На правах рукописи

Лелюк Евгений Андреевич

СИНТЕЗ ПОСТКВАНТОВОЙ СХЕМЫ ИНКАПСУЛЯЦИИ СЕАНСОВОГО КЛЮЧА

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

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

Ростов-на-Дону – 2025

Работа выполнена в ФГАОУ ВО «Южный федеральный университет» на кафедре алгебры и дискретной математики Института математики, механики и компьютерных наук им. И.И. Воровича.

Научный руководитель: **Косолапов Юрий Владимирович,** кандидат технических наук

Официальные оппоненты: **Беззатеев Сергей Валентинович,** доктор технических наук, доцент, ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», г. Санкт-Петербург, заведующий кафедрой «Информационная безопасность»

Малыгина Екатерина Сергеевна, кандидат физико-математических наук, ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики», г. Москва, доцент департамента «Прикладная математика»

Защита состоится «26» декабря 2025 г. в 14:00 на заседании диссертационного совета ЮФУ801.02.10 Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» по адресу: Ростовская обл., г. Таганрог, ул. Шевченко, 2, «Точка кипения» ИТА ЮФУ.

С диссертацией можно ознакомиться в Зональной научной библиотеке им. Ю.А. Жданова Южного федерального университета по адресу: г. Ростов-на-Дону, ул. Зорге, 21 Ж и на сайте: https://hub.sfedu.ru/diss/show/1346732.

Отзыв в 2-х экз. *(с указанием ФИО (полностью), ученой степени со специальностью, звания, организации, подразделения, должности, адреса, телефона, e-mail, даты)* с заверенной подписью рецензента и печатью учреждения просим направлять ученому секретарю диссертационного совета ЮФУ801.02.10 по адресу: 347922, Ростовская обл., г. Таганрог, пер. Некрасовский, 44, к. 302, а также в формате pdf – на e-mail: uaishukova@sfedu.ru.

Автореферат разослан «___» ноября 2025 г.

Ученый секретарь
диссертационного совета
ЮФУ801.02.10,
кандидат технических наук, доцент Ищукова Е.А.

Общая характеристика работы

Актуальность темы исследования. Стойкость применяемых в настоящее время на практике асимметричных криптосистем основана на сложности задач факторизации целых чисел или дискретного логарифмирования в конечной группе. Однако показано[1], что эти задачи могут быть решены за полиномиальное время на квантовом компьютере. Актуальной задачей криптографии в настоящее время является разработка криптосистем, стойких к атакам с использованием квантовых вычислений. Об этом свидетельствует проведение таких конкурсов, как NIST PQC (США), KpqC Competition (Южная Корея), а также работа рабочей группы ТК26 (Российская Федерация) по синтезу новой схемы инкапсуляции сеансового ключа, которая была бы стойкой против нарушителя, имеющего доступ к квантовому компьютеру достаточной мощности. Криптографические системы, в основе которых лежит применение помехоустойчивых кодов (далее – кодовые криптосистемы), рассматриваются как одна из альтернатив используемым в настоящее время асимметричным криптографическим системам.

Степень разработанности темы. Первой кодовой считается криптосистема, предложенная Робертом Мак–Элисом в 1978 году, в основе которой лежит использование кодов Гоппы. Для удобства далее эта система называется Original McEliece. На этой системе основан протокол инкапсуляции сеансового ключа NTS-KEM, участвовавший в конкурсе NIST PQC. Впоследствии этот проект был объединен с проектом Classic McEliece, входящим в число финалистов NIST PQC. Система Classic McEliece также основана на кодах Гоппы. Ее отличие от Original McEliece в том, что в Classic McEliece используется схема шифрования Нидеррайтера. Стойкость обеих систем, в частности, основана на сложности задачи декодирования случайного кода. Для этой задачи на текущий момент не найдено эффективного решения в модели квантовых вычислений.

Системы Original McEliece и Classic McEliece обладают своими достоинствами и недостатками. Первая, например, позволяет без дополнительных преобразований реализовать рандомизированное шифрование, а вторая обладает меньшим размером открытого ключа при сопоставимой стойкости. Тем не менее размер открытого ключа является недостатком систем на кодах Гоппы. Попытки использовать коды Рида–Соломона, коды Рида–Маллера, алгебро–геометрические коды, коды с низкой плотностью проверок на четность для уменьшения ключа не увенчались успехом, поскольку были найдены эффективные атаки на ключ (структурные атаки)

[1]Shor P. W. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press. 1994. P. 124-134.

для соответствующих криптосистем. Отметим, что коды Гоппы принадлежат классу альтернантных кодов. На текущий момент для некоторых классов кодов Гоппы также найдены структурные атаки на соответствующие криптосистемы. Кроме того, была найдена эффективная атака для одного класса подпространственных подкодов кодов Рида–Соломона, которые также являются альтернантными. Эти результаты не исключают появления в будущем эффективных структурных атак на кодовые криптосистемы и на других классах кодов Гоппы. Поэтому, несмотря на имеющиеся стойкие схемы, актуальна задача поиска других эффективно декодируемых помехоустойчивых кодов, обеспечивающих высокую стойкость кодовых криптосистем типа Мак–Элиса при небольшом размере открытого ключа.

Одним из способов получения новых кодов является применение кодовых конструкций. Однако отметим, что применение таких кодовых конструкций на основе известных кодов (базовых кодов), как соединение кодов, прямая сумма кодов, переход от расширений полей к базовым полям, также не позволили повысить стойкость. Тем не менее кодовые конструкции являются перспективными, поскольку позволяют на основе известных кодов строить новые эффективно декодируемые коды. Важным примером кодовой конструкции является тензорное произведение кодов, так как она находит широкое применение в системах защиты данных от помех. В общем случае новые коды принадлежат классу, отличному от класса базовых кодов, т.е. имеют иную структуру (алгебраическую и/или комбинаторную), поэтому структурные атаки на криптосистемы на основе базовых кодов неприменимы непосредственным образом к криптосистемам на новых кодах. Отметим, что многие структурные атаки основаны на использовании произведения Шура–Адамара, поэтому важной считается оценка стойкости криптосистем на основе новых конструкций к такого рода атакам[2].

Целью диссертационного исследования является повышение диверсификации эффективных постквантовых схем инкапсуляции сеансового ключа.

Научная задача, решение которой содержится в работе – разработка, теоретическое обоснование и исследование постквантовых кодовых схем шифрования, основанных на кодовых конструкциях, которые позволяют реализовать механизм инкапсуляции сеансового ключа, стойкий к атакам с использованием квантового компьютера.

Для достижения поставленной цели в диссертации решаются следующие **задачи**:

[2]Chizhov I.V. A Hadamard Product of Linear Codes: Algebraic Properties and Algorithms for Calculating It. MoscowUniv.Comput.Math.Cybern. 2023. Vol. 47, no. 4. P. 239-250.

1. Исследовать основанный на замене помехоустойчивого кода в схеме Мак–Элиса способ построения асимметричных кодовых криптосистем для инкапсуляции сеансового ключа, способы анализа стойкости этих систем к атакам на ключ и шифрограмму, а также свойства и характеристики кодов, влияющие на эту стойкость.
2. Исследовать способы построения новых кодов, основанные на комбинировании известных кодов. Выбрать перспективную для использования в схеме Мак–Элиса кодовую конструкцию. Описать криптографические свойства и характеристики выбранных кодов, в том числе свойства произведения Шура–Адамара.
3. Разработать алгоритмы гарантированного и вероятностного декодирования выбранных кодов с целью применения в схеме Мак–Элиса.
4. Разработать асимметричную криптосистему типа Мак–Элиса на выбранных кодах и провести анализ стойкости этой системы к атакам на ключ и шифрограмму. Описать параметры построенной криптосистемы, обеспечивающие ее эффективность.

Объект исследования. Объектом исследования являются постквантовые схемы инкапсуляции сеансового ключа для защиты конфиденциальности данных.

Предмет исследования. Предметом исследования являются методы построения эффективных кодовых криптосистем типа Мак–Элиса.

Методология и методы исследования. В диссертационной работе для теоретического исследования были использованы методы дискретной математики, теории кодирования, теории вероятностей, комбинаторного анализа, теории графов, анализа стойкости криптографических схем. Для экспериментального исследования использовались методы процедурного и объектно–ориентированного программирования.

