарушителя $\mathcal{A}$, в то время как второе задано оракулом подписи. Из этого следует, что эти события независимы и

$$p \leqslant \sum_{\Pi} \Pr[\Pi^{\mathrm{F}} = \Pi] \Pr[c_{*,1} \in \Pi_{c,(*,1)}].$$

Поскольку все c_i являются функциями независимых случайных величин для всех $i \in \{0, \delta-1\}$, то события $c_{i,1} \in \Pi^{\mathrm{F}}_{c,(i,1)}$ также независимы. Отсюда

$$\begin{aligned}
p &\leqslant \sum_{\Pi} \Pr[\Pi^{\mathrm{F}} = \Pi] \prod_{i=0}^{\delta-1} \Pr[c_{i,1} \in \Pi_{c,(i,1)}] \leqslant \\
&\leqslant \sum_{\Pi} \Pr[\Pi^{\mathrm{F}} = \Pi] \left(\max_{i \in \{0,\delta-1\}} \Pr[c_{i,1} \in \Pi_{c,(i,1)}] \right)^\delta \leqslant \\
&\leqslant \left(\max_{\Pi} \max_{i \in \{0,\delta-1\}} \Pr[c_{i,1} \in \Pi_{c,(i,1)}] \right)^\delta \sum_{\Pi} \Pr[\Pi^{\mathrm{F}} = \Pi] = \\
&= \left(\max_{\Pi} \max_{i \in \{0,\delta-1\}} \Pr[c_{i,1} \in \Pi_{c,(i,1)}] \right)^\delta \leqslant \left(\max_{\Pi} \max_{i \in \{0,\delta-1\}} \sum_{y \in \Pi_{c,(i,1)}} \Pr[c_{i,1} = y] \right)^\delta \leqslant \\
&\leqslant \left(\max_{\Pi} \max_{i \in \{0,\delta-1\}} \left|\Pi_{c,(i,1)}\right| \max_{y \in \Pi_{c,(i,1)}} \Pr[c_{i,1} = y] \right)^\delta \leqslant \\
&\leqslant \left(q_f \max_{i \in \{0,\delta-1\}} \max_{y \in \mathbb{F}_2^\ell} \Pr[h(x_i) = y] \right)^\delta \leqslant \left(q_f \sum_{i \in \{0,\delta-1\}} \max_{y \in \mathbb{F}_2^\ell} \Pr[h(x_i) = y] \right)^\delta \leqslant \\
&\leqslant \left(\delta q_f \max_{y \in \mathbb{F}_2^\ell} \Pr[h(x) = y] \right)^\delta.
\end{aligned}$$

Обозначим $p_h = \max_{y \in \mathbb{F}_2^\ell} \Pr[h(x) = y]$. Тогда существует алгоритм поиска коллизии хэш-функции h, имеющий сложность $T' = \frac{2\tilde{c}}{p_h}$, где $\tilde{c}$ — это константа,

зависящая от модели вычислений и соответствующая сложности однократного вычисления значения хэш-функции. Тогда для оптимального алгоритма T_{Coll}, решающего задачу $\mathsf{Coll}(h)$, справедливо

$$T_{\mathsf{Coll}} \leqslant T' \quad \text{и} \quad p_h \leqslant \frac{2\tilde{c}}{T_{\mathsf{Coll}}}.$$

Наконец, получаем

$$p \leqslant \left(\frac{2\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}.$$

Обозначим $p_h = \max_{y \in \mathbb{F}_2^\ell} \Pr[h(x) = y]$. Тогда существует алгоритм $\mathcal{C}$, который находит коллизию хэш-функции следующим образом. Он выбирает t случайных входов x_i и вычисляет их хэш-значения. $\mathcal{C}$ останавливается после того, как нашел коллизию. Тогда событие «$\mathcal{C}$ проиграет» раскладывается на два несовместимых события: «не существует такого $x \in \{x_i\}_{i=1}^t$, что $h(x) = y$» и «существует лишь один такой x». Мы утверждаем, что алгоритм делает не более $\frac{14}{p_h}$ шагов и имеет вероятность успеха не менее $1 - \frac{1}{e}$.

Чтобы доказать этот факт, мы рассмотрим отдельно два случая: $p_h \leqslant 0.25$ и $p_h > 0.25$. В первом случае число шагов можно взять равным $t_1 := \frac{3}{p_h}$. Тогда

$$\Pr[\mathcal{C} \text{ проиграет}] = (1-p_h)^{t_1} + \sum_{i=1}^{t_1} p_h(1-p_h)^{t_1-1} = (1-p_h)^{t_1} + t_1 p_h (1-p_h)^{t_1-1} \leqslant$$
$$\leqslant e^{-3} + \frac{\frac{3}{p_h} \cdot p_h e^{-3}}{1-p_h} = e^{-3}\left(1 + \frac{3}{1-p_h}\right) \leqslant 5e^{-3} < e^{-1}.$$

Здесь мы пользовались тем, что $(1+w)^z \leqslant e^{wz}$ для $z > 0$.

