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»

Автореферат диссертации Лелюка Евгения Андреевича, посвящённый синтезу постквантовой схемы инкапсуляции сеансового ключа, отражает актуальную для современной криптографии научную задачу, связанную с утратой стойкости классических асимметричных схем под воздействием квантовых алгоритмов, в частности алгоритма Шора для задач факторизации и дискретного логарифмирования. На этом фоне развитие постквантовых механизмов инкапсуляции ключей, в том числе в рамках международных инициатив по стандартизации, а также отечественных проектов, делает выбор направления на кодовые криптосистемы типа Мак-Элиса обоснованным и своевременным. Указание на крупный размер открытого ключа в классической системе на кодах Гоппы и постановка задачи поиска альтернативных эффективно декодируемых кодовых конструкций, в частности D-кодов как обобщения тензорного произведения, свидетельствуют о корректной формулировке исследовательской проблемы и высокой степени её практической значимости.

В работе последовательно решена комплексная научная задача повышения диверсификации эффективных постквантовых схем инкапсуляции сеансового ключа за счёт построения и анализа криптосистемы типа Мак-Элиса на D-кодах на основе двоичных кодов Рида-Маллера. В автореферате чётко сформулированы цели и задачи исследования: от изучения способов замены базового кода в схеме Мак-Элиса и анализа параметров стойкости до выбора перспективной кодовой конструкции, разработки алгоритмов гарантированного и вероятностного декодирования и синтеза новой криптосистемы с описанием её параметров. Существенное место занимает экспериментальная часть: проведён подбор семейств D-кодов, рассчитаны параметры стойкости к атаке декодированием по информационным совокупностям, исследована корректирующая способность и временные характеристики декодеров ISDDecoder и MatrixDecoder для широкого набора кодов, что позволяет количественно оценить полученный выигрыш по размеру ключа и стойкости относительно оригинальной схемы Мак-Элиса.

Теоретическая и практическая значимость диссертационной работы определяется развитием аппарата исследования D-кодов на основе кодов Рида-Маллера, получением новых результатов о свойствах произведения Шура-Адамара и условиях разложимости, а также предложением критериев выделения сильных и слабых ключей криптосистемы типа Мак-Элиса. Построенная и программно реализованная криптосистема типа Мак-Элиса на D-кодах и соответствующие алгоритмы мажоритарного и вероятностного декодирования обеспечивают улучшенное соотношение между стойкостью, размером открытого ключа и эффективностью декодирования по сравнению с классическими решениями и могут быть использованы при построении постквантовых механизмов инкапсуляции ключей. Внедрение результатов в деятельность профильных организаций и их использование в учебно-исследовательском процессе подтверждают востребованность разработанных методов и их прикладную значимость для задач 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 можно указать, что при анализе стойкости к атакам на шифрограмму в работе используется классический вариант декодирования по информационным совокупностям, тогда как не рассмотрены более современные и эффективные модификации данного подхода, разработанные в последние годы. Учет таких алгоритмов позволил бы получить более актуальные оценки криптостойкости предложенной схемы.

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.

Лепешкин Олег Михайлович, доктор технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гидрометеорологический университет», г. Санкт-Петербург заведующий кафедрой «Информационных технологий и систем безопасности».

195196, Россия, Санкт-Петербург, проспект Металлистов, дом 3.
lepechkin1@yandex.ru, тел. +79052851649.

«08» 12 2025 г. _____ / О. М. Лепешкин /

Подпись О. М. Лепешкина заверяю

Нач. управления кадров Лаптева Л.В.