Основные положения, выносимые на защиту:

1. Алгоритм шифрования и основанные на гарантированном и вероятностном декодировании алгоритмы расшифрования криптосистемы типа Мак–Элиса на конструкции D-кодов. Эти алгоритмы позволяют применять построенную криптосистему для решения задачи организации защищенного канала передачи данных с использованием схемы инкапсуляции сеансового ключа.
2. Алгоритм определения подмножеств сильных и слабых ключей криптосистемы Мак–Элиса на конструкции D-кодов на основе кодов Рида–Маллера, основанный на свойствах произведения Шура–Адамара этих кодов.
3. Алгоритм комбинированной атаки для слабых ключей криптосистемы типа Мак–Элиса на основе D-кодов, использующий структурную атаку для атаки на шифрограмму. Построенный алгоритм

позволяет повысить качество анализа комплексной стойкости кодовых криптосистем.

4. Параметры эффективных стойких криптосистем типа Мак–Элиса на D-кодах для применения в схеме инкапсуляции сеансового ключа. Найденные параметры, в частности, позволяют использовать предложенную схему в прикладных задачах, обеспечивая сопоставимые стойкость и размер открытого ключа с аналогичными схемами на кодах Гоппы в случае эфемерного использования сеансовых ключей.

Научная новизна диссертационной работы заключается в следующем:

1. Разработаны и программно реализованы алгоритмы шифрования и расшифрования криптосистемы типа Мак–Элиса на основе D-кодов. В частности, разработаны и реализованы алгоритмическая модель декодирования с гарантированным исправлением ошибок для D-кодов, **отличающаяся** применением мажоритарного подхода к декодированию, и алгоритмы вероятностного декодирования D-кодов на основе кодов Рида–Маллера, **отличающиеся** декодированием ошибок в количестве, превышающем половину кодового расстояния, и позволяющие за счет этого сократить размер открытого ключа. Построенные алгоритмы обеспечивают эффективное расшифрование в криптосистеме типа Мак–Элиса.
2. Разработан и программно реализован алгоритм определения множества сильных и слабых ключей криптосистемы на D-кодах на основе кодов Рида–Маллера, **отличающийся** использованием найденных криптографических свойств разложимости степеней Шура–Адамара D-кодов на основе кодов Рида–Маллера в прямую сумму кодов Рида–Маллера, и позволяющий эффективно находить параметры стойких систем на D-кодах.
3. Разработан алгоритм комбинированной атаки для слабых ключей криптосистемы типа Мак–Элиса на основе D-кодов, **отличающийся** применением структурной атаки с частичным восстановлением секретного ключа для увеличения вероятности успеха атаки на шифрограмму. Теоретически показано и экспериментально подтверждено, что разработанный алгоритм позволяет для слабых ключей криптосистемы значительно упростить атаку на шифрограмму относительно классической атаки декодированием по информационным совокупностям.
4. На основе разработанных подходов к декодированию D-кодов на кодах Рида–Маллера, исследованных криптографических свойств этих кодов и результатов анализа стойкости построена новая криптосистема типа Мак–Элиса, **отличающаяся** применением

конструкции D-кодов.

Теоретическая значимость. Теоретические результаты, полученные в данном исследовании, в частности, свойства произведения Шура–Адамара D-кодов и результаты анализа стойкости криптосистемы на этих кодах могут использоваться как при дальнейшем изучении криптосистем на D-кодах, например, для уточнения множеств сильных и слабых ключей построенной криптосистемы, так и при разработке новых кодовых криптосистем на основе подкодов прямой суммы кодов.

Практическая ценность. Построенная асимметричная кодовая криптосистема типа Мак–Элиса на D-кодах на основе кодов Рида–Маллера обладает либо большей стойкостью при сопоставимом размере ключа, либо меньшим размером ключа при сопоставимой стойкости, либо большей стойкостью при меньшем размере ключа по сравнению с системой Original McEliece. Это позволяет применять предложенную систему в схемах обеспечения конфиденциальности данных, например, для инкапсуляции сеансового ключа симметричной криптосистемы или для повышения защищенности данных, циркулирующих в информационных системах, за счет использования рандомизированного шифрования. Разработанный теоретико–графовый подход к декодированию D-кодов и, в частности, тензорного произведения кодов может применяться в задаче защиты от помех в каналах связи.

Соответствие диссертации паспорту научной специальности. Диссертация соответствует паспорту научной специальности 2.3.6. – «Методы и системы защиты информации, информационная безопасность» и охватывает следующие области исследования, входящие в эту специальность: «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов» (п. 19).

Достоверность полученных результатов подтверждается корректностью математических выкладок и доказательств теорем, а также экспериментальными исследованиями.

Внедрение результатов работы. Результаты диссертационного исследования, подтвержденные соответствующими актами, используются в:

1. Деятельности Автономной Некоммерческой Организации «Национальный Технологический Центр Цифровой Криптографии» (г. Москва) при выполнении научно-исследовательской работы «Формирование методики и автоматизированных инструментов выбора постквантовых механизмов, основанных на помехоустойчивом кодировании используемых при обеспечении информационной безопасности сетевого взаимодействия», шифр «Кульминация».
2. Деятельности ФГАНУ "Научно-исследовательский институт "Специализированные вычислительные устройства защиты и

автоматика" (г. Ростов-на-Дону) при решении задачи выработки общего сеансового ключа для организации защищенного канала передачи информации.

3. Учебно-исследовательском процессе на кафедре алгебры и дискретной математики Института математики, механики и компьютерных наук им. И.И. Воровича ЮФУ.

Апробация работы. Основные результаты работы были представлены на следующих конференциях и научных семинарах: семинар «Математические методы защиты информации» института математики, механики и компьютерных наук им. И. И. Воровича, Ростов-на-Дону, 2017 г.; III Всероссийский научный форум «Наука будущего – наука молодых», Нижний Новгород, 2017 г.; Научная конференция «Современные информационные технологии: тенденции и перспективы развития» (СИТО), Ростов-на-Дону, 2018, 2019 гг.; XX Международная конференция «Сибирская научная школа–семинар "Компьютерная безопасность и криптография" имени Геннадия Петровича Агибалова» (SibeCRYPT), Новосибирск, 2021 г.; XII Международный симпозиум «Современные тенденции в криптографии» (CTCrypt), Волгоград, 2023 г.; Всероссийский научный семинар «Кибербезопасность: теория и практика», НИЯУ МИФИ, Москва, 2024 г.

Публикации. Основные положения диссертации опубликованы в 9 научных печатных работах, в том числе: 3 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК (категории К1, RSCI), 2 – в научных рецензируемых журналах, индексируемых в базе Scopus (Q3, что соответствует категории ВАК К1), 4 – в материалах конференций и других изданиях. Получено свидетельство о государственной регистрации программы для ЭВМ.

Личный вклад заключается в выполнении основного объема теоретических и экспериментальных исследований, изложенных в диссертационной работе, включая исследование предметной области, формулировку и доказательство лемм и теорем, разработку методов и алгоритмов, входящих в число основных результатов работы, разработку методов и программных систем для проведения экспериментальных исследований, проведение экспериментов, анализ результатов теоретического и экспериментального исследования, оформление результатов в виде публикаций и научных докладов. Все выносимые на защиту результаты получены автором лично.

Объем и структура работы. Диссертация написана на русском языке, состоит из введения, трех глав, заключения, списка используемой литературы из 85 наименований и двух приложений. Полный объем диссертации составляет 156 страниц (в том числе приложений 7 стр.), включая 10 рисунков и 14 таблиц.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, излагается научная новизна и практическая значимость представляемой работы, декларируются положения, выносимые на защиту, область исследования и апробация полученных результатов.

В **первой главе** рассматриваются вопросы использования асимметричных криптосистем в протоколе инкапсуляции сеансового ключа, а также вопросы построения новых кодовых криптосистем для таких протоколов. Другими словами, рассматривается задача синтеза новой схемы инкапсуляции сеансового ключа, которая решается в последующих главах. Приводятся основные понятия теории кодирования, используемые в кодовой криптографии. Также в рамках задачи построения эффективных декодеров для применения в кодовой криптосистеме рассматривается концепция мажоритарного декодирования, на основе которой в следующей главе строится один из декодеров D-кодов: с гарантированным исправлением ошибок.