Если $p_h > 0.25$, зафиксируем $t_2 := 14$ и

$$\Pr[\mathcal{C} \text{ проиграет}] = (1-p_h)^{t_2} + \sum_{i=1}^{t_2} p_h(1-p_h)^{t_2-1} = (1-p_h)^{t_2} + t_2 p_h (1-p_h)^{t_2-1} \leqslant$$
$$\leqslant 0.75^{t_2} + t_2 p_h \cdot 0.75^{t_2-1} = 0.75^{t_2-1}(0.75 + t_2 p_h) < 0.75^{t_2-1}(1+t_2) < e^{-1}.$$

Сложность алгоритма $\mathcal{C}$ в первом случае равна $\frac{3\tilde{c}}{p_h}$, а во втором — $14\tilde{c}$, где $\tilde{c}$ есть константа, зависящая от модели вычислений и соответствующая однократному вычислению хэш-функции. Поэтому сложность всего алгоритма может

быть оценена как $\check{T} = \frac{14\tilde{c}}{p_h}$. Отметим, что, если $p_h > 0$, то алгоритм находит коллизию с вероятностью, равной 1, поскольку $\Pr[\mathcal{C} \text{ проиграет}] \to 0$ при $t \to \infty$.

Тогда можно утверждать, что для сложности оптимального алгоритма T_{Coll} решения задачи $\mathsf{Coll}(h)$ с вероятностью не менее $1 - \frac{1}{e}$ верно, что

$$T_{\mathsf{Coll}} \leqslant \check{T} \quad \text{и} \quad p_h \leqslant \frac{14\tilde{c}}{T_{\mathsf{Coll}}}.$$

Наконец, получаем

$$p' \leqslant \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}.$$

Обозначим через G событие, заключающееся в том, что условие со строки 23 ни разу не выполнилось. Тогда из того, что случилось событие $\overline{G}$, следует, что условие было выполнено хотя бы единожды за q_f запросов $\mathcal{A}$. Если $m^i \| c^i$ есть строки, сформированные во время работы алгоритма генерации подписи, то

$$\begin{aligned}\Pr[\overline{G}] &= \Pr[m^1\|c^1 \in \Pi^{\mathrm{F}} \vee \ldots \vee m^{q_s}\|c^{q_s} \in \Pi^{\mathrm{F}}] \leqslant \Pr[c^1 \in \Pi_c^F \vee \ldots \vee c^{q_s} \in \Pi_c^F] = \\ &= 1 - \Pr[c^1 \notin \Pi_c^F \wedge \ldots \wedge c^{q_s} \notin \Pi_c^F] = 1 - \prod_{i=1}^{q_s} \Pr[c^i \notin \Pi_c^F] = \\ &= 1 - \prod_{i=1}^{q_s}(1 - \Pr[c^i \in \Pi_c^F]) = 1 - (1-p')^{q_s}.\end{aligned}$$

Тогда используя неравенство Бернулли при $p' \leqslant 1, q_s > 0$, получим

$$\Pr[\overline{G}] \leqslant 1 - 1 + q_s p' \leqslant q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{Coll}}\right)^{\delta}.$$

Поскольку

$$\begin{aligned}\Pr[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1] &= \Pr[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1 \wedge G] + \Pr[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1 \wedge \overline{G}] \leqslant \\ &\leqslant \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1] + \Pr[\overline{G}],\end{aligned}$$

то

$$\Pr[\mathbf{Exp}^1(\mathcal{A}) \Rightarrow 1] - \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1] \leqslant \Pr[\overline{G}] = q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{Coll}}\right)^{\delta}.$$

Теперь на основе нарушителя $\mathcal{A}$ построим нарушителя $\mathcal{B}$, который строит экзистенциальную подделку подписи в модели EUF-NMA. Он симулирует оракулы F и Sign, используя алгоритмы SimF и SimSign. Алгоритм SimSign повторяет алгоритм Sign из эксперимента $\mathbf{Exp}^2$. Оракул F^* является случайным оракулом $\mathcal{B}$.

$\mathcal{B}^{\mathrm{F}^*}(y)$

1 : $\mathcal{L} \leftarrow \varnothing$
2 : $\Pi^{\mathrm{F}} \leftarrow \varnothing$
3 : $(m, c\|r) \leftarrow\!\!\$\ \mathcal{A}^{\mathrm{SimSign},\mathrm{SimF}}(y)$
4 : **if** $m \in \mathcal{L}$: **return** 0
5 : **return** $(m, c\|r)$

Oracle $\mathrm{SimF}(\alpha)$

1 : $\beta \leftarrow \mathrm{F}^*(\alpha)$
2 : $\Pi^{\mathrm{F}} \leftarrow \Pi^{\mathrm{F}} \cup \{(\alpha, \beta)\}$
3 : **return** β

