ОТЗЫВ

на автореферат диссертации Лелюка Евгения Андреевича, выполненной на тему «Синтез постквантовой схемы инкапсуляции сеансового ключа» и представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Главной задачей исследования, выполненного Е. А. Лелюком, стало выявление и обоснование альтернативных кодовых конструкций для криптосистемы Мак-Элиса. Актуальность данного направления определяется тем, что оригинальная схема на основе кодов Гоппы сохраняет устойчивость к криптоанализу уже почти полвека: известные методы взлома не обладают полиномиальной сложностью, что делает систему привлекательной в качестве базы для постквантового KEM (механизма инкапсуляции сеансового ключа). Однако именно эта устойчивость побуждает исследователей искать уязвимости, поскольку уверенность в надёжности сегодня не исключает появления эффективных атак завтра. Одним из стратегических подходов повышения устойчивости криптографических систем является создание резервных аналогов. В своей работе Е. А. Лелюк реализовал именно такой подход, предложив заменить кодовую основу схемы Мак-Элиса. Такой путь позволяет использовать уже известные оценки стойкости к атакам на открытый шифротекст, независящие от конкретного кода, однако требует, чтобы новый код допускал эффективное декодирование и при этом не повторял структуры, ранее признанные непригодными для построения безопасных криптосистем Мак-Элиса.

В качестве перспективной альтернативы выбрано семейство D-кодов, построенных на базе двоичных кодов Рида–Маллера. Эта постановка потребовала решения трёх взаимосвязанных задач: 1) разработка эффективных алгоритмов декодирования D-кодов; 2) анализ их криптографических характеристик, влияющих на стойкость к атакам на секретный ключ; 3) определение таких параметров кода, при которых обеспечивается высокая криптостойкость схемы в целом. Можно утверждать, что автор успешно справился с поставленными задачами.

Основные научные результаты диссертации:

1. Разработка декодеров для D-кодов.

Создана алгоритмическая реализация мажоритарного декодера, способного гарантированно исправлять ошибки до половины минимального кодового расстояния. Кроме того, предложены два вероятностных декодера, использующих блочную структуру кодовых слов D-кодов и демонстрирующих способность корректировать ошибки за пределами гарантированного радиуса. Это позволило

значительно сократить размер открытого ключа в криптосхеме без потери надёжности.

2. Исследование криптографических свойств D-кодов.

Проанализированы степени Шура–Адамара D-кодов, построенных на основе кодов Рида–Маллера. Установлены условия, при которых такие степени раскладываются в прямую сумму неразложимых подкодов. Показано, что в случае разложимости возрастает вероятность успешной атаки на открытый шифротекст. На этой основе разработана комбинированная атака, снижающая уровень защиты схемы до уровня исходных кодов Рида–Маллера.

3. Обоснование выбора параметров для устойчивой схемы.

С учётом полученных результатов по декодированию и анализу структурных свойств D-кодов предложена методика подбора параметров, обеспечивающих высокую устойчивость как к атакам на ключ, так и на шифротекст. Найдены конкретные параметрические значения, при которых схема на D-кодах демонстрирует меньший объём открытого ключа по сравнению с классической версией на кодах Гоппы, сохраняя при этом сопоставимый уровень стойкости.

Структура диссертации. Работа состоит из введения, трёх глав и заключения.

Первая глава посвящена теоретическим основам: рассматриваются принципы асимметричного шифрования, механизм KEM, ключевые понятия теории кодирования, описание криптосистемы Мак-Элиса и её KEM-версии, а также обзор известных классов атак на кодовые криптосистемы.

Во второй главе вводятся D-коды, изучаются их свойства и проводится анализ разложимости степеней Шура–Адамара. Решается задача декодирования: предлагается мажоритарный декодер на основе алгоритма Паттерсона и два вероятностных декодера, использующих внутреннюю блочную структуру. Приведены экспериментальные данные, подтверждающие превосходство вероятностных методов по корректирующей способности.

Третья глава фокусируется на синтезе и анализе постквантового KEM на основе D-кодов. Разработан алгоритм классификации ключей на «сильные» и «слабые». Для слабых ключей предложена комбинированная атака, сочетающая структурный анализ и декодирование с ошибками, с оценкой её вычислительной эффективности. Для сильных ключей определены практические параметры, обеспечивающие реализуемость схемы. Завершает главу сравнительный анализ с оригинальной системой на кодах Гоппы при различных стратегиях декодирования.

Полученные результаты носят новизну и значимость как для теории кодовой криптографии, так и для практики постквантовой защиты информации. Они опубликованы в 9 научных работах, включая 3 статьи в журналах из перечня ВАК (категория К1), 2 публикации в изданиях, индексируемых в Scopus (Q3, что соответствует категории К1 ВАК), 4 доклада на конференциях, а также свидетельство о государственной регистрации программы для ЭВМ.

Диссертация Лелюка Евгения Андреевича «Синтез постквантовой схемы инкапсуляции сеансового ключа» 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 присуждения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Баранов Владимр Витальевич,
кандидат военных наук 20.01.09, доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова»
кафедра «Информационная безопасность», заведующий кафедрой
346428, Ростовская обл., г.Новочеркасск, ул. Просвещения, 132
baranov.vv.2015@yandex.ru +7 (928)-100-05098

«12» 12 2025 г. _____ / *В.В. Баранов* /

Подпись *кандидат военных наук, доцента Баранова Владимира Витальевича* заверяю
Учёный секретарь
Совета вуза ЮРГПУ(НПИ) _____ Холодкова Нина Николаевна