ОТЗЫВ

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

Постквантовая криптография является одним из самых актуальных и обсуждаемых направлений в современной криптографии. Разработка систем постквантовой криптографии, то есть систем, стойких по отношению к атакам с использованием гипотетического квантового компьютера, ведется международным сообществом в рамках американского конкурса NIST PQ, южнокорейского конкурса KpqC, международной организации ISO и российской организации ТК26.

Исследования проводятся по двум направлениям: построение протоколов инкапсуляции ключа (и, в качестве составной части, схемы шифрования с открытым ключом), а также построение схем электронной подписи. Результаты исследований должны обеспечить создание и применение асимметричных систем, способных заменить современные асимметричные системы в тот момент, когда квантовые компьютеры достигнут достаточно большой вычислительной мощности.

В диссертационной работе Высоцкой В.В., согласно представленному тексту автореферата, рассмотрены подходы к достижению сформулированной выше цели, которые базируются на применении кодов, исправляющих ошибки.

Актуальность исследований по этому направлению сохраняется, несмотря на достаточное количество предложенных вариантов схем, выдвинутых в рамках каждой из перечисленных организаций, и в литературе в целом. До настоящего времени ни одна схема подписи на кодах не принята окончательно для стандартизации.

В автореферате, в разделе с общей характеристикой работы, последовательно изложено развитие этого направления от первых основополагающих работ до настоящего времени.

В первой главе диссертации, согласно автореферату, изучается вопрос о порождении подкодов, потенциально применимых для построения криптографически стойких схем. В частности, показано, что при случайной генерации доля «хороших» подкодов стремится к нулю. Вместе с тем предложен конструктивный способ генерации так называемых нестабильных подкодов, которые гипотетически могут быть использованы при синтезе стойких схем.

Во второй главе, в рамках основной задачи, исследуется построение квазициклических кодов, которые эффективны в практических реализациях. Автору удалось построить алгоритм генерации невырожденных квазициклических матриц через их представление в форме матрицы многочленов и получить практически удовлетворительные оценки трудоемкости этого алгоритма.

В третьей главе анализируются возможности построения схем на основе конструкции В.М. Сидельникова. Возможные атаки на них связаны со свойством, является ли код кодом с разложимым квадратом. Автором сформулированы три условия, гарантирующие неразложимый квадрат у соответствующего кода.

Еще одна глава диссертации представляет новую схему подписи, которая не зависит от типа используемого кода. Установлено, что такая подпись при корректно выбранных параметрах является доказуемо стойкой. В настоящее время эта схема рассматривается в Техническом Комитете 26 как проект национального стандарта.

Таким образом, судя по автореферату и публикациям, автор диссертационной работы провел математически строгое теоретическое исследование по актуальному и перспективному направлению с оценкой перспектив их практического применения.

С учетом изложенного, представленная к рассмотрению диссертация на тему: «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» по уровню выполнения, новизне и актуальности соответствует 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,
Зам. начальника отдела ООО «КРИПТО-ПРО»
Ошкин Игорь Борисович

«12» 11 2025г.

27018, г. Москва, ул. Сущевский Вал, дом 18, +7(495) 995-48-20
oshkin@cryptopro.ru

Подпись Ошкина И.Б. удостоверяю

Начальник отдела кадров.
ООО «КРИПТО-ПРО» Н.В. Дыбова