Асимметричные шифросистемы обычно не используются для защиты непосредственно пользовательских данных, но при этом являются основой многих криптографических протоколов, в частности, протоколов инкапсуляции сеансового ключа (KEM, key encapsulation mechanism). Целью протоколов KEM является передача от отправителя к получателю сеансового ключа $\mathbf{K} \in \{0,1\}^m$, например, симметричного шифра (где обычно $m \in \{128,192,256\}$), на котором выполняется шифрование пользовательских данных. Протокол KEM представляет собой тройку алгоритмов:

KeyGen: используется получателем информации для генерации открытого pk' и секретного sk' ключей, причем открытый передается отправителю;

Encaps: применяется отправителем для инкапсуляции с помощью открытого ключа pk' сеансового ключа $\mathbf{K}$ в последовательность битов $\mathbf{c}$; выходом алгоритма Encaps является пара ($\mathbf{K}$,$\mathbf{c}$), причем получателю передается $\mathbf{c}$;

Decaps: применяется получателем для извлечения (декапсуляции) сеансового ключа $\mathbf{K}$ из $\mathbf{c}$ с помощью секретного ключа sk'.

Обычно выделяют два типа стойкости протокола KEM: стойкие к атаке на основе подобранного открытого текста (IND-CPA, **ind**istinguishability under **c**hosen **p**laintext **a**ttack) и стойкие к атаке на основе подобранного шифртекста (IND-CCA1/2, **ind**istinguishability under **c**hosen **c**iphertext **a**ttack). IND-CPA-стойкости протокола KEM достаточно для эфемерной или одноразовой инкапсуляции, в то время как для многоразового использования KEM необходима IND-CCA-стойкость. При этом стойкость

$\lambda_{\mathsf{KEM}} \in \mathbb{N}$ механизма KEM может быть определена как отрицательный двоичный логарифм вероятности успеха наилучшей известной атаки на KEM.

Одним из вариантов реализации протоколов KEM в постквантовую эпоху является реализация на основе кодовых криптосистем. Приведем необходимые сведения из теории кодирования. Пусть $\mathbb{F}_q^n$ – векторное пространство над полем Галуа $\mathbb{F}_q$. Для вектора $\mathbf{x}(\in \mathbb{F}_q^n)$ множество его ненулевых координат называется *носителем* вектора $\mathbf{x}$ и обозначается $\mathrm{supp}(\mathbf{x})$. *Вес* $\mathrm{wt}(\mathbf{x})$ вектора $\mathbf{x}$ определяется как $|\mathrm{supp}(\mathbf{x})|$. (Здесь и далее символом $|A|$ обозначается мощность множества A.) Линейное подпространство C размерности k пространства $\mathbb{F}_q^n$ называется *линейным кодом*. Пусть $\dim(C) = k$ и $n(C) = n$ – размерность и длина кода соответственно, а $d(C) = \min_{\mathbf{c}\in C, \mathbf{c}\neq \mathbf{0}}\{\mathrm{wt}(\mathbf{c})\} = d$ – минимальное кодовое расстояние кода C, тогда код C называют $[n,k,d]_q$-кодом. Порождающую матрицу кода C обозначим G_C, то есть $C = \mathcal{L}(G_C)$. Здесь и далее через $\mathcal{L}(U)$ обозначается линейная оболочка множества U. Проверочную матрицу кода C обозначим H_C. Двойственный код к коду C обозначим для удобства $\overline{C}$, то есть $\overline{C} = \mathcal{L}(G_{\overline{C}}) = \mathcal{L}(H_C)$. Тензорное произведение $C_1 \otimes C_2$ двух $[n_i,k_i,d_i]_q$-кодов $C_i(\subset \mathbb{F}_q^{n_i})$, где $i \in \{1,2\}$, можно определить как $\mathcal{L}(G_{C_1} \otimes G_{C_2})$, где $G_{C_1} \otimes G_{C_2}$ – тензорное произведение матриц. Известно, что $C_1 \otimes C_2$ является $[n_1n_2, k_1k_2, d_1d_2]_q$-кодом.

Важными криптографическими свойствами линейных кодов являются свойства произведения Шура–Адамара и разложимости. В частности, эти свойства могут применяться в кодовой криптографии для построения различителя, который может использоваться для создания структурной атаки. Для двух векторов $\mathbf{a} = (a_1,...,a_n)$ и $\mathbf{b} = (b_1,...,b_n)$ из $\mathbb{F}_q^n$ *произведением Шура–Адамара* называется вектор $\mathbf{a} \star \mathbf{b} = (a_1b_1,...,a_nb_n)$. А произведением Шура–Адамара $k \times n$-матрицы $A = (\mathbf{a}_i)$ и $l \times n$-матрицы $B = (\mathbf{b}_j)$ называется матрица $A \star B = (\mathbf{a}_i \star \mathbf{b}_j)$, $i \in [\![1,k]\!]$, $j = [\![1,l]\!]$. Здесь и далее запись $[\![a,b]\!]$ означает диапазон целых чисел от a до b включительно. Для кодов C и D из $\mathbb{F}_q^n$ их произведение Шура–Адамара определяется следующим образом: $C \star D = \mathcal{L}(\{\mathbf{x} \star \mathbf{y} | \mathbf{x} \in C, \mathbf{y} \in D\})$. Известно, что $C \star D = \mathcal{L}(G_C \star G_D)$. Произведение $C \star C$ далее обозначается C^2 и называется *квадратом* кода C. $[n,k]_q$-код C называется *разложимым*, если для любой его порождающей матрицы G_C найдется такая невырожденная $(k \times k)$-матрица M и перестановочная $(n \times n)$-матрица Q, что $MG_CQ = \mathrm{diag}(A_1,...,A_r), \mathrm{rank}(A_i) \geqslant 1, r \geqslant 2$.

Напомним схему кодовой асимметричной криптосистемы, предложенную Робертом Мак–Элисом в 1978 году. Пусть $C \subseteq \mathbb{F}_q^n$ – линейный $[n,k,d]_q$-код, для которого известен эффективный декодер $\mathsf{Decoder} : \mathbb{F}_q^n \to C \cup \{\perp\}$, где $\perp$ – признак ошибочного декодирования. Секретным ключом схемы Мак–Элиса на коде C является пара $sk = (S,P)$, где невырожденная $(k \times k)$-матрица S и $(n \times n)$-матрица перестановки P выбираются случайно;

открытым ключом является пара $pk = (\tilde{G},t)$, где $t \in \mathbb{N}$ и

$$\tilde{G} = SG_CP. \tag{1}$$

В ряде случаев код C может быть секретным, тогда порождающая матрица G_C будет частью sk. Шифрование сообщения $\mathbf{m} \in \mathbb{F}_q^k$ выполняется по правилу: $\mathbf{c} = \mathbf{m}\tilde{G} + \mathbf{e}$, $\mathrm{wt}(\mathbf{e}) = t$. Для расшифрования, достаточно по кодовому слову $\mathsf{Decoder}(\mathbf{c}P^{-1}) = \mathbf{m}'\tilde{G}$ (в случае $\mathsf{Decoder}(\mathbf{c}P^{-1}) \neq \perp$) найти вектор $\mathbf{m}'$ и вычислить $\mathbf{m}'S^{-1} = \mathbf{m}$.

Важными характеристиками систем типа Мак–Элиса являются стойкость, размер открытого ключа $\tilde{G}$ (число байт для хранения матрицы $\tilde{G}$, далее pk_size) и время расшифрования. Под стойкостью $\lambda_{\mathsf{OW}} \in \mathbb{N}$ (**O**ne-**W**ay-стойкость или OW–стойкость) асимметричной схемы обычно понимают отрицательный двоичный логарифм вероятности успеха наилучшей атаки дешифрования шифртекста, полученного при шифровании случайно и равновероятно выбранного открытого текста. В случае, когда для криптосистемы типа Мак–Элиса неизвестны эффективные атаки на ключ, стойкость принято оценивать с помощью вероятности успешного декодирования по информационным совокупностям (далее – ДИС или ISD от английского **i**nformation **s**et **d**ecoding). В настоящей работе под OW–стойкостью λ_{OW} криптосистемы типа Мак–Элиса на $[n,k,d]_q$-коде здесь и далее понимается отрицательный двоичный логарифм вероятности успеха классического алгоритма ДИС, или иначе, логарифм сложности этого алгоритма: $\lambda_{\mathsf{OW}} = -\log_2\left(C_{n-t}^k/C_n^k\right)$.

Вторая глава посвящена исследованию D-кодов. Именно, приводится определение D-кодов и исследуются их криптографические свойства. В частности, находятся условия разложимости степеней Шура–Адамара D-кодов на основе кодов Рида–Маллера в прямую сумму неразложимых кодов. Для эффективного расшифрования в главе строятся алгоритмические модели гарантированного и вероятностных декодеров для D-кодов. В качестве гарантированного строится мажоритарный декодер, а в качестве вероятностных – декодеры, использующие блочную структуру кодового слова D-кода. Для вероятностных декодеров приводятся результаты экспериментов, демонстрирующих их эффективность.

Одним обобщением конструкции тензорного произведения является конструкция D-кода, впервые предложенная Касами и Лином[3]. Кратко определим эти коды. Пусть $C_1(k_i) \subseteq \mathbb{F}_q^{n_1}$, $k_i \geqslant 0$, $C_2(\ell_i) \subseteq \mathbb{F}_q^{n_2}$, $\ell_i \geqslant 0$, $i \in [\![1,s]\!]$; коды $C_1(k_i)$, $C_2(\ell_i)$ будем называть *базовыми*. Определим код

$$\overline{C(D)} = \sum_{i=1}^{s} \overline{C_1(k_i)} \otimes \overline{C_2(\ell_i)}. \tag{2}$$

[3]Kasami T., Lin S. On the Construction of a Class of Majority–Logic Decodable Codes. IEEE Transactions on Information Theory. 1971. Vol. IT-17, no. 5. P. 600-610

Если для $s \geqslant 2$ и $i < s$ во введенных обозначениях выполняется $\overline{C_1(k_i)} \subset \overline{C_1(k_{i+1})}$, $\overline{C_2(\ell_{i+1})} \subset \overline{C_2(\ell_i)}$, а также условия из [3], то $\overline{C(D)}$ является D-кодом и может быть декодирован. Отметим, что D является подмножеством множества пар целых неотрицательных чисел и определяет множество пар (k_i, ℓ_i) из (2).

В качестве базовых кодов далее рассматриваются бинарные $[n,k,d]_2$-коды Рида–Маллера $\mathrm{RM}_2(r,m)(\subset \mathbb{F}_2^n)$, где $r,m \in \mathbb{N}$, $r \leqslant m$, $n = 2^m$, $k = \sum_{i=0}^{r} {}^{i}_{n}$, $d = 2^{m-r}$. В [1] показано, что при определенном выборе множества D, D-код на основе кодов Рида–Маллера может быть кодом Рида–Маллера или его подкодом с тем же кодовым расстоянием.

Пусть $r^1_{k_i} = m_1 - k_i$, $r^2_{\ell_i} = m_2 - \ell_i$ – порядки кодов Рида–Маллера $C_1(k_i) = \mathrm{RM}_2(r^1_{k_i}, m_1)$ и $C_2(\ell_i) = \mathrm{RM}_2(r^2_{\ell_i}, m_2)$ соответственно, а

$$\overline{r}^1_{k_i} = m_1 - (m_1 - k_i) - 1 = k_i - 1, \overline{r}^2_{\ell_i} = m_2 - (m_2 - \ell_i) - 1 = \ell_i - 1 \qquad (3)$$

– порядки двойственных кодов $\overline{C_1(k_i)} = \mathrm{RM}_2(\overline{r}^1_{k_i}, m_1)$ и $\overline{C_2(\ell_i)} = \mathrm{RM}_2(\overline{r}^2_{\ell_i}, m_2)$ соответственно. В работе сформулированы и доказаны следующие теоремы, описывающие свойства произведения Шура–Адамара D-кодов на основе кодов Рида–Маллера.

Теорема 1. *Пусть $\overline{C(D)}$ вида (2), $\overline{r}^1_{k_i}, \overline{r}^2_{\ell_i}$ вида (3).*

1) Если $\overline{r}^1_{k_1} \geqslant m_1/2$ и $\overline{r}^2_{\ell_1} < m_2/2$, то $\overline{C(D)}^2 = \mathbb{F}_2^{n_1} \otimes \overline{C_2(\ell_1)}^2$.

2) Если $\overline{r}^1_{k_s} < m_1/2$ и $\overline{r}^2_{\ell_s} \geqslant m_2/2$, то $\overline{C(D)}^2 = \overline{C_1(k_s)}^2 \otimes \mathbb{F}_2^{n_2}$.

Теорема 2. *Пусть $\overline{C(D)}$ – код вида (2) и выполняется хотя бы одно из условий:*

1) существует $i \in [\![1,s]\!]$, что $\overline{r}^1_{k_i} \geqslant m_1/2$ и $\overline{r}^2_{\ell_i} \geqslant m_2/2$;

2) существуют $p \in [\![1,s]\!]$, $j \in [\![1,s]\!]$, $p \neq j$, что $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} \geqslant m_1$ и $\overline{r}^2_{\ell_p} + \overline{r}^2_{\ell_j} \geqslant m_2$.

Тогда $\overline{C(D)}^2 = \mathbb{F}_2^{n_1 n_2}$.

Теорема 3. *Пусть $\overline{C(D)}$ код вида (2) и выполняются условия $\overline{r}^1_{k_1} < m_1/2$, $\overline{r}^2_{\ell_1} \geqslant m_2/2$, и $\overline{r}^1_{k_j} \geqslant m_1/2$, $\overline{r}^2_{\ell_j} < m_2/2$ для любых $j \geqslant 2$. Если для любых $p \in [\![1,s]\!]$, $j \in [\![1,s]\!]$, $p \neq j$ выполняются неравенства $\overline{r}^1_{k_p} + \overline{r}^1_{k_j} \geqslant m_1$ и $\overline{r}^2_{\ell_p} + \overline{r}^2_{\ell_j} < m_2$, то $\overline{C(D)}^2 = \overline{\tilde{C}_1 \otimes \tilde{C}_2}$, $\overline{C(D)}^3 = \mathbb{F}_2^{n_1 n_2}$, где $\tilde{C}_1 = \overline{\overline{C_1(k_1)}^2}$, $\tilde{C}_2 = \overline{\overline{C_2(\ell_2)}^2 + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \overline{C_2(\ell_p)} \star \overline{C_2(\ell_j)}}$.*

Теорема 4. *Пусть $\overline{C(D)}$ код вида (2) и выполняются условия $\overline{r}^1_{k_j} < m_1/2$, $\overline{r}^2_{\ell_j} \geqslant m_2/2$ для любых $j < s$ и $\overline{r}^1_{k_s} \geqslant m_1/2$, $\overline{r}^2_{\ell_s} < m_2/2$. Если для любых $p \in [\![1,s]\!]$, $j \in [\![1,s]\!]$, $p \neq j$ выполняются неравенства*

$\overline{r}^1_{k_p} + \overline{r}^1_{k_j} < m_1\ u\ \overline{r}^2_{\ell_p} + \overline{r}^2_{\ell_j} \geqslant m_2,\ mo\ \overline{C(D)}^2 = \overline{\hat{C}_1 \otimes \hat{C}_2},\ \overline{C(D)}^3 = \mathbb{F}_2^{n_1 n_2},$
$\text{где } \hat{C}_1 = \overline{\overline{C_1(k_{s-1})}^2 + \sum_{\substack{p,j=1 \\ p \neq j}}^{s} \overline{C_1(k_p)} \star \overline{C_1(k_j)}},\ \hat{C}_2 = \overline{C_2(\ell_s)}^2.$

Далее для применения в схеме Мак–Элиса исследуется вопрос эффективного декодирования D-кодов. Как было сказано ранее, при использовании кодов Рида–Маллера в качестве базовых для D-кодов, D-код может быть кодом Рида–Маллера или его подкодом. В этом случае одним из способов декодирования является использование декодера кода Рида–Маллера. В общем же случае для линейных кодов существуют разные подходы к декодированию. Условно их можно разделить на гарантированное и вероятностное. В первом случае декодеры нацелены на гарантированное исправление любых векторов ошибок, имеющих вес в пределах половины кодового расстояния. Во втором случае декодеры нацелены на исправление большего количества ошибок, но обладают ненулевой вероятностью ошибочного декодирования (DFR, decoding failure rate).

В качестве гарантированного в работе строится мажоритарный декодер на основе подхода Мэсси[4]. Строится декодер на основе использования декодирующих деревьев для тензорного произведения двух кодов $C_1 \otimes C_2$, как частного случая D-кода. Соответствующая алгоритмическая модель реализована на языке C++. Также определяется конструкция декодирующего графа для базового кода, которая является улучшением конструкции декодирующего дерева. На основе декодирующего графа строится алгоритмическая модель декодирования D-кодов.