Теперь обозначим через $\mathrm{Out}(\mathcal{A})$ и $\mathrm{Out}(\mathcal{B})$ пары $(m, c\|r)$, которые выдают нарушитель $\mathcal{A}$ в эксперименте $\mathbf{Exp}^2$ и нарушитель $\mathcal{B}$ в эксперименте EUF-NMA, соответственно. $\mathrm{Out}(\mathcal{A})_{m,c}$ и $\mathrm{Out}(\mathcal{B})_{m,c}$ есть проекции выходов нарушителей на $m\|c$. Отметим, что проекция не определена в случае, когда нарушитель $\mathcal{B}$ возвращает 0 (при $m \in \mathcal{L}$). Но далее будем рассматривать только те эксперименты, выход которых равен 1, что исключает этот случай.

Также определим

$$\mathrm{V}(F, m, c, r) := \mathsf{Ver}(y, m, c\|r),$$

где Ver — это алгоритм проверки подписи, использующий функцию F. Также для $m \in \mathbb{F}_2^*, c \in \mathbb{F}_2^{3\delta\ell}$ определим

$$p_{m,c} := \Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1 \wedge \mathrm{Out}(\mathcal{B})_{m,c} = m\|c] =$$

$$= \Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1 \wedge \mathrm{Out}(\mathcal{B})_{m,c} = m\|c \wedge m\|c \in \Pi^{\mathrm{F}}] +$$
$$+ \Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1 \wedge \mathrm{Out}(\mathcal{B})_{m,c} = m\|c \wedge m\|c \notin \Pi^{\mathrm{F}}].$$

Если $m\|c \notin \Pi^{\mathrm{F}}$, то нарушитель не знает истинного хэш-значения для этой строки, и ему приходится угадывать его. Это возможно сделать с вероятностью

равной $3^{-\delta}$. Также отметим, что результат эксперимента EUF-NMA равен результату работы алгоритма проверки подписи, поэтому верно, что

$$\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) = \text{V}(\text{F}, m, c, r). \tag{4.3}$$

Отсюда

$$p_{m,c} = \Pr[\text{V}(\text{F}, m, c, r) \wedge \text{Out}(\mathcal{B})_{m,c} = m\|c \wedge m\|c \in \Pi^{\text{F}}] + 3^{-\delta}.$$

Для строки $m\|c \in \Pi^{\text{F}}$ выполнено

$$\text{V}(\text{F}^*, m, c, r) = \text{V}(\text{F}, m, c, r),$$

поскольку оракул хэширования F нарушителя $\mathcal{A}$ строго задан оракулом F^* нарушителя $\mathcal{B}$. Тогда

$$p_{m,c} = \Pr[\text{V}(\text{F}^*, m, c, r) \wedge \text{Out}(\mathcal{B})_{m,c} = m\|c \wedge m\|c \in \Pi^{\text{F}}] + 3^{-\delta}.$$

Аналогично тому, как было доказано равенство (4.3), можно показать, что

$$\mathbf{Exp}^2(\mathcal{A}) = \text{V}(\text{F}^*, m, c, r).$$

Противник $\mathcal{B}$ всегда возвращает выход $\mathcal{A}$, поэтому

$$\text{Out}(\mathcal{B})_{m,c} = \text{Out}(\mathcal{A})_{m,c}.$$

Наконец стратегия $\mathcal{A}$ в случае, когда $m\|c \notin \Pi^{\text{F}}$, совпадает со стратегией $\mathcal{B}$ и, следовательно, имеет ту же вероятность успеха, равную $3^{-\delta}$.

Из приведенных аргументов получаем, что

$$\begin{aligned} p_{m,c} &= \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1 \wedge \text{Out}(\mathcal{A})_{m,c} = m\|c \wedge m\|c \in \Pi^{\text{F}}] + \\ &+ \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1 \wedge \text{Out}(\mathcal{A})_{m,c} = m\|c \wedge m\|c \notin \Pi^{\text{F}}] = \\ &= \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1 \wedge \text{Out}(\mathcal{A})_{m,c} = m\|c]. \end{aligned}$$

Таким образом,

$$\Pr[\mathbf{Exp}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \Rightarrow 1] = \Pr[\mathbf{Exp}(\mathcal{B}) \Rightarrow 1 \wedge \bigvee_{(m,c)} \text{Out}(\mathcal{B})_{m,c} = m\|c] =$$

$$= \sum_{(m,c)} p_{m,c} = \sum_{(m,c)} \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1 \wedge \text{Out}(\mathcal{A})_{m,c} = m\|c] = \Pr[\mathbf{Exp}^2(\mathcal{A}) \Rightarrow 1].$$

Следовательно,

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \geqslant \mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) - q_s \cdot \left(\frac{2\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}.$$

Противник $\mathcal{B}$ запускает $\mathcal{A}$ и симулирует q_f запросов к оракулу F и q_s запросов к оракулу Sign. Отметим, что сложность оракула Sign не превосходит сложности оригинального алгоритма генерации подписи. Поэтому сложность $\mathcal{B}$ не превосходит $T + c''(q_f + q_s T^{Sig}_{\text{Stern}})$. □

Следствие 13. *Пусть $\mathcal{A}$ — нарушитель, решающий задачу* EUF-CMA *для подписи на основе схемы идентификации Штерна, делая не более q_f запросов к оракулу хэширования* F *и не более q_s запросов к оракулу генерации подписи* Sign. *Тогда*

$$\mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \max\left\{ 15q_f \cdot \sqrt[3]{\frac{\delta^2(T + \tilde{\tilde{c}}(2q_f + q_s T^{Sig}_{\text{Stern}}))}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \right.$$

$$\left. + \left(\frac{2}{3}\right)^{\delta} \cdot (1 + q_f) + q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}, \left(\frac{2}{3}\right)^{\delta} \cdot \left(1 + q_f\left(1 + 2\delta \cdot 1.1^{\delta}\right)\right) + q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta} \right\}, \tag{4.4}$$

где T^{Sig}_{Stern} — сложность алгоритма генерации подписи, T есть максимальная возможная сложность нарушителя $\mathcal{A}$, T_{SD} и T_{Coll} — сложности оптимальных алгоритмов, решающих задачи $\mathsf{SD}(H, y, \omega)$ и $\mathsf{Coll}(h)$ с вероятностями успеха не менее, чем $1 - \frac{1}{e}$, а $\tilde{c}$ и $\tilde{\tilde{c}}$ — константы, зависящие от модели вычислений.

Доказательство. Сложность $\hat{T}$ нарушителя в модели EUF-NMA с одним запросом к оракулу хэширования из Теорем 21–23 не превышает $T + \tilde{\tilde{c}}(2q_f +$

$q_s T^{Sig}_{\text{Stern}}$), где T — сложность нарушителя в модели EUF-CMA, а $\tilde{\tilde{c}} = \max\{c', c''\}$. Также для нарушителя $\mathcal{B}$, делающего не более q_f запросов к оракулу хэширования в модели EUF-NMA, справедливо, что

$$\mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) \leqslant \max\left\{ 15q_f \cdot \sqrt[3]{\frac{\delta^2 \hat{T}}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \left(\frac{2}{3}\right)^{\delta} \cdot (1 + q_f), \right.$$
$$\left. \left(\frac{2}{3}\right)^{\delta} \cdot \left(1 + q_f \left(1 + 2\delta \cdot 1.1^{\delta}\right)\right) \right\},$$

откуда

$$\mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \mathsf{Adv}^{\text{EUF-NMA}}_{\text{Stern}}(\mathcal{B}) + q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta} \leqslant$$

$$\leqslant \max\left\{ 15q_f \cdot \sqrt[3]{\frac{\delta^2 \hat{T}}{\min\{T_{\mathsf{SD}}, T_{\mathsf{Coll}}\}}} + \left(\frac{2}{3}\right)^{\delta} \cdot (1 + q_f) + q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}, \right.$$
$$\left. \left(\frac{2}{3}\right)^{\delta} \cdot \left(1 + q_f \left(1 + 2\delta \cdot 1.1^{\delta}\right)\right) + q_s \cdot \left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta} \right\}.$$

□

4.3. Выводы к четвертой главе

Подход к построению электронной подписи с применением преобразования Фиата–Шамира позволяет исключить из схемы функцию декодирования, что дает возможность выбирать коды общего вида без предъявления требования на существование эффективного алгоритма декодирования, которое было обязательным для схем типа CFS. Теперь схема не только избегает уязвимостей, порожденных особенностями кодов специального вида, но и сводится к NP-трудной задаче синдромного декодирования произвольного линейного кода.

Кроме того, за счет отсутствия требования на однозначность декодирования, в предложенной схеме возможно увеличение числа ошибок, вносимых в кодовое слово. Так, при выборе параметров, можно задать вес ошибки равным кодовому расстоянию d, а не классическому значению $\lfloor \frac{d-1}{2} \rfloor$. Такое значение

обеспечивает максимальную трудоемкость известных экспоненциальных алгоритмов типа ISD, решающих задачу синдромного декодирования.

Стоит отметить, что стойкость предложенной схемы подписи также сводится к задаче поиска коллизии хэш-функции h. Сложность этой задачи контролируется выбором функции. Однако, требование на использование криптографически стойкой хэш-функции явно или неявно предъявляется и к схемам типа CFS. Следовательно, по сравнению с ними предложенная схема не накладывает никаких дополнительных ограничений.

Результаты настоящей главы позволяют построить электронную подпись на основе протокола идентификации Штерна с требуемым уровнем криптографической стойкости через выбор параметров, дающих малое значение величины $\mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A})$. В частности, представленные результаты нашли практическое применение в Российской Федерации в процессе стандартизации электронной подписи под названием «Шиповник».

Заключение

К основными результатами диссертационной работы можно отнести следующее.

