ОТЗЫВ официального оппонента
на диссертацию на соискание ученой степени
кандидата физико-математических наук
Высоцкой Виктории Владимировны

на тему: «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки»
по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы диссертации.

Сегодня актуальность постквантовой криптографии уступает только актуальности ИИ. Так в популярном прогнозе 10 главных стратегических технологических трендов Gartner на 2025 год (https://www.gartner.com/en/articles/top-technology-trends-2025) тренд постквантовой криптографии идет вторым, после агентного ИИ.

Это связано с тем, что большинство используемых криптографических систем базируются на некоторых задачах из теории чисел и теории конечных полей, которые могут быть решены, а соответствующие криптографические системы будут сломаны, при появлении достаточно надежного и большого (по числу кубитов) квантового компьютера, а прогресс в этом направлении идет очень быстрый.

И если в области собственно постквантового шифрования достигнут значительный прогресс и даже рекомендованы соответствующие проекты стандартов, то в области так называемой электронной подписи еще нет такой ясности. Поэтому актуальность темы диссертации, посвященной исследованию различных схем электронной подписи, базирующихся на кодах с исправлением ошибок, несомненна.

Степень обоснованности положений, выносимых на защиту, научных выводов и рекомендаций, сформулированных в диссертации

Все положения выносимые на защиту, строго обоснованы и доказаны.

Отмечу, что работа с аппаратом линейной алгебры над конечными кольцами не так проста, как может показаться. Например, как правильно отмечает диссертант, алгоритм Гаусса не всегда приводит матрицу к треугольному виду над кольцом с делителями нуля, так как в обратимой матрице все её элементы могут быть необратимыми элементами кольца, см. соответствующий пример на стр.80 диссертации.

Достоверность и новизна полученных научных результатов, выводов и рекомендаций.

Достоверность полученных результатов основывается на строгих математических доказательствах всех утверждений, выносимых диссертантом на защиту, а также публикацией в журналах, по тематике диссертации, и аппробацией на научных конференциях и семинарах.

Все основные результаты полно отражены в четырех статьях, опубликованных в рецензируемых периодических научных изданиях, индексируемых в базе ядра Российского индекса научного цитирования.

Все вынесенные на защиту результаты являются новыми, впервые полученные автором диссертации. Среди них особенно отмечу результаты второй главы, получение которых потребовало применения довольно тонкой техники как линейной алгебры над конечными кольцами, так и теории вероятностей. Также отмечу новую схему электронной (я предпочитаю говорить - цифровой) подписи, разработанную и исследованную в четвертой главе.

Замечания по диссертации.

Автор диссертации допускает пару неточностей при классификации сложности некоторых задач теории кодирования. А именно, известно, что задача декодирования линейного кода по минимуму расстояния является NP-полной и автор правильно указывает на работу [6] E. Berlekamp, R. McEliece and H. van Tilborg, "On the inherent intractability of certain coding problems (Corresp.)," in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978, doi: 10.1109/TIT.1978.1055873, где это впервые было доказано. Однако затем автор пишет (стр.33) «Работа [6] показала, что это же верно для задачи CF». Задача CF известна как задача о вычислении минимального расстояния линейного кода и ее сложность оставалась неизвестной еще 20 лет после работы [6], и NP-полнота была доказана в A. Vardy. The intractability of computing the minimum distance of a code. IEEE Transactions on Information Theory, 43(6):1757–1766, Nov. 1997. Для полноты картину отмечу, что даже приближенное вычисление расстояния кода тоже NP-полная задача, см. I. Dumer, D. Micciancio and M. Sudan, "Hardness of approximating the minimum distance of a linear code," in IEEE Transactions on Information Theory, vol. 49, no. 1, pp. 22-37, Jan. 2003, doi: 10.1109/TIT.2002.806118.

Вывод

Указанные замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, а именно, направлениям:

11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Содержание диссертации также отвечает критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова. Диссертационное исследование оформлено согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Высоцкая Виктория Владимировна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

доктор физико-математических наук,
вице-президент по науке и академическому сотрудничеству
Сколковского института науки и технологии

Кабатянский Григорий Анатольевич

11.11.2025

Подпись Кабатянского Г.А. подтверждаю
Руководитель отдела кадрового администрирования
Гук О.С.

Контактные данные:

тел.: , e-mail: g.kabatyansky@skoltech.ru
Специальность, по которой официальным оппонентом
защищена диссертация: 05.13.17 - Теоретические основы информатики

Адрес места работы:

121205, г. Москва, территория инновационного центра «Сколково», Большой бульвар, д. 30 стр.1 Сколтех, ректорат