Далее решается задача построения вероятностного декодера для D-кодов на основе кодов Рида–Маллера. Построены два вероятностных декодера: декодер с использованием декодирования по информационным совокупностям (ДИС) (алгоритм ISDDecoder) и декодер на основе декодирования кодов–произведений, в которых кодовое слово может быть представлено в виде матрицы (алгоритм MatrixDecoder).

Поясним алгоритм ISDDecoder. Пусть $n_i = 2^{m_i}$, $i \in \{1,2\}$, C – $[n,k,d]_2$-код вида (2). Из представления (2) следует, что

$$C \subseteq \mathbb{F}_2^{n_1} \otimes \mathrm{RM}_2(\ell_1,m_2) = \underbrace{\mathrm{RM}_2(\ell_1,m_2) \times \cdots \times \mathrm{RM}_2(\ell_1,m_2)}_{n_1}. \qquad (4)$$

Следовательно, кодовое слово кода C представляет собой конкатенацию кодовых слов кода $\mathrm{RM}_2(\ell_1,m_2)$. Поэтому декодирование кода C может заключаться в применении некоторого известного декодера DecRow : $\{0,1\}^{2^{m_2}} \to \mathrm{RM}_2(\ell_1,m_2) \cup \{\perp\}$ кода $\mathrm{RM}_2(\ell_1,m_2)$ к каждому из n_1 блоков длины n_2 испорченного кодового слова $\mathbf{z} = \mathbf{z}_1 \parallel \cdots \parallel \mathbf{z}_{n_1}$. Для этого построен вспомогательный алгоритм BlockDecoder. Отметим, что в

[4]Massey J. L. Threshold Decoding. Cambridge:MIT Press. 1963.

качестве DecRow могут использоваться как гарантированные, так и вероятностные алгоритмы декодирования. При этом в обоих случаях алгоритм BlockDecoder может вернуть неправильный результат, то есть некоторое количество блоков $\mathbf{z}_i$ зашумленного кодового вектора $\mathbf{z}$ будут декодированы неправильно. Если блок был декодирован правильно, то назовем его *хорошим*, в противном случае – *плохим*. После выполнения алгоритма BlockDecoder применяется модифицированное ДИС, где осуществляется попытка выбора хороших блоков и составления из них информационной совокупности, по которой впоследствии восстанавливается исходное кодовое слово. Вероятность ошибочного декодирования DFR в случае $i \in \mathbb{N}$ итераций ДИС алгоритма ISDDecoder обозначим как $\mathrm{DFR}_1(i)$.

Поясним алгоритм MatrixDecoder. Из вида (2) следует, что $C \subseteq (\mathbb{F}_2^{n_1} \otimes \mathrm{RM}_2(\ell_1,m_2)) \cap (\mathrm{RM}_2(k_s,m_1) \otimes \mathbb{F}_2^{n_2}), n_i = 2^{m_i}, i \in \{1,2\}$. Следовательно, алгоритм декодирования испорченного кодового слова $\mathbf{z}$ кода C может быть основан на способе декодирования кодов–произведений: 1) представить $\mathbf{z}$ в виде $(n_1 \times n_2)$-матрицы, строки которой – испорченные кодовые слова кода $\mathrm{RM}_2(\ell_1,m_2)$, а столбцы – испорченные кодовые слова кода $\mathrm{RM}_2(k_s,m_1)$; 2) применить декодер DecRow по строкам, а затем к результату декодирования применить декодер DecCol по столбцам. Вероятность ошибочного декодирования для MatrixDecoder обозначим DFR_2.

Стоит отметить, что для обеспечения IND-CCA-стойкости необходимо, чтобы $\mathrm{DFR} \leqslant 2^{-\lambda_{\mathsf{KEM}}}$. А для IND-CPA-стойкости, то есть для одноразового использования ключей достаточно, чтобы $\mathrm{DFR} \leqslant 10^{-\gamma}$, где γ – параметр *отказоустойчивости* системы. При этом имеет смысл выбирать $\gamma \in \{5,6,...,9\}$[5,6].

В работе были проведены эксперименты по оценке работы декодеров ISDDecoder и MatrixDecoder. Для этого была выполнена программная реализация соответствующих алгоритмов на языке C++. В качестве DecRow в обоих алгоритмах используется декодер Йе–Аббе[7], как и DecCol в алгоритме MatrixDecoder. В таблице 1 представлены параметры D-кодов вида (2), выбранные для использования в криптосистеме типа Мак–Элиса. Эти коды получены следующим образом. В качестве $\mathrm{RM}_2(\ell_1, m_2)$ из вида (4) выбраны коды $\mathrm{RM}_2(2,7)$, $\mathrm{RM}_2(3,7)$, $\mathrm{RM}_2(2,8)$, $\mathrm{RM}_2(3,8)$, $\mathrm{RM}_2(2,9)$, обладающие высокой корректирующей способностью при использовании декодера Йе–Аббе. Для каждого из этих кодов найдены такие D-коды, что

[5]Campagna M., Crockett E. Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS). Internet-Draft: draft-campagna-tls-bike-sike-hybrid-07. Internet Engineering Task Force. 2021

[6]Drucker N., Gueron S., Kostic D. A lean BIKE KEM design for ephemeral key agreement. 2024. URL: https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/a-lean-bike-kem.pdf (дата обращения: 07.02.2025)

[7]Ye M., Abbe E. Recursive projection-aggregation decoding of Reed-Muller codes. IEEE Transactions on Information Theory. 2020. Vol. 66, no. 8. P.4948-4965

соответствующие им криптосистемы, во-первых, являются стойкими к комбинированной атаке, о которой пойдет речь в третьей главе, а во-вторых, стойкость λ_{OW} к классической атаке декодированием по информационным совокупностям находится в пределах стойкости системы Original McEliece. При этом в таблице 1 приводится номер кода D-кода, его обозначение вида:

$$[(r_1^1, r_1^2), (r_2^1, r_2^2), ...] = \mathrm{RM}_2(r_1^1, m_1) \otimes \mathrm{RM}_2(r_1^2, m_2) + \\ + \mathrm{RM}_2(r_2^1, m_1) \otimes \mathrm{RM}_2(r_2^2, m_2) + ..., \quad (5)$$

где m_1 и m_2 также приведены в таблице вместе с параметрами $[n, k, d]_2$.

Таблица 1 — D-коды

Номер кода	D-код	$[n,k,d]_2$	m_1	m_2
1	$[(1,2),(2,1)]$	[16384,376,2048]	5	9
2	$[(1,2),(2,1),(3,0)]$	[16384,414,2048]	6	8
3	$[(0,2),(3,1)]$	[16384,406,1024]	6	8
4	$[(1,2),(3,1)]$	[8192,402,512]	5	8
5	$[(1,2),(4,1)]$	[8192,603,256]	6	7
6	$[(1,2),(3,1)]$	[16384,680,1024]	7	7
7	$[(1,2),(3,1)]$	[16384,476,1024]	5	9
8	$[(2,3),(3,0)]$	[8192,1498,256]	5	8
9	$[(2,3),(3,1)]$	[8192,1578,256]	5	8
10	$[(1,2),(3,1)]$	[16384,574,1024]	6	8
11	$[(2,2),(3,0)]$	[16384,876,1024]	7	7
12	$[(0,2),(4,1)]$	[16384,813,512]	7	7
13	$[(1,2),(3,1)]$	[32768,672,2048]	6	9
14	$[(2,3),(3,2)]$	[8192,1858,256]	5	8
15	$[(2,2),(3,1)]$	[16384,1121,1024]	7	7
16	$[(2,3),(3,0)]$	[16384,2066,512]	6	8
17	$[(2,2),(5,1)]$	[16384,1569,256]	7	7
18	$[(1,2),(4,1)]$	[32768,822,1024]	6	9
19	$[(2,3),(3,2)]$	[16384,2786,512]	6	8

В работе выполнена экспериментальная оценка корректирующей способности декодера ISDDecoder для кодов из таблицы 1. В таблице 2 приводятся результаты для нескольких D-кодов, которые будут в дальнейшем использоваться для сравнения с оригинальной системой Мак–Элиса на кодах Гоппы. Здесь $I_9 = \min\{i \in \mathbb{N} : \mathrm{DFR}_1(i) \leqslant 10^{-\gamma}, \gamma = 9\}$, а t – количество добавляемых ошибок.