1. Описана структура всех подкодов кодов Рида–Маллера второго порядка, свойства которых являются причиной уязвимости соответствующих вариантов схемы подписи CFS. Такое описание, в частности, помогает построить подкод, дающий схему подписи, стойкую к известным атакам. Для кодов произвольного порядка выписаны оценки, задающие стойкие подкоды, и показано, что число таки кодов стремится к нулю с ростом параметра m, задающего код Рида–Маллера. Таким образом, при случайном выборе подкода кода Рида–Маллера почти невозможно построить стойкую схему подписи.

2. Для другого варианта схемы подписи CFS, в котором ключи строятся на основе квазициклических кодов, предложены алгоритмы, позволяющие эффективно генерировать ключевую пару. Известные ранее алгоритмы при решении этой задачи либо не использовали структуру кода, что сказывалось на их трудоемкости, либо, несмотря на специализацию, работали за экспоненциальное время.

3. При справедливости дополнительного условия в случае, когда ключи подписи CFS строятся на основе конструкции Сидельникова, получены соотношения, описывающие классы эквивалентности секретных ключей. Это же условие является необходимым для ряда известных атак и выполняется с вероятностью, близкой к единице. В совокупности это говорит о невозможности использования конструкции Сидельникова при случайном выборе экземпляров кодов. Поэтому в работе предложено несколько специальных классов секретных ключей, схемы на которых не подвержены известным атакам.

4. Наконец, предложен вариант построения схемы электронной подписи, которая лишена недостатков, связанных с особенностями базовых кодов. Синтез такой подписи состоит в применении преобразования Фиата–Шамира к протоколу идентификации Штерна. Стойкость построенной схемы обоснована и сведена к NP-трудной задаче декодирования случайного линейного кода.

Полученные в диссертации результаты могут быть применены при разработке новых подходов к проектированию криптографических схем с открытым ключом. Работа позволяет выбирать наиболее стойкие классы кодов для кодовых систем, исключая неперспективные варианты, а также способствует повышению эффективности и безопасности построения электронных подписей.

Эти результаты могут найти применение в различных областях, в частности:

1. при синтезе и анализе схем электронной подписи, построенных на основе кодов, исправляющих ошибки;

2. в учебном процессе студентов-математиков, проходящих обучение в рамках специализации «Математические и программные методы обеспечения информационной безопасности»;

3. в научных центрах, проводящих исследования в области защиты информации.

Список литературы

1. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. — 1997. — Т. 26, № 5. — С. 1484—1509.
2. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance / L. M. K. Vandersypen [и др.] // Nature. — 2001. — Т. 414. — С. 883—887.
3. *Grover L. K.* A fast quantum mechanical algorithm for database search // Proc. 28th Annual ACM Symposium on the Theory of Computation. — 1996. — С. 212—219.
4. *Castryck W., Decru T.* An efficient key recovery attack on sidh (preliminary version) // IACR Cryptology ePrint Archive. — 2022. — С. 15.
5. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // The Deep Space Network Progress Report. — 1978. — Т. 42, № 44. — С. 114—116.
6. *NIST.* Calls for proposals. — 2017. — URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.
7. *Moody D.* Status report on the first round of the NIST post-quantum cryptography standardization process // NIST report. — 2019. — С. 1—27.
8. Post quantum signature scheme based on modified Reed-Muller code pqsigRM / W. Lee [и др.] // NIST proposal. — 2017. — С. 1—35.
9. Supporting documentation of RaCoSS (Random Code-based Signature Scheme) / P. S. Roy [и др.] // NIST proposal. — 2017. — С. 1—26.
10. Ranksign — a signature proposal for the NIST's call / N. Aragon [и др.] // NIST proposal. — 2017. — С. 1—22.

11. A modified pqsigRM: RM code-based signature scheme / Y.-W. Lee [и др.] // IACR Cryptology ePrint Archive. — 2018. — С. 18.

12. Codes and Restricted Objects Signature Scheme (CROSS) / M. Baldi [и др.] // NIST proposal. — 2023. — С. 1—59.

13. Enhanced pqsigRM: code-based digital signature scheme with short signature and fast verification for post-quantum cryptography : тех. отч. / J. Cho [и др.]. — 2023. — С. 1—28.

14. FuLeeca / S. Ritterhoff [и др.] // NIST proposal. — 2023. — С. 1—29.

15. LESS: Linear Equivalence Signature Scheme / M. Baldi [и др.] // NIST proposal. — 2023. — С. 1—37.

16. Matrix Equivalence Digital Signature (MEDS) / T. Chou [и др.] // NIST proposal. — 2023. — С. 1—29.

17. Wave / G. Banegas [и др.] // NIST proposal. — 2017. — С. 1—51.

18. Технический комитет 26 по стандартизации «Криптографическая защита информации». — URL: https://tc26.ru.

19. Report on evaluation of KpqC Round-2 candidates / D. J. Bernstein [и др.] // IACR Cryptology ePrint Archive. — 2024. — December.

