

ОТЗЫВ
на автореферат диссертации
Высоцкой Виктории Владимировны
«Анализ постквантовых схем электронной подписи,
построенных на кодах, исправляющих ошибки»,
представленной на соискание
ученой степени кандидата физико-математических наук
по специальности 2.3.6 – «Методы и системы защиты информации,
информационная безопасность»

Ожидаемое создание квантового вычислителя достаточной мощности является угрозой для традиционных асимметричных криптографических механизмов, стойкость которых основана на задачах из теории чисел. Угроза связана с реализацией квантового алгоритма Шора, который может раскладывать числа на простые множители и решать задачу дискретного логарифмирования за полиномиальное время. Ответом на эту угрозу является развитие так называемых постквантовых криптографических механизмов, взлом которых, как предполагается, невозможен за полиномиальное время даже на квантовом вычислителе. К числу таковых, в частности, относят механизмы, стойкость которых связана со сложностью решения задач из теории корректирующих кодов, некоторые из которых являются NP-трудными, что позволяет предположить и высокую трудоемкость взлома самого механизма. С учетом сказанного тема и содержание диссертационной работы являются актуальными как в теоретическом, так и в практическом смысле. Дополнительную актуальность работе придает необходимость опережающей (до появления квантового вычислителя) стандартизации асимметричных криптосхем в национальной системе стандартизации.

Диссертационная работа Высоцкой В.В. решает задачу анализа существующих подходов к построению схем цифровой подписи и построения схемы, стойкость которой не зависит от структуры (класса) используемых кодов.

В работе рассмотрены свойства схем подписи на основе подкодов кодов Рида-Маллера порядка g и получена оценка доли подкодов, дающих предположительно стойкую схему по отношению к методам анализа, основанных на квадрате Адамара кода. Также исследованы свойства конкатенированных кодов – подход Сидельникова – для получения оценок мощности множества открытых ключей и описания структуры секретных ключей.

Синтезная часть работы представлена схемой подписи, базирующейся на протоколе идентификации Штерна. Предложенная конструкция преодолевает проблему структурности, т.е. определенной регулярности используемых кодов, которая может давать нестойкие варианты схем. Отметим отдельно, что синтезированная в работе схема цифровой подписи рассматривается как кандидат для стандартизации в Российской Федерации.

Автореферат диссертации хорошо структурирован, позволяет сделать вывод о научной новизне результатов, их теоретической и практической значимости. Результаты диссертации опубликованы в 5 статьях, 4 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Отметим, однако, что в тексте автореферата не приведен ни один численный пример, позволяющих соотнести уровень стойкости схем подписи с их эксплуатационными характеристиками. Это, впрочем, не снижает научной ценности полученных результатов, в предположении, что такие формулы приведены в тексте диссертации.

Считаю, что автореферат диссертации и процитированные публикации по уровню выполнения, новизне и актуальности в полной мере характеризуют соответствие диссертации критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова для диссертаций на соискание ученой степени

кандидата наук, а ее автор, Высоцкая Виктория Владимировна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Кандидат физико-математических наук,
заместитель генерального директора АО «ИнфоТеКС»
по науке и инновациям

Уривский А.В.

«18» ноября 2025 г.

Контактные данные:

тел.:

e-mail: urivskiy@infotecs.ru

Адрес места работы:

127273, Москва, ул. Отрадная, д. 2Б, стр. 1

Я, Уривский Алексей Викторович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

Подпись Уривского А.В. удостоверяю

Начальник отдела кадров АО «ИнфоТеКС»

Продан А.М.