Отзыв научного руководителя диссертации Е. А. Лелюка
«Синтез постквантовой схемы инкапсуляции сеансового ключа»,
представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 “Методы и системы защиты информации, информационная безопасность”

Основной целью диссертационного исследования Е.А. Лелюка является поиск альтернативы кодам Гоппы для криптосистемы типа Мак-Элиса. Актуальность такого исследования связана с тем, что асимметричная схема шифрования Мак-Элиса на кодах Гоппы уже почти пятьдесят лет не поддается криптоанализу (известные атаки не являются полиномиальными), что позволяет судить о потенциально высокой стойкости этой схемы и рассматривать ее как основу для постквантового механизма инкапсуляции сеансового ключа. Однако возможное утверждение системы Мак-Элиса на кодах Гоппы в качестве одного из официально допустимых постквантовых криптопримитивов только мотивирует исследователей к поиску способов «расшатывания» этой криптосистемы. И ее высокая стойкость в настоящий момент не гарантирует отсутствие эффективных атак в будущем. Одним из способов нивелирования риска взлома любой криптосистемы может быть переход на альтернативную систему. В диссертационном исследовании Е.А. Лелюка выбран путь построения альтернативы на основе замены кода в схеме Мак-Элиса. С одной стороны, это несколько упрощает анализ, так как для этой схемы уже известны наилучшие атаки на сообщение, не зависящие от кода. С другой стороны, трудность задачи состоит в том, что альтернативный код должен быть эффективно декодируемым и отличаться от известных кодов, на которых попытки построить схему шифрования типа Мак-Элиса оказались неуспешными.

В диссертационном исследовании в качестве потенциально подходящего семейства кодов для схемы типа Мак-Элиса выбрано семейство так называемых *D*-кодов, в которых базовыми являются двоичные коды Рида-Маллера. Евгению, для достижения поставленной в диссертационном исследовании цели, предстояло решить три непростые задачи: 1) исследовать возможности эффективного декодирования *D*-кодов, 2) исследовать свойства *D*-кодов, влияющие на стойкость схемы Мак-Элиса к известным атакам на ключ, 3) выделить параметры *D*-кодов, обеспечивающие высокую стойкость соответствующей схемы шифрования. Полагаю, что со всеми задачами Лелюк Е.А. успешно справился.

В диссертации Е.А. Лелюка, в рамках обозначенных задач получены следующие основные результаты:

- **эффективные декодеры *D*-кодов для схемы типа Мак-Элиса**: построена алгоритмическая модель мажоритарного декодера, позволяющего гарантированно исправлять ошибки веса, не превышающего половины кодового расстояния; разработаны вероятностные декодеры, эффективно исправляющие ошибки за пределами половины кодового расстояния, что позволило существенно сократить размер ключа схемы шифрования;

- **криптографические свойства *D*-кодов**: исследовано представление степеней Шура-Адамара для *D*-кодов, основанных на двоичных кодах Рида-Маллера; это позволило выделить *D*-коды, для которых степени Шура-Адамара являются разложимыми кодами, а также те *D*-коды, для которых такие степени не являются разложимыми; доказано, что в случае разложимых степеней удается существенно повысить вероятность атаки на сообщение: разработана атака, сводящая в этом случае стойкость схемы на *D*-кодах к стойкости схемы на двоичных кодах Рида-Маллера;
- **параметры *D*-кодов для стойкой схемы типа Мак-Элиса:** на основе результатов построения вероятностных декодеров и исследования криптографических свойств *D*-кодов разработана и реализована схема выбора параметров *D*-кодов, обеспечивающих высокую стойкость соответствующей схемы Мак-Элиса к атакам на ключ и сообщение; это позволило найти параметры, при которых схема Мак-Элиса на *D*-кодах имеет меньший публичный ключ, чем в случае использования кодов Гоппы, и при этом не уступает по уровню стойкости.

О структуре диссертации. Диссертация Лелюка Евгения состоит из введения, трех глав и заключения. В первой главе рассматривается схема асимметричного шифрования и механизм инкапсуляции сеансового ключа (KEM), вводятся основные понятия теории кодирования, используемые в кодовой криптографии, приводится описание криптосистемы Мак-Элиса и KEM на ее основе, а также приводится классификация атак на кодовые криптосистемы. Во второй главе определены *D*-коды и получены их криптографические свойства. В частности, найдены условия, при которых некоторая степень Шура–Адамара *D*-кода на основе кодов Рида–Маллера разложима в прямую сумму неразложимых кодов. В этой главе также решается задача декодирования *D*-кодов. В качестве гарантированного декодера строится мажоритарный декодер на основе подхода Мэсси. В качестве вероятностных строятся два декодера, использующие блочную структуру кодового слова *D*-кода. В конце главе приведены результаты проведенных экспериментов по оценке эффективности построенных вероятностных декодеров, показывающие их более высокую корректирующую способность относительно гарантированных декодеров. Третья глава посвящена синтезу схемы инкапсуляции сеансового ключа на основе системы типа Мак–Элиса на *D*-кодах на основе кодов Рида–Маллера, а также исследована ее стойкость. Описан алгоритм выделения множеств сильных и слабых ключей системы на *D*-кодах. Для слабых ключей криптосистемы построена комбинированная атака, позволяющая с помощью структурной атаки значительно повысить эффективность атаки на сообщение, и приводится оценка ее эффективности. Для сильных ключей криптосистемы найдены параметры для возможности практического применения. В конце главы проводится сравнение с оригинальной системой на кодах Гоппы при использовании разных подходов к декодированию *D*-кодов.

Полученные результаты являются новыми и представляют несомненный научный и практический интерес, что подтверждается публикацией их в рейтинговых изданиях и докладах на международных конференциях и семинарах по информационной безопасности и криптографии. По теме диссертации опубликовано 9 работ, из которых 3 — в ведущих рецензируемых научных журналах, входящих в перечень ВАК (категории К1), 2 — в научных

рецензируемых изданиях, индексируемых в базе Scopus (Q3, что соответствует категории ВАК К1), 4 — в материалах конференций и других изданиях; также получено свидетельство о государственной регистрации программы для ЭВМ.

Все исследования, описанные Е.А. Лелюком в его диссертационной работе, получены им самостоятельно, научным руководителям (до 2020 г. Евгений выполнял исследование под руководством Деундяка Владимира Михайловича) принадлежит постановка задач и обсуждение полученных результатов. Считаю, что диссертация соответствует паспорту специальности 2.3.6 “Методы и системы защиты информации, информационная безопасность”, а Е.А. Лелюк заслуживает присуждения ученой степени кандидата технических наук.

Сведения о научном руководителе:
Косолапов Юрий Владимирович,
кандидат технических наук (05.13.19 Методы и системы защиты информации, информационная безопасность)
Место работы: Южный федеральный университет
Должность: доцент кафедры алгебры дискретной математики Института математики, механики и компьютерных наук им. И.И. Воровича
Телефон: 8-906-183-30-20
E-mail: yvkosolapov@sfedu.ru

Косолапов Юрий Владимирович

Федеральное государственное автономное образовательное учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Личную подпись Косолапова Ю.В.
ЗАВЕРЯЮ:
Специалист по управлению персоналом 1 категории Волкова Н.С.
«15» ноября 2025 г.

УПРАВЛЕНИЕ ДЕЛАМИ И КАДРОВОЙ РАБОТЫ