20. *PQCRYPTO*. Post-quantum cryptography for long-term. — URL: https://web.archive.org/web/20250210182614/https://www.iso.org/organization/5984715.html (дата обр. 10.02.2025).

21. *IETF*. Post-Quantum Cryptography. — URL: https://web.archive.org/web/20250422202535/https://wiki.ietf.org/group/sec/PQCAgility (дата обр. 22.04.2025).

22. *Stern J.* Can one design a signature scheme based on error-correcting codes? // Lecture Notes in Computer Science. — 1995. — Т. 917. — С. 424—426.

23. *Kabatianskii G., Krouk E., Smeets B.* A digital signature scheme based on random error-correcting codes // Crytography and Coding. Cryptography and Coding 1997. Lecture Notes in Computer Science. — 1997. — Т. 1355. — С. 161—167.

24. *Cayrel P.-L., Otmani A., Vergnaud D.* On Kabatianskii–Krouk–Smeets signatures // Arithmetic of Finite Fields. WAIFI 2007. Lecture Notes in Computer Science. Т. 4547. — 2007. — С. 237—252.

25. *Courtois N., Finiasz M., Sendrier N.* How to achieve a McEliece-based digital signature scheme // Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science. Т. 2248. — 2001. — С. 157—174.

26. *Dallot L.* Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme // Research in Cryptology. WEWoRC 2007. Lecture Notes in Computer Science. Т. 4945. — 2008. — С. 65—77.

27. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. — 1986. — Т. 15, № 2. — С. 159—166.

28. *Berlekamp E. R., McEliece R. J., Tilborg H. C. A. van.* On the inherent intractability of certain coding problems // IEEE Transactions on Information Theory. — 1978. — Т. 24, № 3. — С. 384—386.

29. *Barg S.* Some new NP-complete coding problems // Probl. Peredachi Inf. — 1994. — Т. 30, № 3. — С. 23—28.

30. *Гоппа В. Д.* Новый класс линейных корректирующих кодов // Пробл. передачи информ. — 1970. — Т. 6, № 3. — С. 24—30.

31. *Bogdanov A., Lee C. H.* Homomorphic encryption from codes // arXiv. — 2011. — С. 18.

32. *Minder L.*, *Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS (Advances in Cryptology — EUROCRYPT 2007). — 2007. — Т. 4515. — С. 347—360.

33. *Бородин М. А.*, *Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера // Дискретная Математика. — 2014. — Т. 26, № 1. — С. 10—20.

34. *Сидельников В. М.*, *Шестаков С. О.* О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона // Дискрет. матем. — 1992. — Т. 4, № 3. — С. 57—63.

35. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes / A. Couvreur [и др.] // Designs, Codes and Cryptography. — 2014. — Т. 73, № 2. — С. 641—666.

36. *Couvreur A.*, *Márquez-Corbella I.*, *Pellikaan R.* Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes // Coding Theory Appl.ications. CIM Ser. Math. Sci. — 2015. — Т. 3. — С. 133—140.

37. *Чижов И. В.*, *Бородин М. А.* Классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера // Дискретная Математика. — 2020. — Т. 32, № 1. — С. 115—134.

38. *Чижов И.* Полная классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера // Вестн. Моск. Ун-та. — 2024. — Т. 15, № 1. — С. 57—70.

39. *Couvreur A.*, *Otmani A.*, *Tillich J.-P.* Polynomial time attack on wild McEliece over quadratic extensions // IEEE Transactions on Information Theory. — 2017. — Т. 63, № 1. — С. 404—427.

40. *Wieschebrink C.* An attack on a modified niederreiter encryption scheme // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial

Intelligence and Lecture Notes in Bioinformatics). — 2006. — Т. 3958. — С. 14—26.

41. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). — 2010. — Т. 6061. — С. 61—72.

42. *Berger T. P.*, *Loidreau P.* How to mask the structure of codes for a cryptographic use // Designs, Codes, and Cryptography. — 2005. — Т. 35, № 1. — С. 63—79.

43. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида–Маллера // Дискрет. матем. — 1994. — Т. 6, № 2. — С. 3—20.

44. *Чижов И. В.*, *Конюхов С. А.*, *Давлетшина А. М.* Эффективная структурная атака на криптосистему Мак-Элиса–Сидельникова // International Journal of Open Information Technologies. — 2020. — Т. 8, № 7. — С. 1—10.

45. *Otmani A.*, *Kalachi H. T.* Square code attack on a modified Sidelnikov cryptosystem Lecture Notes in Computer Science. — 2015. — Т. 9084. — С. 173—183.

46. *Чижов И. В.*, *Попова Е. А.* Структурная атака на криптосистемы типа Мак-Элиса–Сидельникова, построенной на основе комбинирования случайных кодов с кодами Рида–Маллера // International Journal of Open Information Technologies. — 2020. — Т. 8, № 6. — С. 24—33.

