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

Современные широко применяемые криптографические схемы с открытым ключом основаны на нескольких задачах, таких как факторизация целых чисел и вычисление дискретного логарифма. Вычислительная сложность этих задач не имеет строгого обоснования, однако все известные классические алгоритмы их решения характеризуются экспоненциальной вычислительной сложностью.

В 1994 году Питер Шор предложил квантовые алгоритмы, позволяющие решать обе эти задачи за полиномиальное время. Первоначально эти алгоритмы имели чисто теоретический характер, но с развитием квантовых вычислительных технологий стали практически реализуемыми для малых параметров. Это делает очевидной необходимость разработки криптографических систем, устойчивых к атакам с использованием квантового компьютера.

Диссертационная работа Высоцкой В.В. посвящена построению схем электронной подписи, стойкость которых не снижается под действием атак Шора.

Первая группа подписей использует идею Николя Куртуа, Мэттью Финиаша и Николаса Сендрие. В 2001 году они предложили подпись, известную сейчас как подпись CFS, использующую как основу схему шифрования Мак-Элиса (и ее двойственную версию, схему Нидеррайтера). Для генерации подписи сообщение предлагается «расшифровать» так, как

если бы оно было шифртекстом относительно выбранного семейства кодов, а для проверки подписи происходит шифрование подписи. Оригинальная версия схемы использовала коды Гоппы, однако полученные для них параметры оказались непрактичными с точки зрения времени работы схемы. Это стимулировало появление множества модификаций подписи CFS на основе других классов кодов. У некоторые из них оказались хорошие эксплуатационные характеристики, но впоследствии они были атакованы, тогда как другие до сих пор не исследованы в полной мере.

В диссертационной работе Высоцкая В.В. анализирует вопросы стойкости и эффективности построения схемы подписи CFS на квазициклических кодах, подкодах кодов Рида-Маллера и последовательно соединенных кодах Рида-Соломона.

Вторая группа подписей, рассмотренная в работе, основана на применении идеи Фиата-Шамира, которая позволяет преобразовать интерактивный протокол идентификации в схему подписи. В качестве такого протокола выбрана схема Штерна, построенная на кодах, исправляющих ошибки.

Научная новизна, обоснованность и достоверность результатов диссертации

Глава 1 диссертационной работы содержит анализ стойкости схемы CFS на кодах, полученных из кодов Рида-Маллера исключением некоторого количества базовых векторов. Описаны структурные свойства этих кодов, обеспечивающих устойчивость схемы подписи к известным атакам. Также определена доля таких кодов.

Глава 2 посвящена алгоритмам построения случайной невырожденной квазициклической матрицы, которая требуется в алгоритме генерации ключей схемы подписи CFS на квазициклических кодах. Параллельно с построением

таких алгоритмов исследуются алгоритмы, работающие в факторкольцах кольца многочленов.

Глава 3 анализирует стойкость схемы подписи CFS, ключи которой задаются двумя копиями одного и того же кода. Часть результатов получена для линейных кодов, не имеющих фиксированной структуры, а уточненные результаты приведены для обобщенных кодов Рида-Соломона. Предложены три новых класса ключей схемы подписи на основе обобщенных кодов Рида-Соломона, делающих ее стойкой к известным атакам.

В Главе 4 предлагается новый подход к построению схемы электронной подписи на основе кодов, исправляющих ошибки. Такая подпись не требует наличия у кода эффективного алгоритма декодирования, поэтому может быть построена на случайном линейном коде. Это исключает возможность построения структурных атак. Помимо этого, диссертационная работа содержит обоснование стойкости схемы в релевантной для подписи модели.

Всем утверждениям и теоремам, содержащимся в работе, даны строгие доказательства.

Ее результаты опубликованы автором в рецензируемых изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index».

Замечания к диссертации

1. Не до конца понятна логика расположения глав диссертации. Глава 2 содержит анализ эффективности схемы подписи, в то время как Главы 1, 3 и 4 в основном исследуют стойкость. Логичнее было бы отделить Главу 2, например, поставив ее в начало работы.

2. В Главе 1 содержится Алгоритм 1, описание которого приведено в Приложении А. Утверждается, что этот алгоритм улучшает теоретически

обоснованную верхнюю оценку, приведенную в Теореме 4. Однако работа алгоритма проиллюстрирована лишь на одном примере, на Рис. 1.3, для частного случая полиномов степени 5. Хотелось бы, чтобы работа включала более подробный анализ алгоритма, доказывающий его превосходство для полиномов произвольной степени.

Заключение

Считаю, что диссертация Высоцкой В.В. соответствует 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.

Указанные выше замечания не умаляют значимости диссертационного исследования. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М. В. Ломоносова к работам подобного рода. Ее содержание соответствует 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. Диссертация оформлена 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.

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,
профессор кафедры дискретной математики
механико-математического факультета
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный университет имени М.В. Ломоносова»

Гашков Сергей Борисович

Контактные данные:

тел.: 7(495)9394268, e-mail: sbgashkov@gmail.com
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, д.1, Главное здание
МГУ имени М.В. Ломоносова, механико-математический факультет
Тел.: 7(495)9394268; e-mail: sergey.gashkov@math.msu.ru

Подпись сотрудника механико-математического факультета
Московского государственного университета имени М.В. Ломоносова
Гашкова Сергей Борисовича удостоверяю: