МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М.В.ЛОМОНОСОВА

Отзыв научного руководителя на диссертацию
Высоцкой Виктории Владимировны
«Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки», представленную на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Общая характеристика соискателя. Высоцкая Виктория Владимировна окончила сначала бакалавриат факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова в 2016 году, а затем в 2018 году и магистратуру того же факультета с красным дипломом. С 2018 по 2022 год она обучалась в очной аспирантуре факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Во время обучения В.В.Высоцкая проявила себя способной ученицей, умеющей разобраться в достаточно большом и сложном материале по теме диссертации.

В настоящее время В.В.Высоцкая работает на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова в должности математика. Она читает обязательные курсы, непосредственно связанные с тематикой ее диссертации.

Актуальность темы. Кандидатская диссертация Высоцкой Виктории Владимировны посвящена вопросам построения электронных подписей на основе кодов, исправляющих ошибки, а также анализа подобных конструкций.

В настоящее время мировое криптографическое сообщество уделяет большое внимание так называемым постквантовым криптосистемам с открытым ключом, к которым относятся и все теоретико-кодовые криптосистемы, рассматриваемые в диссертации.

В 1994 году П. Шор предложил эффективный алгоритм решения задачи целочисленной факторизации и задачи дискретного логарифмирования в произвольной коммутативной конечной группе. Фактически алгоритм Шора позволяет с использованием квантового ускорителя взламывать все криптографические механизмы с открытым ключом, используемые в настоящее время на практике.

Альтернативой классическим механизмам являются криптографические схемы, построенные на каких-либо $\mathbb{NP}$-трудных задачах, так как исследовали считаю, что именно для этого класса задач нельзя построить эффективных квантовых алгоритмов. Такие криптосистемы называются постквантовыми, т.е. считается, что они будут стойкими даже после появления квантовых компьютеров большой мощности.

К постквантовым относятся практически все теоретико-кодовые криптосистемы, стойкость которых основана на сложности декодирования кода общего положения, либо на других вычислительно сложных теоретико-кодовых задачах.

Пожалуй старейшей теоретико-кодовой криптосистемой является криптосистема Мак-Элиса, предложенная в 1978 году Р. Мак-Элисом. Идея построения этой криптосистемы сводится к маскировке некоторого линейного кода, имеющего эффективные алгоритма декодирования, под так называемый код общего положения, который не имеет видимой алгебраической, комбинаторной или иной структуры. Оригинальная криптосистема Мак-Элиса строится на двоичных неприводимых кодах Гоппы. При использовании подобного класса кодов оказывается сложно из криптосистемы Мак-Элиса построить схему подписи. Однако эта криптосистема, по-существу, является целым каркасом для построения криптографических механизмов и протоколов. Класс кодов, является базовым элементом конструкции. Его можно модифицировать и получать криптомеханизмы с новыми свойствами и новыми тактико-техническими и пользовательскими характеристиками. А значит меняя класс кодов можно подобрать такой, чтобы он имел достаточно большой радиус покрытия.

В 1986 году Г. Нидеррайтер предложил, во-первых, модификацию криптосистемы Мак-Элиса, которая, правда, полностью эквивалентна этой криптосистеме, а, во-вторых, решил использовать для построения криптосистемы обобщенные коды Рида–Соломона.

Но в 1992 году В.М.Сидельников совместно с С.О.Шестаковым построили эффективную атаку восстановления секретного ключа на криптосистемы Мак-Элиса и Нидеррайтера, основанные на обобщенных кодах Рида–Соломона.

При этом в 1994 году сам В.М.Сидельников предложил использовать для построению криптосистемы коды Рида–Маллера, в некотором смысле, родственные кодам Рида–Соломона. Однако в 2006 году была построена достаточно эффективная атака Миндера—Шокроллахи на эту модификацию, а в 2014 года М.А.Бородиным и И.В.Чижовым была предложена первая полиномиальная атака на эту криптосистему.

Однако исследователи не останавливаются на идее использовать коды Рида–Соломона, коды Рида–Маллера и производные от них коды для построения криптосистем и предлагают все новые и новые модификации криптосистемы Мак-Элиса на основе таких кодов. Это связано с тем, что как раз указанные классы кодов имеют большой радиус покрытия и они могут использоваться для построения схемы электронной подписи из криптосистемы Мак-Элиса.

Кроме того, сама возможность использовать в конструкциях Мак-Элиса и Нидеррайтера различные классы кодов, побуждает исследователей предлагать свои модификации криптосистем на разнообразных классах кодов, обладающих затейливой алгебраической структурой.

В целом интерес к исследованию теоретико-кодовых криптосистем был подогрет конкурсом Национального института стандартов и технологий США (NIST USA), который в 2016 году объявил, что планирует в течение 10 лет разработать новый набор стандартов в области постквантовой криптографии. С этого момента начался настоящий бум исследований как в области постквантовой криптографии, так и в области кодовой криптографии.

Хотя конкурс официально был завершен и был выбран набор победителей, однако, в силу того, что финалисты не удовлетворяют всех потребностей в криптографических механизмах, был объявлен дополнительный раунд по схемам электронной подписи. Поэтому можно с уверенностью сказать, что процесс не завершится, а перейдет в вялотекущую стадию, поэтому исследования в области постквантовой криптографии останутся актуальными и в дальнейшем.

В России также ведутся работы в области стандартизации постквантовых механизмов с открытым ключом. В 2019 году в рамках Технического комитета 26 Росстандарта России была создана группа по постквантовой криптографии. В рамках этой группы активно ведутся работы в области стандартизации постквантовых механизмов, в том числе, построенных на основе кодов, исправляющих ошибки.

Как уже ранее отмечалось, наиболее интересны с точки зрения практики два постквантовых криптографических механизма — это схемы инкапсуляции ключа и схемы электронной подписи. Причем механизмов электронной подписи, которые построены на задачах теории кодов, исправляющих ошибки, не так много. Во-первых, старейшей является конструкция схем подписи CFS, работающая в парадигме хешируем—подписываем (hash-and-sign). Второй конструкцией являются схемы, построенные с использованием преобразования Фиата–Шамира из протоколов доказательства с нулевым разглашением знания секрета. В диссертации уделяется вопрос обеим этим подходам.

Таким образом, в диссертации Высоцкой Виктории Владимировны решаются актуальные и практически значимые для защиты информации задачи.

Цели и задачи. Целью диссертации В.В.Высоцкой является анализ методов построения схем электронной подписи на основе кодов, исправляющих ошибки, путем исследования структурных свойств кодов, лежащих в основе схем подписи, а также анализ подходов, не зависящих от конкретного класса кодов.

Для достижения поставленной цели автором решались следующие задачи:

1. Исследовать стойкость схемы 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. Исследовать подход, связанный с применением преобразования Фиата–Шамира к схеме идентификации Штерна, для возможного построения новой схемы электронной подписи на основе кодов, исправляющих ошибки, стойкость которой не зависела бы от какой-либо структуры используемого кода.

Степень достижения целей и задач. В результате автором получены следующие основные результаты:

1. Описаны структурные свойства подкодов кода Рида–Маллера $RM(2,m)$, при которых схема подписи CFS будет устойчива к атакам, применимым к схемам, построенным на всем коде Рида–Маллера. Описаны структурные свойства и предложен алгоритм генерации подкодов кода $RM(r,m)$, для которых схема подписи CFS не будет подвержена известным структурным атакам.
2. Установлены условия, которые гарантируют существование обратной матрицы у квазициклической матрицы над факторкольцом $\mathbb{F}_2[x]/(x^r-1)$. Также получены нижние оценки доли обратимых матриц среди всех матриц заданного размера над факторкольцом $\mathbb{F}_2[x]/(x^r-1)$.
3. Предложен эффективный алгоритм вычисления определителя квазициклической матрицы над факторкольцом $\mathbb{F}_2[x]/(x^r-1)$ и эффективный алгоритм порождения обратимых матриц с равномерным распределением на множестве всех обратимых квазициклических матриц заданного размера.
4. Установлена оценка снизу на мощность множества открытых ключей схемы подписи, построенной на основе конструкции Сидельникова. Описана структура классов эквивалентности секретных ключей схемы через группы автоморфизмов линейного кода и его квадрата Шура–Адамара.

Для случая, когда в схеме используется обобщенный код Рида–Соломона, структура класса эквивалентности секретных ключей описана более точно, чем для общей конструкции и выделены три подкласса секретных ключей, которые не позволяют проводить структурные атаки на основе произведения Шура–Адамара линейных кодов.

5. 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) при условии сложности задачи декодирования случайного линейного кода.

Таким образом, считаю, что поставленные задачи полностью выполнены и цель работы достигнута.

Структура работы. 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 и 4 алгоритма и 1 приложение. Список литературы включает 84 наименования на 9 страницах.

Во введении работы обосновывается актуальность выбранной темы диссертации, сформулированы цели и задачи исследований.

Глава 1 посвящена вопросам исследования алгебраической структуры ключей электронной подписи CFS на основе подкодов кодов Рида–Маллера. Известно, что если квадрат Адамара (или Шура–Адамара) подкода совпадает с квадратом соответствующего кода Рида–Маллера, то на схему подписи CFS можно применить структурную атаку Бородина–Чижова.

С целью выявления подкодов, потенциально пригодных для криптографического применения, рассматриваются вопрос построения подкодов Рида–Маллера путем исключения из стандартного базиса кода Рида–Маллера векторов-значений некоторого количества мономов, при этом решается задачи минимизации числа исключаемых векторов.

В главе 2 изучаются вопросы построения схемы электронной подписи CFS на основе квазициклических кодов. При использовании квазициклических ко-

дов в схеме CFS встает задача порождения случайной невырожденной матрицы над факторкольцом кольца многочленов $\mathbb{F}_2[x]/(x^r - 1)$. Однако в общем случае для колец не работают классические алгоритмы линейной алгебры над полем, включая алгоритм Гауссова исключения. Поэтому автором разрабатываются вычислительно эффективные подходы поиска определителя матрицы и проверки его на равенство нулю. При этом описанные алгоритмы обладают низкой вычислительной сложностью и могут использоваться в схемах CFS для больших значений параметров.

Глава 3 посвящена изучению схемы подписи CFS, построенной на основе операции комбинирования кодов друг с другом. В качестве комбинирующей операции рассматривается последовательное соединение кодов друг с другом. Рассматриваются два класса базовых кодов, участвующих в соединении. Первый класс — коды Рида–Соломона, а второй класс — коды общего вида. В итоге описываются классы эквивалентности секретных ключей для кодов Рида–Соломона и выделяются классы, для которых не работают известные атаки.

В главе 4 рассматривается вопрос построения схемы электронной подписи в парадигме применения преобразования Фиата–Шамира к схеме идентификации Штерна. Построена релевантная модель противника и доказана стойкость новой схемы подписи в этой модели противника при условии сложности задачи декодирования кода общего положения.

Оригинальность работы. Все полученные в диссертации результаты получены автором диссертации самостоятельно. В публикациях, выполненных в соавторстве, другим авторам либо принадлежит постановка задачи, либо доказательство вспомогательных утверждений.

Диссертация представляется к защите впервые.

Научная новизна. Все результаты работы являются новыми и представляют существенную научную ценность.

Практическая и теоретическая значимость. Диссертация носит в основном теоретический характер и представляет собой цельное законченное исследование.

Результаты работы значительно развивают математические подходы к построению и обоснованию стойкости криптографических схем подписи, основанных на кодах, исправляющих ошибки.

Результаты диссертации частично были использованы в рамках Технического комитета 26 Росстандарта при разработке схемы подписи «Шиповник».

Достоверность положений. Достоверность полученных результатов подтверждается строгими математическими доказательствами, приведенными в тексте диссертации, а также программной реализацией предложенных методов. Доказательства существенно используют методы алгебраической теории кодирования, дискретной математики, комбинаторики, линейной алгебры, теории графов и теории вероятностей.

Основные результаты, полученные в диссертации, излагались на международных и всероссийских конференциях и научно-исследовательских семинарах, и опубликованы в печатных рецензируемых научных журналах.

Вывод. Диссертация Высоцкой Виктории Владимировны «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» соответствует паспорту специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки): полученные в ней результаты соотносятся с разделами 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».

Считаю, что диссертационная работа Высоцкой Виктории Владимировны «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» удовлетворяет всем требованиям «Положения о присуж-

дении ученых степеней в МГУ имени М.В. Ломоносова» и рекомендую ее к защите в диссертационном совете МГУ 012.3 на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Научный руководитель:
доцент кафедры информационной
безопасности факультета
ВМК МГУ имени М.В.Ломоносова,
канд. физ.-мат. наук И.В. Чижов

Контактные данные.

ФИО: Чижов Иван Владимирович.

Ученая степень: кандидат физико-математических наук.

E-mail: chizhoviv@my.msu.ru, тел.: 8(495)930-43-76 (раб.).

Специальность, по которой И.В. Чижовым была защищена кандидатская диссертация: 05.13.19 — «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Адрес места работы: 119234, Москва, Ленинские горы, дом 1, стр. 52, МГУ имени М.В. Ломоносова, 2-й учебный корпус, факультет ВМК, кафедра информационной безопасности.

Должность: доцент кафедры информационной безопасности.

Подпись Чижова Ивана Владимировича удостоверяю:

Декан факультета
ВМК МГУ имени М.В. Ломоносова,
академик И.А. Соколов