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»

Исследование криптографических схем, стойких к атакам с использованием квантового компьютера, в настоящее время является актуальной задачей. Это подтверждается продолжающимися процессами стандартизации постквантовых криптографических алгоритмов. В работе рассматриваются кодовые криптосистемы как один из перспективных методов построения постквантовых систем. Действительно, криптосистемы типа Мак-Элиса являются одним из наиболее популярных подходов к построению постквантовых схем. Для оригинальной системы, использующей коды Гоппы, до сих пор не найдено эффективных алгоритмов структурных атак. Однако, эта система также обладает недостатком в виде большого размера открытого ключа. В попытке преодолеть этот и другие ограничения оригинальной криптосистемы, в работе предполагается использовать другие помехоустойчивые коды. В частности, предлагается использовать D-коды – класс кодовых конструкций, обобщающий конструкцию тензорного произведения кодов. Таким образом, представленная работа посвящена решению важной научной задачи.

Результаты исследования включают разработку новых методов декодирования D-кодов, в том числе гарантированных и вероятностных декодеров, опирающихся на особенности внутренней структуры таких кодов. Проведён анализ стойкости построенной криптосистемы с использованием произведения Шура-Адамара. На базе полученных результатов предложена новая схема инкапсуляции, демонстрирующая улучшенное соотношение между стойкостью и размером открытого ключа по сравнению с оригинальной системой на кодах Гоппы.

Автореферат написан научным языком, выдержанным в соответствии с требованиями к диссертационным работам. Структура документа логична: постановка задачи, анализ существующих решений, изложение предложенного подхода, описание результатов и заключение. Материал изложен последовательно, с достаточной детализацией, позволяющей оценить научную и практическую значимость работы.

По содержанию автореферата можно указать на отдельные недостатки работы:

- Аббревиатура KEM (key encapsulation mechanism) в тексте автореферата переводится по-разному — как «схема», «протокол» и «механизм». Во избежание разночтений рекомендуется использовать терминологию согласно ПНСТ 799-2022.
- При определении стойкости кодовых криптосистем против ISD атак для более точной оценки целесообразно использовать наиболее эффективный алгоритм данного класса, например, алгоритм Босса-Мэя.
- Время работы алгоритма ISD в некоторых таблицах приводится в виде степени двойки, а в других – в экспоненциальной записи. Для улучшения читаемости рекомендуется использовать однообразный вариант записи.

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

Турченко Олег Юрьевич,
Кандидат технических наук
по специальности 2.3.6
«Методы и системы защиты информации,
информационная безопасность»
Общество с ограниченной ответственностью «КуАпп»
Старший исследователь-криптограф
121205, город Москва, б-р Большой (Инновационного Центра Сколково Тер), д. 30 стр. 1, эт. 3 пом. 33 рб. 33-1
oturchenko@qapp.tech
+7-951-495-46-75

«03» октября 2025 г. _____ / О. Ю. Турченко /

Подпись О. Ю. Турченко заверяю

Генеральный директор ООО "КуАпп"
Гугля А. П.