ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Лелюка Евгения Андреевича на тему
«Синтез постквантовой схемы инкапсуляции сеансового ключа»,
представленную на соискание учёной степени кандидата технических наук
по специальности 2.3.6 «Методы и системы защиты информации,
информационная безопасность»

Актуальность избранной темы

Одним из главных вызовов современной криптографии стало развитие квантовых вычислений. Традиционные асимметричные криптосистемы основаны на сложности факторизации целых чисел и вычисления дискретного логарифма в конечных группах. Однако известно, что при наличии достаточно мощного квантового компьютера обе эти задачи могут решаться за полиномиальное время. Поэтому сегодня особую актуальность приобретает разработка криптографических механизмов, устойчивых к квантовым атакам.

Значимость этого направления подтверждается не только теоретическими исследованиями, но и практическими инициативами. В разных странах ведется активная работа по стандартизации постквантовых решений, что подтверждается конкурсами NIST PQC в США, KpqC Competition в Южной Корее, а также деятельностью российской рабочей группы ТК26, занимающейся созданием схемы инкапсуляции сеансового ключа, устойчивой к нарушителю с доступом к квантовому компьютеру. В качестве одной из альтернатив асимметричным криптосистемам рассматриваются схемы, основанные на помехоустойчивых кодах.

Первой кодовой криптосистемой считается схема Роберта Мак-Элиса, предложенная в 1978 году и основанная на кодах Гоппы. На ее основе был создан протокол инкапсуляции сеансового ключа NTS-KEM, участвовавший в конкурсе NIST PQC, а позднее объединенный с проектом Classic McEliece, вошедшим в число финалистов конкурса. Стойкость Original McEliece и связанных с ней решений, в частности, определяется трудностью задачи декодирования случайного кода, для которой пока не найдено эффективного квантового алгоритма. Вместе с тем существенным недостатком схем на кодах Гоппы остается большой размер открытого ключа. Стремление уменьшить его привело к исследованию других семейств кодов, включая коды Рида-Соломона, Рида-Маллера, алгебро-геометрические коды и коды с низкой плотностью проверок на четность. Однако эти попытки не привели к успеху, поскольку для соответствующих криптосистем были найдены эффективные структурные атаки. Важно и то, что коды Гоппы относятся к

классу альтернантных кодов. Для некоторых их классов уже предложены структурные атаки, а эффективная атака была найдена и для одного из классов подпространственных подкодов кодов Рида-Соломона, также принадлежащих к альтернантным кодам.

Таким образом, несмотря на существование стойких схем, задача поиска новых эффективно декодируемых помехоустойчивых кодов остается актуальной. Не исключено, что в будущем появятся эффективные структурные атаки и на другие классы кодов Гоппы. Поэтому по-прежнему важна разработка новых кодовых конструкций, позволяющих создавать криптосистемы типа Мак-Элиса с высокой стойкостью и меньшим размером открытого ключа.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Научные результаты, положения, выводы и рекомендации, изложенные в диссертации, обоснованы в ходе, как теоретических исследований, так и при проведении вычислительных экспериментов и создании алгоритмов обработки информации. Это подтверждается их апробацией на научных конференциях, которые достаточно полно излагают ключевые результаты исследования, а также внедрением результатов работы в образовательную и научно-практическую деятельность, что подтверждается актами внедрения.

Научная новизна результатов, научных положений выводов и рекомендаций и их значимость

В диссертации получен ряд новых научных результатов, к основным из которых можно отнести следующие:

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.

Новизна результатов, положений, выводов и рекомендаций, сформулированных в диссертации, подтверждается: отсутствием в доступной литературе работ с аналогичными научными и техническими решениями; положительными отзывами специалистов на опубликованные статьи, доклады, представленные на конференциях; наличием свидетельства о государственной регистрации программы для ЭВМ.

Теоретическая значимость результатов исследования

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 кодовых криптосистем на основе подкодов прямой суммы кодов.

Практическая ценность работы

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.

