Отзыв на автореферат диссертации
Лелюка Евгения Андреевича
“Синтез постквантовой схемы инкапсуляции сеансового ключа”, представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 “Методы и системы защиты информации, информационная безопасность”

Введение. Автореферат посвящён разработке эффективных и стойких к квантовым атакам постквантовых схем инкапсуляции сеансового ключа, основанных на кодовых криптосистемах. Работа выполнена на высоком научном уровне, обладает актуальностью и научной новизной.

Актуальность исследования. В условиях появления квантовых вычислений классические асимметричные криптосистемы, основанные на факторизации и дискретном логарифмировании, становятся уязвимыми.

Автор справедливо подчеркивает, что криптосистемы типа Мак–Элиса — один из немногих проверенных подходов к построению постквантовых алгоритмов, но они обладают рядом ограничений: большими открытыми ключами и возможностью появления структурных атак на некоторые семейства кодов.

Исследование новых кодовых конструкций, в частности D-кодов, представляется важной научной задачей, имеющей прямое прикладное значение. Особенно это актуально в контексте продолжающегося как в России (ТК 26), так и в мире (ISO) процесса стандартизации постквантовых криптографических механизмов.

Научная новизна. В работе получены следующие новые результаты:

1. Разработаны алгоритмы гарантированного и вероятностного декодирования *D*-кодов, включая мажоритарный декодер и два типа вероятностных декодеров на основе информационных совокупностей и матричного представления кодового слова.
2. Предложен алгоритм выделения сильных и слабых ключей криптосистемы на основе анализа свойств произведения Шура–Адамара *D*-кодов.
3. Разработана комбинированная атака на слабые ключи, эффективно использующая структурные свойства кода для повышения вероятности успеха атаки на шифрограмму.
4. Синтезирована и исследована новая постквантовая криптосистема типа Мак–Элиса на *D*-кодах, обладающая улучшенным соотношением между стойкостью, скоростью и размером открытого ключа.

Все перечисленные результаты являются оригинальными и имеют существенную теоретическую и практическую ценность.

Теоретическая значимость работы. Полученные автором результаты по свойствам произведения Шура–Адамара *D*-кодов на основе базовых кодов Рида–Маллера расширяют существующие представления о структуре таких кодов и могут быть использованы

при построении новых семейств постквантовых криптосистем, а также при анализе их устойчивости к структурным атакам.

Разработанные алгоритмы декодирования представляют ценность для теории кодирования, особенно в задачах декодирования кодов, получающихся комбинированием других кодов.

Практическая значимость. Практическая ценность работы подтверждена программной реализацией декодеров и экспериментальным анализом эффективности предложенной схемы. Приведенные в работе результаты внедрены в профильных организациях, занимающихся разработкой криптографических алгоритмов и защищенных систем связи, что указывает на востребованность предложенных решений.

Разработанная криптосистема позволяет либо уменьшить размер открытого ключа при сохранении уровня стойкости, либо повысить стойкость при сопоставимых параметрах — по сравнению с классической системой `Classic McEliece` на кодах Гоппы.

Стиль и структура автореферата. Автореферат написан грамотным научным языком, результаты изложены ясно, структура соответствует требованиям ВАК. Таблицы и экспериментальные данные позволяют объективно оценить предложенные алгоритмы, а также параметры криптосистемы.

Замечания. К работе у рецензента имеются следующие замечания:

1. В работе можно было бы подробнее осветить сравнение не только с современными реализациями `Classic McEliece`, но и с KEM `PALOMA`, представленной в корейском конкурсе KpqC.
2. Желательно было бы расширить интерпретацию теорем 1–4 из второй главы. Из текста автореферата не ясна их ценность и значимость.
3. В диссертации изучается стойкость построенной криптосистемы относительно комбинированной атаки, предложенной автором, и общей атаки декодирования с использованием информационных множеств. Вместе с тем следовало бы обсудить применимость атак, построенных для криптосистемы Мак-Элиса на кодах Рида–Маллера, а также иных возможных структурных атак.
4. Иногда в автореферате предложение начинается с формулы, что затрудняет чтение текста.
5. Рецензенту кажется неудачным выбранное обозначение дуального кода как код с чертой ($\overline{C}$). Оно крайне затрудняет восприятие текста и понимание сути теорем.
6. В таблице 7 было бы лучше использовать не значение вероятности успеха декодирования по информационным совокупностям, а двоичный логарифм от этой вероятности.

Эти замечания носят уточняющий характер и не влияют на общую высокую оценку исследования.

Заключение. Диссертационная работа Е. А. Лелюка является законченной научно-исследовательской работой, в которой решена актуальная задача синтеза эффективной постквантовой схемы инкапсуляции сеансового ключа.

Считаю, что полученные результаты обладают научной новизной, теоретической и практической значимостью и соответствуют требованиям, предъявляемым к кандидатским диссертациям по специальности 2.3.6 “Методы и системы защиты информации, информационная безопасность”.

Автор заслуживает присуждения ученой степени кандидата технических наук.

Рецензент:
доцент кафедры информационной безопасности
ВМК МГУ имени М.В.Ломоносова
канд. физ.-мат. наук Чижов И.В.

24.11.2025 г.

Контактные данные.

ФИО: Чижов Иван Владимирович.

Ученая степень: кандидат физико-математических наук.

E-mail: chizhoviv@my.msu.ru, тел.: 8(495)930-43-76 (раб.).

Специальность, по которой И.В. Чижовым была защищена кандидатская диссертация: 05.13.19 — “Методы и системы защиты информации, информационная безопасность” (физико-математические науки).

Место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования “Московский государственный университет имени М.В.Ломоносова”, факультет вычислительной математики и кибернетики, кафедра информационной безопасности.

Адрес места работы: 119234, Москва, Ленинские горы, дом 1, стр. 52, 2-й учебный корпус.

Должность: доцент кафедры информационной безопасности.

Подпись Чижова Ивана Владимировича удостоверяю:

Декан факультета
ВМК МГУ имени М.В. Ломоносова
академик Соколов И.А.