В таблице 3 приводится оценка времени декодирования с помощью алгоритма ISDDecoder (измерение времени выполнения операций во всех экспериментах настоящей работы производилось на компьютере с процессором Intel Core i7-4771 3.50GHz и оперативной памятью 32 ГБ). Для каждого набора параметров экспериментов из таблицы 2, а именно, D-кода, количества блоков K и значения количества ошибок t приводится

Таблица 2 — Оценка корректирующей способности декодера ISDDecoder

Номер кода	K	P_2	t	Кол-во экспери-ментов	Макс. кол-во плохих блоков	$\mathrm{DFR}_1(0)$	I_9
1	18	0.8301	3749	500000	1	0.000136	26
7	27	0.8251	3830	500000	1	0.000332	237
13	44	0.6626	7687	500000	1	0.000772	88
13	44	0.6626	7772	500000	2	0.00131	105
18	59	0.9161	7279	500000	1	0.0000356	146

время декодирования в миллисекундах. В частности, T_{block} – среднее время, необходимое для выполнения алгоритма BlockDecoder, T_{ISD} – среднее время, необходимое для выполнения одной итерации ДИС, T_1 – среднее время декодирования с помощью алгоритма ISDDecoder, а T_1' – время выполнения алгоритма для обеспечения IND-CPA-стойкости (при $\gamma = 9$) в худшем случае (без раннего выхода из ДИС), то есть $T_1' = T_{block} + T_{\mathrm{ISD}} I_9$.

Таблица 3 — Оценка времени декодирования алгоритмом ISDDecoder

Номер кода	K	t	T_{block}	T_{ISD}	T_1'	T_1
1	18	3749	1726	34	2610	1767
7	27	3830	1706	50	13556	1767
13	44	7687	3535	158	17439	3774
13	44	7772	3535	158	20125	3775
18	59	7279	3440	228	36728	3689

В таблице 4 приводится оценка корректирующей способности декодера MatrixDecoder и его времени декодирования для кодов из таблицы 1, где T_2 – среднее время работы в миллисекундах.

Третья глава посвящена исследованию стойкости криптосистемы типа Мак–Элиса на D-кодах на основе кодов Рида–Маллера. Именно, выделяются множества сильных и слабых ключей криптосистемы. Для слабых ключей криптосистемы строится комбинированная атака, позволяющая с помощью структурной атаки значительно повысить эффективность атаки на шифрограмму, и приводится оценка ее эффективности. Для сильных ключей криптосистемы подбираются параметры для возможности практического применения и проводится сравнение с кодовыми системами на кодах Гоппы при разных подходах к декодированию D-кодов.

Рассмотрим код $\overline{C(D)}$ вида (2) и систему McE($\overline{C(D)}$) на этом коде. Пусть $k = \dim(\overline{C(D)})$, $k_2 = \dim(\overline{C_2(\ell_1)})$ Так как код $\overline{C(D)}$ имеет вид (2), то для $\tau_i = \{(i-1)n_2 + 1,...,in_2\}$ проекция кода $\overline{C(D)}$ на множество τ_i, получаемая путем отбрасывания в кодовых словах всех координат, за

Таблица 4 — Оценка корректирующей способности декодера MatrixDecoder и его времени декодирования

Номер кода	t	DFR_2	T_2	Номер кода	t	DFR_2	T_2
1	4000	$1.54E$–12	2375	11	1706	$5.963E$–20	7985
1	3749	$1.173E$–17	2375	12	1706	$2.167E$–9	127822
2	3392	0.000273	3172	13	7687	$1.344E$–14	8673
3	3392	0.000273	3235	13	7772	$1.128E$–13	8673
4	1744	0.0296	906	14	673	0.000104	45800
5	1194	0.119	9892	15	1706	$5.963E$–20	8001
6	1706	$5.963E$–20	7828	16	1292	$3.802E$–9	81084
7	3830	$5.338E$–8	2907	17	1706	0.000115	1233434
8	612	$5.522E$–6	43597	18	7279	$6.379E$–10	41893
9	612	$5.522E$–6	46722	19	1083	$2.955E$–14	80396
10	3237	$4.557E$–6	3156				

исключением координат из множества τ_i, совпадает с $\overline{C_2(\ell_1)}$, $i \in [\![1,n_1]\!]$. Поэтому найдутся такие $(k \times k_2)$-матрицы M_1, ..., M_{n_1} ранга k_2, что $G_{\overline{C(D)}} = (M_1|...|M_{n_1})\mathrm{diag}(G_{\overline{C_2(\ell_1)}},...,G_{\overline{C_2(\ell_1)}})$.

Для кода $\overline{C_2(\ell_1)}$ и криптосистемы McE($\overline{C_2(\ell_1)}$) обозначим через Attack алгоритм, принимающий на вход открытый ключ $\tilde{G}'$ криптосистемы Мак–Элиса на коде Рида–Маллера $\overline{C_2(\ell_1)}$ с порождающей матрицей $G_{\overline{C_2(\ell_1)}}$ и возвращающий невырожденную $(k_2 \times k_2)$-матрицу S' и перестановочную $(n_2 \times n_2)$-матрицу P', для которых $\tilde{G}' = S' G_{\overline{C_2(\ell_1)}} P'$.

Теорема 5. *Пусть Attack – алгоритм полиномиальной сложности. Если* $\overline{C(D)}^v = \mathbb{F}_q^{n_1} \otimes \overline{C_2(\ell_1)}^v$ *для некоторого* $v(\in \mathbb{N})$, *код* $\overline{C_2(\ell_1)}^v$ *неразложимый, то существует алгоритм AttackDKey полиномиальной сложности, который по матрице* $\tilde{G}$ *вида* (1) *находит такую перестановку* π, *что* $\pi(\mathcal{L}(\tilde{G})) \subseteq \mathbb{F}_q^{n_1} \otimes \overline{C_2(\ell_1)}$.

Перестановке π соответствует матрица Π такая, что $\tilde{G}\Pi = (\hat{S}_1 G_{\overline{C_2(\ell_1)}} \parallel ... \parallel \hat{S}_{n_1} G_{\overline{C_2(\ell_1)}}) = (\hat{G}_1 \parallel ... \parallel \hat{G}_{n_1}) = \hat{G}$, где $\hat{S}_i$ – $(k \times k_2)$–матрица ранга k_2.

Тогда если для кода $\overline{C(D)}$ выполнены условия теоремы 5, то к шифрограмме $\mathbf{z}$ может быть применена построенная в работе атака AttackDCipher. Отметим, что теоремы 1, 2, 3, 4 описывают условия применимости атаки AttackDCipher для D-кодов на основе кодов Рида–Маллера.

В таблице 5 приведены коды, являющиеся тензорным произведением кодов Рида–Маллера. Для этих кодов применима атака AttackDCipher. В таблице содержится оценка вероятности успеха предложенной атаки в сравнении с вероятностью $P_{ISD} = C_{n-t}^k / C_n^k$ успеха атаки простым декодированием по информационным совокупностям. При этом вероятность

успеха атаки AttackDCipher оценивается как в худшем для атакующего случае (P^{min}_{attack}), так и в среднем (P^{avg}_{attack}).

Таблица 5 — Вероятность успеха атаки AttackDCipher для тензорного произведения кодов Рида–Маллера

$\mathrm{RM}_2(r_1,m_1)\otimes\mathrm{RM}_2(r_2,m_2)$	p	K_p	P_{ISD}	P^{min}_{attack}	P^{avg}_{attack}
$\mathrm{RM}_2(4,7)\otimes\mathrm{RM}_2(3,7)$	0.5	101	2.379E-14	5.427E-06	1.219E-01
$\mathrm{RM}_2(5,7)\otimes\mathrm{RM}_2(3,7)$	0.3	120	1.577E-09	5.945E-05	2.265E-02
$\mathrm{RM}_2(6,7)\otimes\mathrm{RM}_2(3,7)$	0.9	127	1.716E-05	7.812E-03	7.812E-03
$\mathrm{RM}_2(4,8)\otimes\mathrm{RM}_2(3,8)$	0.4	164	4.868E-30	4.690E-08	1.721E-01
$\mathrm{RM}_2(5,8)\otimes\mathrm{RM}_2(3,8)$	0.1	219	1.931E-21	1.488E-07	2.749E-02
$\mathrm{RM}_2(6,8)\otimes\mathrm{RM}_2(3,8)$	0.3	247	9.941E-13	1.019E-05	1.179E-02
$\mathrm{RM}_2(7,8)\otimes\mathrm{RM}_2(3,8)$	0.9	255	5.694E-07	3.906E-03	3.906E-03
$\mathrm{RM}_2(4,8)\otimes\mathrm{RM}_2(3,7)$	0.4	164	4.412E-22	4.611E-08	1.692E-01
$\mathrm{RM}_2(4,8)\otimes\mathrm{RM}_2(2,8)$	0.4	164	2.788E-22	4.645E-08	1.705E-01

В таблице 6 приводится оценка вероятности успеха атаки AttackDCipher для D-кодов на основе кодов Рида–Маллера, для которых выполнены условия теоремы 5. Также, как и в таблице 5, здесь вероятность оценивается в худшем для атакующего случае и в среднем. При этом в первом столбце таблицы приводится обозначение D-кода вида (5), где $m_1 = m_2 = 8$. По таблицам 5 и 6 видно, что вероятность успеха

Таблица 6 — Вероятность успеха атаки AttackDCipher для D-кодов на основе кодов Рида–Маллера

D-код	p	K_p	P_{ISD}	P^{min}_{attack}	P^{avg}_{attack}
$[(4,3),(5,2)]$	0.01	219	1.013E-34	1.117E-16	0.145
$[(4,3),(5,2),(6,1)]$	0.01	247	2.646E-35	0	0.011
$[(4,3),(5,2),(6,1),(7,0)]$	0.01	255	2.536E-35	0	0.004

атаки AttackDCipher значительно превосходит вероятность успеха атаки простым декодированием по информационным совокупностям.

