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»

В 1994 г. Шор опубликовал два алгоритма для квантовых компьютеров, которые эффективно решают две важнейшие задачи современной криптографии: задачи дискретного логарифмирования и факторизации целых чисел. Шор, в частности, предложил квантовый алгоритм, который позволяет за полиномиальное от $log\ N$ число операций разложить натуральное число N на множители. Это значит, что за полиномиальное от длины числа N число операций можно решить задачу факторизации. С техническим прогрессом в создании мощных квантовых компьютеров основные криптографические схемы, такие как RSA и криптосистемы на эллиптических кривых, становятся все более уязвимыми. В 1978 г. Мак-Элис построил первую кодовую криптосистему с открытым ключом, которая основана на применении помехоустойчивых кодов. При этом эффективные атаки на секретные ключи этой криптосистемы до сих пор не найдены. Рассматриваемая работа посвящена исследованию криптосистем с открытым ключом на основе помехоустойчивых кодов. Поэтому направление исследования является актуальным.

Проведенное исследование демонстрирует комплексный и системный подход к решению поставленной задачи. Автором получены весомые научно-практические результаты, которые вносят значимый вклад в область постквантовой криптографии. Теоретическая глубина работы подтверждается разработанными алгоритмическими моделями и проведенным криптографическим анализом, а практическая ценность – найденными параметрами криптосистемы, обеспечивающими конкурентоспособные характеристики.

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.

Большая часть современной криптографии основана на (недоказанных) предположениях. Это особенно актуально, когда речь идет о вычислительной безопасности. Например, в качестве предположения может выступать предположение о вычислительной сложности задачи обучения с ошибками (LWE) из теории решеток. В качестве замечания к работе отметим, что не сформулировано в явном виде криптографическое предположение, на основе которого рассматриваются криптосистемы с открытыми ключами.

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

Диссертационная работа 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.

Рацеев Сергей Михайлович,
доктор физико-математических наук
(специальность 01.01.06 – математическая логика, алгебра и теория чисел),
доцент,
профессор кафедры информационной безопасности и теории управления,
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский государственный университет»,
432017, Российская Федерация, город Ульяновск, улица Льва Толстого, дом 42,
e-mail: ratseevsm@mail.ru,
тел. (8422) 37-24-73.

«20» 11 2025 г. / С. М. Рацеев /

Подпись С. М. Рацеева заверяю

УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Подпись С.М. Рацеева
«ЗАВЕРЯЮ»
Ученый секретарь
Ученого совета УлГУ О.А. Литвинко
20 г.