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»

Развитие квантовых вычислений ставит под угрозу стойкость широко применяемых асимметричных криптосистем, основанных на задачах факторизации и дискретного логарифмирования. Показано, что эти задачи могут быть эффективно решены на квантовом компьютере с использованием алгоритма Шора, что приводит к необходимости перехода к криптографическим схемам, устойчивым в постквантовую эпоху. Международные инициативы – такие как конкурс NIST PQC, корейский KpqC и работы российских профильных технических комитетов – подтверждают высокую значимость разработки новых постквантовых механизмов защиты данных.

Одним из перспективных направлений остаются кодовые криптосистемы типа Мак-Элиса, основанные на сложности задачи декодирования случайного линейного кода. Однако существующие протоколы, включая системы Original McEliece и Classic McEliece, основанные на кодах Гоппы, характеризуются большими размерами ключей, а также потенциальной уязвимостью к будущим структурным атакам. Как показывает развитие криптоанализа, в некоторых классах альтернантных кодов уже найдены эффективные структурные атаки, что создаёт риск для дальнейшего применения таких систем

В связи с этим актуальной является задача разработки новых классов эффективно декодируемых помехоустойчивых кодов, позволяющих создавать более компактные и устойчивые кодовые криптосистемы. Одним из перспективных направлений является применение кодовых конструкций – таких как тензорные произведения и суммы тензорных произведений – которые позволяют формировать новые коды с иной структурой, уменьшая риск успешных структурных атак.

В диссертационной работе получен комплекс значимых теоретических и прикладных результатов, направленных на создание новой кодовой криптосистемы типа Мак-Элиса на основе D-кодов. К наиболее существенным результатам относятся:

- Алгоритмическая модель гарантированного мажоритарного декодирования для D-кодов, позволяющая исправлять ошибки до половины кодового расстояния.
- Два вероятностных декодера, обеспечивающих исправление ошибок сверх половины кодового расстояния и позволяющих уменьшить размер открытого ключа в криптосистеме типа Мак-Элиса.
- Автор получил условия разложимости и неразложимости степеней произведения Шура-Адамара D-кодов, что позволяет определять уязвимые и стойкие классы кодов. Установленные свойства позволяют аналитически выявлять сильные и слабые ключи, что важно для обеспечения стойкости криптосистемы.
- На основе разработанных декодеров и исследованных криптографических свойств построена новая асимметричная криптосистема типа Мак-Элиса, обеспечивающая снижение размера открытого ключа или повышение стойкости при сопоставимых параметрах по сравнению с оригинальной криптосистемой Мак-Элиса.

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.

По содержанию автореферата можно указать на отдельные недостатки работы:

1. Вероятностные схемы декодирования обладают ненулевой вероятностью ошибки DFR. В диссертации приведены только экспериментальные оценки DFR, однако аналитические оценки или строгие границы могли бы усилить теоретическую значимость результатов.

2. В работе при экспериментальной оценке эффективности вероятностных декодеров используется базовая, не оптимизированная реализация алгоритмов. Автор отмечает потенциальные направления для ускорения и улучшения этих реализаций, однако данные оптимизации фактически не применены и их влияние на производительность декодеров не исследовано. Такие результаты были бы полезными для более точного сравнения с существующими схемами.

Отмеченные недостатки не относятся к вопросам, выносимым на защиту, и не влияют 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.

Сафарьян Ольга Александровна
Кандидат технических наук 2.2.13. «Радиотехника, в том числе системы и устройства телевидения», доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»
Кафедра «Кибербезопасность информационных систем», заведующий кафедрой
344000, г. Ростов-на-Дону, пл. Гагарина, д. 1
spu-46.2@donstu.ru тел. 8(863)2-381-518

«24» ноября 2025 г. _____ / О. А. Сафарьян /

Подпись О. А. Сафарьян заверяю

Начальник управления кадров
О. И. Костина
«19» 11 2025

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)
УПРАВЛЕНИЕ КАДРОВ