В теоремах 2, 3, 4 получены условия на D-код на кодах Рида–Маллера, при которых криптосистема $\mathrm{McE}(\overline{C(D)})$ является гарантированно стойкой к структурной атаке AttackDKey и, соответственно, к атаке AttackDCipher. На основе этих результатов построен алгоритм IsDCodeStrong, позволяющий для заданного D-кода на основе кодов Рида–Маллера определить его принадлежность множеству слабых или сильных ключей (в смысле применимости построенной комбинированной атаки AttackDCipher). Алгоритм IsDCodeStrong также был программно реализован на языке Python.

В таблице 7 приводятся стойкие к атакам AttackDKey и AttackDCipher D-коды на кодах Рида–Маллера при $m_1 = m_2 = 8$. Для этих кодов приводится вероятность P_{ISD} успеха атаки декодированием по информационным совокупностям. Стоит отметить, что в соответствии с [1], код с номером 1 из таблицы 7 является кодом Рида–Маллера $\mathrm{RM}_2(8,16)$, а код под номером 2 его подкодом коразмерности 1. Известно, что криптосистемы на этих кодах не являются стойкими к структурным атакам, поэтому их не целесообразно использовать в криптосистеме.

Таблица 7 — Стойкие к атакам AttackDKey, AttackDCipher D-коды

№	D-код	k	d	P_{ISD}
1*	$[(0,8),(1,7),(2,6),(3,5),(4,4),(5,3),(6,2),(7,1),(8,0)]$	39203	256	1.715E-51
2*	$[(0,8),(1,7),(2,6),(3,5),(4,4),(5,3),(6,2),(7,1)]$	39202	256	1.723E-51
3	$[(1,7),(2,6),(3,5),(4,4),(5,3),(6,2),(7,1)]$	39201	256	1.732E-51
4	$[(1,7),(2,6),(3,5),(4,4),(5,3),(6,2)]$	39129	256	2.458E-51
5	$[(2,6),(3,5),(4,4),(5,3),(6,2)]$	39057	256	3.486E-51
6	$[(2,6),(3,5),(4,4),(5,3)]$	38021	256	4.796E-49
7	$[(3,5),(4,4),(5,3)]$	36985	256	5.498E-47
8	$[(2,5),(4,3)]$	19821	512	7.279E-41
9	$[(4,4)]$	26569	256	1.156E-29

Отметим также, что при использовании гарантированного декодера размер открытого ключа соответствующей криптосистемы получается достаточно большим. В таблице 8 представлено сравнение криптосистемы Original McEliece, криптосистемы на двоичных кодах Рида–Маллера и предлагаемой системы на D-кодах на основе двоичных кодов Рида–Маллера (коды с номерами 3 и 8 из таблицы 7). Для удобства эти криптосистемы в таблицах 8, 10 обозначены McE(G), McE(RM) и McE(D) соответственно.

Таблица 8 — Сравнение характеристик криптосистем типа Мак–Элиса с использованием гарантированного декодера

	McE(G)	McE(RM)		McE(D)	
$[n,k,d]_2$	[3488, 2720, $\geqslant 129$]	[65536, 14893, 1024]	[65536, 39203, 256]	[65536, 19821, 512]	[65536, 39201, 256]
t	64	511	127	255	127
λ_{OW}	142.8	192.62	169.37	136.16	169.37
pk_size, МБ	1.13	116.35	306.27	154.85	306.25
Decoder	декодер Паттерсона	декодер Рида		мажоритарный декодер	
Структурные атаки	–	+		–	

Можно добиться увеличения стойкости системы Мак–Элиса к атакам

на шифрограмму путем увеличения веса добавляемого вектора ошибок. Это, в свою очередь, позволяет для заданного уровня стойкости уменьшить размер ключа.

Одним из способов увеличения количества исправляемых ошибок является использование построенных вероятностных декодеров ISDDecoder и MatrixDecoder. В таблице 9 приводятся параметры криптосистемы типа Мак–Элиса на основе D-кодов из таблицы 1 при использовании декодеров ISDDecoder и MatrixDecoder. Отметим, что эти коды являются стойкими к атакам AttackDKey и AttackDCipher. Как было сказано ранее, в обоих алгоритмах ISDDecoder и MatrixDecoder предполагается использование декодера Йе–Аббе.

Таблица 9 — Характеристики системы типа Мак–Элиса на D-кодах с использованием вероятностных декодеров

Номер кода	pk_size, МБ	t	λ_{OW}	Номер кода	pk_size, МБ	t	λ_{OW}
1	0.734	4000	153.87	11	1.711	1706	143.04
1	0.734	3749	142.82	12	1.588	1706	132.47
2	0.809	3392	140.55	13	2.625	7687	262.28
3	0.793	3392	137.8	13	2.625	7772	265.61
4	0.393	1744	142.82	14	1.814	673	262.22
5	0.589	1194	142.81	15	2.189	1706	184.58
6	1.328	1706	110.3	16	4.035	1292	262.47
7	0.93	3830	185.96	17	3.064	1706	262.40
8	1.463	612	186.11	18	3.211	7279	302.23
9	1.541	612	197.24	19	5.441	1083	302.32
10	1.121	3237	185.94				

В таблице 10 приводится сравнение системы McE(D) на D-кодах с системами Original McEliece и Classic McEliece на кодах Гоппы. Сравнение проводится для пяти уровней стойкости системы McE(G), которые соответствуют базовым наборам параметров (mceliece348864, mceliece460896, mceliece6688128, mceliece6960119, mceliece8192128) криптосистемы Classic McEliece.

Как видно из таблицы, использование D-кодов в криптосистеме типа Мак–Элиса позволяет сократить размер открытого ключа относительно системы Original McEliece. Отметим, что в таблице также имеются D-коды, для которых криптосистема обладает меньшим размером ключа даже при значительно большей стойкости λ_{OW}, например, коды 7 и 18. Однако для найденных D-кодов криптосистема McE(D) уступает системе Classic McEliece по размеру ключа. Сравнивая криптосистемы Мак–Элиса на кодах Гоппы и D-кодах, стоит отметить, что время расшифрования у последней больше, как при декодировании алгоритмом ISDDecoder, так

Таблица 10 — Сравнение характеристик криптосистем типа Мак–Элиса при использовании вероятностных декодеров для D-кодов

McE(G)					McE(D)			
Уровень стойкости	t	λ_{OW}	pk_size, Original McEliece, МБ	pk_size, Classic McEliece, МБ	Номер кода	t	λ_{OW}	pk_size, МБ
1 (348864)	64	142.8	1.13	0.25	1	3749	142.82	0.73
2 (460896)	96	185.92	1.85	0.5	7	3830	185.96	0.93
3 (6688128)	128	262.28	4.01	1	13	7687	262.28	2.63
4 (6960119)	119	265.6	4.49	1	13	7772	265.61	2.63
5 (8192128)	128	302.21	6.38	1.29	18	7279	302.23	3.21

и алгоритмом MatrixDecoder. Действительно, у систем на кодах Гоппы время расшифрования составляет от 20 до 120 миллисекунд в зависимости от выбранных параметров. Однако отметим, что такое время достигается при использовании оптимизированной реализации декодера[8], в то время как в таблицах 3 и 4 указано время работы алгоритмов, для которых не ставилась цель создания оптимальной реализации. Существует большой потенциал для ускорения алгоритмов ISDDecoder и MatrixDecoder. Например, они хорошо поддаются распараллеливанию, в том числе за счет параллельного декодирования блоков в BlockDecoder.

Таким образом, в настоящей работе удалось построить криптосистему с меньшим ключом, чем в криптосистеме Original McEliece, только для протокола KEM с IND-CPA-стойкостью (для передачи эфемерных криптографических ключей). Однако, учитывая интерес мирового и в том числе отечественного криптографического сообщества к протоколам KEM с IND-CPA-стойкостью, это ограничение представляется не таким существенным. Кроме того, как было недавно показано, двоичные коды Рида-Маллера достигают емкости в симметричных каналах без памяти, поэтому ожидается дальнейшее развитие методов эффективного декодирования этих кодов, которые могут позволить не только уменьшить время расшифрования в предлагаемой криптосистеме, но и повысить класс стойкости за счет уменьшения вероятности ошибочного декодирования.

Заключение

Основным результатом работы является решение актуальной научной задачи, имеющей практическую значимость: построена асимметричная кодовая криптосистема типа Мак–Элиса на D-кодах на основе кодов Рида–Маллера, которая обладает либо большей стойкостью при сопоставимом размере ключа, либо меньшим размером ключа при сопоставимой

[8] Albrecht M. R. [et al.]. Classic McEliece: Conservative Code-Based Cryptography. NIST PQC Call for Proposals, 2022. Round 4 Submission. 2022.

стойкости, либо большей стойкостью при меньшем размере ключа по сравнению с системой Original McEliece. Это позволяет применять предложенную систему в механизме инкапсуляции сеансового ключа симметричной криптосистемы, а также для повышения защищенности данных, циркулирующих в информационных системах, за счет использования рандомизированного шифрования.

В процессе работы были получены следующие результаты:

1. Разработана алгоритмическая модель мажоритарного декодирования D-кодов.
2. Разработаны алгоритмы вероятностного декодирования D-кодов на основе кодов Рида–Маллера.
3. Получены условия разложимости квадрата Шура–Адамара D-кодов на основе кодов Рида–Маллера в прямую сумму неразложимых кодов.
4. Построена комбинированная атака для слабых ключей криптосистемы типа Мак–Элиса на основе подкодов прямой суммы кодов, использующая структурную атаку для атаки на шифрограмму.
5. Найдены параметры криптосистемы типа Мак–Элиса на D-кодах на основе кодов Рида–Маллера, соответствующие сильным ключам, для которых размер открытого ключа меньше, чем у оригинальной системы Мак–Элиса на кодах Гоппы.

В завершение настоящего исследования считаю важным выразить глубокую признательность и искреннюю благодарность и почтить светлую память моего первого научного руководителя, к.ф.-м.н. Деундяка Владимира Михайловича, сыгравшего ключевую роль в становлении меня как исследователя. Его вера в мои способности, неугасимый энтузиазм, трудолюбие и искреннее увлечение наукой вдохновили меня на выбор научного пути и заложили основу всей последующей работы. Он навсегда останется в памяти примером истинного ученого и прирожденного наставника.

Отдельную благодарность выражаю моему научному руководителю, к.т.н. Косолапову Юрию Владимировичу, под чьим руководством была завершена данная работа. Его поддержка, внимание к деталям, оптимизм и уверенность в успешном завершении исследования оказались неоценимыми в процессе преодоления научных и организационных трудностей. Благодаря его помощи и профессионализму удалось довести диссертационное исследование до логического и научно обоснованного завершения.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Статьи в научных изданиях, входящих в Перечень ВАК

1. Косолапов, Ю. В. О структурной стойкости криптосистемы типа Мак-Элиса на сумме тензорных произведений бинарных кодов Рида-Маллера / Ю. В. Косолапов, Е. А. Лелюк // Прикладная дискретная математика. – 2022. – № 57. – С. 22-39. – DOI 10.17223/20710410/57/2. (К1, RSCI, Scopus)
2. Косолапов, Ю. В. Криптосистема типа Мак-Элиса на D-кодах / Ю. В. Косолапов, Е. А. Лелюк // Математические вопросы криптографии. – 2024. – Т. 15, № 2. – С. 69-90. – DOI 10.4213/mvk470. (К1, RSCI)
3. Косолапов, Ю. В. О параметрах системы шифрования типа Мак-Элиса на D-кодах, основанных на двоичных кодах Рида-Маллера / Ю. В. Косолапов, Е. А. Лелюк // Прикладная дискретная математика. – 2025. – № 67. – С. 7-35. – DOI 10.17223/20710410/67/1. (К1, RSCI, Scopus)

Статьи в научных изданиях, входящих в Scopus

4. Deundyak, V. M. A Graph-Theoretical Method for Decoding Some Group MLD-Codes / V. M. Deundyak, E. A. Lelyuk // Journal of Applied and Industrial Mathematics. – 2020. – Vol. 14, No. 2. – P. 265-280. – DOI 10.1134/S1990478920020064. (Scopus, Q3)
5. Deundyak, V. M. Decoding the Tensor Product of MLD Codes and Applications for Code Cryptosystems / V. M. Deundyak, Y. V. Kosolapov, E. A. Lelyuk // Automatic Control and Computer Sciences. – 2018. – Vol. 52, No. 7. – P. 647-657. – DOI 10.3103/S0146411618070064. (Scopus, Q3)

Статьи в журналах, индексированных в РИНЦ

6. Косолапов, Ю. В. О разложимости произведения Шура - Адамара суммы тензорных произведений кодов Рида-Маллера / Ю. В. Косолапов, Е. А. Лелюк // Прикладная дискретная математика. Приложение. – 2021. – № 14. – С. 158-161. – DOI 10.17223/2226308X/14/35.

Публикации в сборниках трудов конференций

7. Лелюк, Е. А. Декодирование М-ортогонального семейства кодов / Е. А. Лелюк // Современные информационные технологии: тенденции и перспективы развития : материалы XXVI научной конференции, (Южный федеральный университет, Ростов-на-Дону, 18–19 апреля 2019 г.) / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования

«Южный федеральный университет», Институт математики, механики и компьютерных наук им. И. И. Воровича ; редакционная коллегия: Г. В. Муратова, Я. М. Ерусалимский, С. С. Михалкович, В. С. Пилиди, В. Ю. Тополов. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, Южный федеральный университет, 2019. – С. 164-166.

8. Деундяк, В. М. О декодировании кодов на основе D-конструкции / В. М. Деундяк, Е. А. Лелюк // Современные информационные технологии: тенденции и перспективы развития : материалы XXV научной конференции, (Южный федеральный университет, Ростов-на-Дону, 17–18 мая 2018 г.) / Министерство науки и высшего образования Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Институт математики, механики и компьютерных наук им. И. И. Воровича ; редакционная коллегия: Г. В. Муратова, Я. М. Ерусалимский, С. С. Михалкович, В. С. Пилиди, В. Ю. Тополов. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – С. 63-64.
9. Лелюк, Е. А. Декодирование тензорных произведений кодов на некоммутативных группах / Е. А. Лелюк // Сборник тезисов участников форума "Наука будущего – наука молодых [Нижний Новгород, 12–14 сентября 2017 г. : в 2 т.]. Т. 1. – Москва ; Нижний Новгород : Инконсалт К, 2017. – С. 126-127.

Свидетельство о государственной регистрации программы для ЭВМ

10. Свидетельство о государственной регистрации программы для ЭВМ № 2024691736 Российская Федерация. Программное средство определения множества сильных и слабых ключей криптосистемы на D-кодах на основе кодов Рида-Маллера : № 2024690988 : заявл. 14.12.2024 : опубл. 24.12.2024 / Е. А. Лелюк ; правообладатель Е. А. Лелюк.

Личный вклад автора в работы, выполненные в соавторстве

В [1] и [6] исследованы свойства Шура–Адамара D-кодов на основе кодов Рида–Маллера и получены условия их разложимости в прямую сумму неразложимых кодов. В [2] и [3] проведены эксперименты по оценке эффективности работы вероятностных декодеров для D-кодов на основе кодов Рида–Маллера и найдены параметры криптосистемы типа Мак–Элиса на основе этих кодов, позволяющие применять систему на практике в схеме инкапсуляции сеансового ключа. В [4], [5] и [8] построена алгоритмическая модель гарантированного декодера для D-кодов на основе мажоритарного подхода Мэсси.