47. *Чижов И. В.* Квадрат Адамара последовательно соединенных линейных кодов // Дискретная математика. — 2023. — Т. 3. — С. 100—124.

48. *Eaton E.*, *Parent A.* QC-MDPC KEM: a key encapsulation mechanism based on the QC-MDPC McEliece encryption scheme : тех. отч. — 2017. — С. 1—51.

49. LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes / M. Baldi [и др.] // NIST proposal. — 2017. — С. 1—22.

50. Cryptanalysis of LEDAcrypt / D. Apon [и др.] // Advances in Cryptology – CRYPTO 2020. CRYPTO 2020. Lecture Notes in Computer Science. — 2020. — Т. 12172. — С. 389—418.

51. Bike: Bit Flipping Key Encapsulation / N. Aragon [и др.] // NIST proposal. — 2017. — С. 1—74.

52. Hamming Quasi-Cyclic (HQC) / J.-C. Deneuville [и др.] // NIST proposal. — 2017. — С. 1—62.

53. Hamming Quasi-Cyclic (HQC) / C. A. Melchor [и др.] // NIST proposal. — 2019. — С. 1—47.

54. *Fiallo E. D.* A digital signature scheme mCFSQC-LDPC based on QC-LDPC codes // Mat. Vopr. Kriptogr. — 2021. — Т. 12, № 4. — С. 99—113.

55. LEDAcrypt: Low-dEnsity parity-check coDe-bAsed cryptographic systems / M. Baldi [и др.] // NIST proposal. — 2019. — С. 1—83.

56. *Fiat A.*, *Shamir A.* How to prove yourself: practical solutions to identification and signature problems // Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science. Т. 263. — 1987. — С. 186—194.

57. *Stern J.* A new identification scheme based on syndrome decoding // CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science. Т. 773. — 1994. — С. 13—21.

58. Commitments and efficient zero-knowledge proofs from learning parity with noise / A. Jain [и др.] // Lecture Notes in Computer Science. — 2012. — Т. 7658 LNCS. — С. 663—680.

59. *Cayrel P.-L.*, *Véron P.*, *el Yousfi Alaoui S. M.* A zero-knowledge identification scheme based on the q-ary syndrome decoding problem // Lecture Notes in Computer Science. — 2011. — Т. 6544 LNCS. — С. 171—186.

60. *Overbeck R.*, *Sendrier N.* Code-based cryptography. — 2009.

61. *Roy P. S.*, *Morozov K.*, *Fukushima K.* Evaluation of code-based signature schemes // IACR Cryptology ePrint Archive. — 2019. — С. 22.

62. Code-based identification and signature schemes in software / S. M. el Yousfi Alaoui [и др.] // Lecture Notes in Computer Science. — 2013. — Т. 8128 LNCS. — С. 122—136.

63. *Pointcheval D.*, *Stern J.* Security proofs for signature schemes // Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science. — 1996. — Т. 1070. — С. 387—398.

64. *Vysotskaya V.* Characteristics of Hadamard Square of Special Reed–Muller Subcodes // Prikladnaya Diskretnaya Matematika. — 2021. — Т. 53. — С. 75—88.

65. *Высоцкая В. В.*, *Высоцкий Л. И.* Обратимые матрицы над некоторыми факторкольцами: идентификация, построение и анализ // Дискретная математика. — 2021. — Т. 33, № 2. — С. 46—65.

66. *Высоцкая В. В.* О структурных особенностях пространства ключей криптосистемы Мак-Элиса–Сидельникова на обобщенных кодах Рида–Соломона // Дискретная математика. — 2024. — Т. 36, № 4. — С. 28—43.

67. *Vysotskaya V.*, *Chizhov I.* The security of the code-based signature scheme based on the Stern identification protocol // Prikladnaya Diskretnaya Matematika. — 2022. — Т. 57. — С. 67—90.

68. *Vysotskaya V.* New estimates for dimension of Reed–Muller subcodes with maximum Hadamard square // Прикладная дискретная математика. Приложение. — 2020. — № 13. — С. 98—100.

69. *Deundyak V. M.*, *Kosolapov Y. V.* On the strength of asymmetric code cryptosystem based on the merging of generating matrices of linear codes // 16th International Symposium "Problems of Redundancy in Information and Control Systems REDUN 2019. — 2019. — С. 143—148.

70. *Чижов И. В.* Ключевое пространство криптосистемы Мак-Элиса–Сидельникова // Дискрет. матем. — 2009. — Т. 21. — С. 132—159.

71. *MacWilliams F. J., Sloane N. J. A.* The theory of error-correcting codes. — 1977. — С. 744.

72. *Both L., May A.* Decoding linear codes with high error rate and its impact for LPN security // Post-Quantum Cryptography. PQCrypto 2018. LNCS. — 2018. — Т. 10786. — С. 25—46.

73. *Petrank E., Roth R. M.* Is code equivalence easy to decide? // IEEE Transactions on Information Theory. — 1997. — Т. 43, № 5. — С. 1602—1604.

