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»

Актуальность темы диссертационного исследования обусловлена стремительным развитием квантовых вычислительных технологий, создающих угрозу стойкости широко применяемых асимметричных криптосистем, основанных на задачах факторизации и дискретного логарифмирования. В этих условиях переход к постквантовым средствам защиты информации является приоритетным направлением исследований, что подтверждается международными инициативами (конкурс NIST PQC) и отечественными проектами по созданию устойчивых криптографических протоколов. В данном контексте развитие кодовых криптосистем и создание новых схем типа Мак-Элиса на основе эффективно декодируемых кодовых конструкций представляется особенно значимым и своевременным. Таким образом, выбор темы диссертации является полностью обоснованным и отвечает современным потребностям криптографической практики.

Работа содержит существенные теоретические результаты, связанные с исследованием криптографических свойств D-кодов, анализом свойств произведений Шура-Адамара и определением условий разложимости степеней этих кодов. Предложенные автором алгоритмические модели гарантированного и вероятностного декодирования, а также методы анализа стойкости криптосистемы опираются на строгие математические выкладки и представляют интерес для развития теории кодирования и постквантовой криптографии. Полученные результаты расширяют представления о возможностях применения комбинированных кодовых конструкций в криптографических схемах и могут использоваться в дальнейших теоретических исследованиях свойств подкодов тензорных произведений кодов.

Практическая ценность работы подтверждается разработанной и программно реализованной криптосистемой типа Мак-Элиса на D-кодах, демонстрирующей улучшенное соотношение между стойкостью, размером открытого ключа и эффективностью декодирования в сценариях одноразовой инкапсуляции сеансового ключа. Внедрение результатов в деятельность профильных организаций, а также использование в образовательном и исследовательском процессе свидетельствуют о востребованности предложенных решений. Представленные экспериментальные оценки корректирующей способности и временных характеристик декодеров подтверждают применимость разработанных методов в практических задачах защиты информации.

Автореферат выполнен в соответствии с актуальными стандартами научных работ, характеризуется строгой структурой и логичной последовательностью изложения. Представленные результаты исследования содержат необходимый уровень детализации для объективной оценки их теоретической значимости и практической применимости.

В качестве замечания стоит отметить, что в работе недостаточно раскрыт сравнительный анализ предложенной схемы с другими постквантовыми механизмами инкапсуляции ключей, участвовавшими в конкурсе NIST PQC, что позволило бы более полно оценить её положение среди современных KEM и подчеркнуть преимущества и ограничения разработанного подхода.

Данное замечание не влияет на положительную оценку автореферата и диссертационной работы.

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 присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Осипян Валерий Осипович,
доктор физ.-мат. наук, доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики
Профессор каф. анализа данных и искусственно интеллекта
350040, г. Краснодар ул. Ставропольская д. 149
rector@kubsu.ru +7 (861) 219-95-01

«08» 12 2025 г. _____ / В. О. Осипян /

Подпись В. О. Осипяна заверяю

Подлинность подписи Осипяна В. О.
ЗАВЕРЯЮ
Специалист по кадрам Чучупало Ю. А.