ОТЗЫВ официального оппонента
на диссертацию на соискание ученой степени
кандидата 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

Синтез криптографических схем традиционно осуществляется на основе классических моделей вычислений и с учетом возможных атак, которым они могут подвергаться. При анализе уязвимостей важно точно формулировать модель нарушителя, в частности его вычислительные ресурсы и допустимое время на проведение атаки, поскольку именно от этого зависит ее практическая реализуемость. Стойкой считается та схема, решение которой занимает время, превышающее некоторый обозначенный порог. Обычно оно выбирается с запасом и исчисляется миллионами лет на классическом вычислителе. С ростом вычислительных возможностей персональных компьютеров и появлением суперкомпьютеров приходится корректировать параметры, задающие схему, так, чтобы стойкость осталась прежней.

Ситуация кардинально изменилась с появлением концепции квантового компьютера, оперирующего не битами, а кубитами, и способного эффективно решать целый класс задач, ранее считавшихся вычислительно сложными. Так, согласно результатам Питера Шора 1994 года, задачи факторизации и дискретного логарифмирования могут быть решены на квантовом компьютере за полиномиальное время относительно длины входа. И именно эти задачи лежат в основе стойкости большинства современных криптографических схем с открытым ключом, к которым относятся, в том числе, схемы электронной подписи.

Несмотря на то, что создание реального квантового компьютера, способного реализовать такие атаки, еще не завершено, и нет полной уверенности в том, что это произойдет в обозримом будущем, крупные

технологические компании (IBM, Google, Microsoft и др.) ежегодно демонстрируют прогресс в наращивании квантовой мощности и даже предоставляют облачный доступ к экспериментальным квантовым вычислительным системам. Необходимость применения постквантовой криптографии была подчеркнута в выступлении директора ФСБ России А.В.Бортникова на совещании Совета глав спецслужб СНГ в Самарканде в октябре 2025 года, где было прямо указано на риски, связанные со ставкой западных стран на развитие квантовых вычислений.

Диссертационная работа Высоцкой Виктории Владимировны посвящена исследованию альтернативной основы построения электронных подписей: кодов, исправляющих ошибки. Для задач на кодах пока не предложено эффективного алгоритма решения на квантовом вычислителе, при этом коды лежат в основе ряда схем электронной подписи. В диссертационной работе рассматриваются подписи на основе задачи синдромного декодирования, оригинальная версия которой принимает на вход линейный код без выделенной структуры. Про такую задачу еще в 1978 году было показано, что она является NP-полной как задача распознавания.

Преимущественно в работе рассматриваются электронные подписи, основанные на структурированных линейных кодах. Наличие структуры необходимо для построения некоторых схем, однако оно может одновременно приводить к появлению уязвимостей и не позволяет напрямую перенести на такие конструкции известные результаты о NP-сложности. В связи с этим в диссертации ставится задача анализа стойкости подписей на кодах такого типа. Также некоторые варианты схем рассматриваются с точки зрения вычислительной эффективности. В заключительной части работы представлена электронная подпись, основанная на оригинальной постановке задачи синдромного декодирования.

Научная новизна результатов диссертации

Результаты диссертационной работы заключаются в исследовании известной схемы электронной подписи CFS с заменой базовых кодов на

специально выбранные классы. Такие сочетания схемы подписи и используемых кодов рассматриваются впервые. Мотивация выбора каждого класса кодов подробно обоснована во введении и соответствующих разделах диссертации. Для выбранных классов кодов автором предложены математически обоснованные рекомендации по построению ключей подписи.

Кроме того, к числу полностью новых результатов относится разработка альтернативной схемы электронной подписи с теоретическим обоснованием ее стойкости.

Обоснованность и достоверность результатов диссертации

Математические утверждения, содержащиеся в работе, снабжены полными доказательствами. Результаты работы изложены в 5 публикациях, из них 4 работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (ведущие отечественные издания --- журналы «Дискретная математика» и «Прикладная дискретная математика»), индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index». Результаты работы апробированы на международных конференциях и научных семинарах.

Замечания к диссертации

1. Алгоритмы, каждый из которых занимает половину страницы диссертации, было бы лучше вынести в приложение, а в тексте упоминать по номеру приложения. В процессе чтения работы записанные на формальном языке алгоритмы не смотрятся без необходимости.

2. Рассуждения о слабой применимости алгоритма Шенхаге-Штрассена в начале Главы 2 (ссылка на литературу [78]) выглядят скомканными, а потому лишними.

3. В ряде случаев сложноподчиненные предложения для упрощения понимания следовало бы разбить на два или же поменять местами начало и

конец предложения. В этом случае полученные логические конструкции выглядели бы более стандартными.

Заключение

Считаю, что диссертация Высоцкой Виктории Владимировны соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, а именно следующим ее 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.

Замечания к диссертации не являются существенными и не влияют на положительную оценку значимости результатов проведенного исследования. Диссертация отвечает всем требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (по физико-математическим наукам), а также 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, на основании всего вышеизложенного, считаю, что 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:

Профессор, доктор физико-математических наук,
профессор кафедры математической кибернетики
факультета вычислительной математики и кибернетики
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный университет имени М.В.Ломоносова»

Вороненко Андрей Анатольевич 23.10.2025

Контактные данные:

тел.: 7(495)9393010, e-mail: dm6@cs.msu.ru
Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.09 – Дискретная математика и кибернетика

Адрес места работы:

119991, Москва, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус
МГУ имени М.В. Ломоносова, факультет вычислительной математики и кибернетики
Тел.: 7(495)9393010; e-mail: dm6@cs.msu.ru

Подпись сотрудника факультета ВМК МГУ
Московского государственного университета имени М.В. Ломоносова
Вороненко Андрея Анатольевича удостоверяю:

Декан факультета ВМК МГУ,
Академик РАН И.А.Соколов