Достоверность научных результатов, научных положений, выводов и рекомендаций, сформулированных в диссертации

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

Оценка содержания диссертации, степени её завершённости, подтверждение публикаций автора

Во введении обосновывается актуальность темы, дается обзор литературы, формулируются цель и задачи исследования, раскрываются научная новизна и практическая значимость работы, приводятся положения, выносимые на защиту, сведения об апробации результатов и краткое содержание глав.

В первой главе рассматриваются асимметричные криптосистемы в протоколах инкапсуляции сеансового ключа, а также подходы к построению новых кодовых криптосистем. Излагаются основные понятия теории кодирования и основы мажоритарного декодирования, применяемого далее для построения декодера D-кодов с гарантированным исправлением ошибок.

Во второй главе исследуются D-коды и их криптографические свойства. Определяются условия разложимости степеней Шура-Адамара D-кодов на основе кодов Рида-Маллера, а также строятся гарантированный и вероятностные декодеры. Для вероятностных декодеров приводятся экспериментальные результаты, подтверждающие их эффективность.

В третьей главе разрабатывается схема инкапсуляции сеансового ключа на основе системы Мак-Элиса на D-кодах и исследуется ее стойкость. Выделяются сильные и слабые ключи, для слабых ключей описывается комбинированная атака и оценивается ее эффективность. Для сильных ключей подбираются параметры практического применения и проводится сравнение с системой на кодах Гоппы.

В заключении изложен основной научный результат диссертации, а также сформулированы теоретические и практические результаты, полученные в результате диссертационной работы.

В приложениях приводятся акты о внедрении результатов диссертационной работы, а также свидетельство о государственной регистрации программы для ЭВМ.

Диссертация является завершённым научно-исследовательским трудом. Задачи, поставленные автором, решены полностью, цель исследования достигнута.

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. Результаты работы прошли апробацию на научных конференциях различного уровня.

Соответствие 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).

Замечания по диссертационной работе

1. Экспериментальные оценки (например, в Таблице 3) полезны, но не дают обоснования выбора параметров K и I_{max} вне эмпирического подбора.
2. Отсутствие сравнения с современными постквантовыми KEM, не основанными на кодах Гоппы. В работе подробно сравниваются параметры с Original/Classic McEliece, но нет сравнения с другими конкурентами NIST, такими, как BIKE, HQC (кодовые KEM на LDPC и циклических кодах) и Kyber (на решётках), несмотря на иной математический аппарат.
3. Недостаточная мотивация выбора именно кодов Рида-Маллера как базовых. Работа опирается на коды Рида-Маллера, которые исторически известны как уязвимые в криптосистеме Мак-Элиса. Хотя D-конструкция скрывает исходную структуру, остаётся вопрос: почему не рассмотрены другие MLD-коды, которые потенциально могут обеспечить лучшее соотношение «стойкость / размер ключа»?

Приведённые замечания не являются значительными по сравнению с отмеченными выше теоретической значимостью и практической ценностью данной диссертационной работы.

Заключение о соответствии диссертации критериям, установленным Положением о присуждении ученых степеней в ЮФУ для кандидатских диссертаций

Диссертация Лелюка Е. А. представляет собой законченную научно-квалификационную работу, посвящённую решению актуальной задачи, имеющей важное значение в области информационной безопасности. Диссертация обладает научной новизной, имеет теоретическую значимость и практическую ценность. Полученные результаты в полной мере отражены в авторских публикациях. Автореферат полностью отражает содержание диссертации.

Диссертация отвечает требованиям, установленным Положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявленным к диссертациям на соискание учёной степени кандидата наук, а автор, Лелюк Евгений Андреевич, заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Официальный оппонент
Кандидат физико-математических наук (01.01.06 «Математическая логика, алгебра и теория чисел»), доцент департамента «Прикладная математика», Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики»,
Малыгина Екатерина Сергеевна

123458, г. Москва, ул. Таллинская, 34, НИУ ВШЭ, МИЭМ
Тел. служ.: +7 (495) 916-88-29, email: miem@hse.ru

«20» апреля 2026 г. _____/Е. С. Малыгина/

Подпись Е. С. Малыгиной заверяю

Подпись заверяю
Специалист по кадровому делопроизводству
Центра по кадровому администрированию
Управления персонала
Е.Ю. Саркисова