74. LEDAkem: a post-quantum Key Encapsulation Mechanism based on QC-LDPC codes / M. Baldi [и др.] // Post-Quantum Cryptography. PQCrypto 2018. Lecture Notes in Computer Science. — 2018. — Т. 10786. — С. 3—24.

75. *Erdös P., Spencer J.* Probabilistic methods in combinatorics. — 1974. — С. 106.

76. *Rödl V.* On a packing and covering problem // European Journal of Combinatorics. — 1985. — Т. 6, № 1. — С. 69—78.

77. *Storjohann A.* Algorithms for matrix canonical forms. — 2000. — С. 100.

78. *Gall F. le.* Powers of tensors and fast matrix multiplication // Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC. — 2014. — С. 296—303.

79. *Borissov Y., Lee M. H., Nikova S.* Asymptotic behavior of the ratio between the numbers of binary primitive and irreducible // IACR Cryptology ePrint Archive. — 2007. — С. 9.

80. *Lidl R., Niederreiter H.* Finite fields. — 1996. — С. 755.

81. *Тыртышников Е. Е.* Методы численного анализа. — 2007. — С. 320.

82. *Aho A. V., Hopcroft J. E., Ullman J. D.* The design and analysis of computer algorithms. — 1974.

83. *Grinstead C. M., Snell J. L.* Introduction to probability. — 1997. — С. 510.

84. *Чижов И. В.* Число открытых ключей криптосистемы Мак-Элиса–Сидельникова // Вестн. Моск. Ун-та. — 2009. — Т. 15, № 3. — С. 40—46.

Приложение А

Программная реализация Алгоритма 1

```
import copy
import collections

def bin(x,y):
  res = 1
  for i in range(y):
    res *= (x-i)*1.0/(i+1)
  return res

class fs(frozenset):
  def __str__(self):
    return "<{0}>".format(", ".join(str(x) for x in self))
  def __repr__(self):
    return str(self)

def find_min_deg(vert, v_old, ban, ban_set, edge):
  N = len(vert)
  first = True
  for i in range(N):
    if (i in ban) or (edge.union({i}) in ban_set):
      continue
    if first:
      res = i
      first = False
    elif len(vert[i]) < len(vert[res]):
      res = i
    elif len(vert[i]) == len(vert[res]):
      if len(v_old[i]) < len(v_old[res]):
        res = i
  return res

def form_ban(ban_set, count, edge, r, n):
  if r == 0:
    return
  for v in edge:
```

```
36      tmp = edge - {v}
37      count[tmp] += 1
38      if count[tmp] == n-r+1:
39        ban_set.add(tmp)
40        form_ban(ban_set, count, edge-{v}, r-1, n)
41
42  def new_edge(v_old, r, edges, ban_set):
43    ban = set()
44    vert = copy.deepcopy(v_old)
45    N = len(vert)
46    edge = set()
47    inter = set()
48    for i in range(r-1):
49      inter_local = set()
50      to_add = find_min_deg(vert, v_old, ban, ban_set, edge)
51      edge.add(to_add)
52      ban.add(to_add)
53      inter = inter.union(vert[to_add])
54      for edge_to_rem in vert[to_add]:
55        for v in edge_to_rem:
56          if v != to_add:
57            vert[v].remove(edge_to_rem)
58    L = len(edges)
59    for i in range(L):
60      if edge.issubset(edges[i]):
61        ban.add(list(edges[i]-edge)[0])
62    to_add = find_min_deg(vert, v_old, ban, ban_set, edge)
63    edge.add(to_add)
64    inter = inter.union(vert[to_add])
65    return (fs(edge), inter)
66
67  def main(r,n):
68    stop = bin(n,2*r)
69    vert = [set() for i in range(n)]
70    edges = []
71    set_num = 0
72    inter = set()
73    inter_num = 0
74    edge_inter_parts = set()
75    part_to_main = dict()
```

```
76  count = collections.defaultdict(int)
77  ban_set = set()
78  rep_num = 0
79
80  while set_num - rep_num - inter_num < stop:
81    local_rep = set()
82    (edge, inter) = new_edge(vert,r,edges, ban_set)
83    form_ban(ban_set, count, edge, r, n)
84    edges.append(edge)
85    for i in edge:
86      vert[i].add(edge)
87    for e in inter:
88      to_add = fs(edge.intersection(e))
89      edge_inter_parts.add(to_add)
90      part_to_main[to_add] = e
91    for e in edge_inter_parts:
92      inter_add = edge - e
93      if inter_add in edge_inter_parts:
94        tmp1 = part_to_main[inter_add] - inter_add
95        tmp = (part_to_main[e] - edge).union(tmp1)
96        if tmp in edges:
97          local_rep.add(tmp)
98    rep_num += len(local_rep)
99    set_num = bin(len(edges),2)
100   inter_num += len(inter)
101 print(edges)
```