УДК 003.026

КОДОВЫЕ МЕТОДЫ ДЛЯ ПОСТРОЕНИЯ ПРОТОКОЛОВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Калинина Е.А. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – Давыдов В.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. На сегодняшний день, ввиду угрозы появления полноценного квантового компьютера, актуальным является вопрос построения криптографических схем, которые будут устойчивы к атакам с его использованием. Одним важных инструментов в построении таких являются коды, исправляющие ошибки — их использование позволяет свести стойкость криптографических схем к стойкости NP-трудной задачи о синдромном декодировании. Таким образом, в связи с возникшей необходимостью замены текущих криптографических инструментов на постквантовые, важной задачей является проверка возможности использования корректирующих кодов в различных криптографических протоколах.

Основная часть. В данной работе изучена возможность использования корректирующих кодов для построения протоколов с нулевым разглашением. Под протоколом с нулевым разглашением понимается протокол, позволяющий одной из взаимодействующих сторон доказать проверяющему достоверность заданного утверждения [1], не раскрывая при этом никакой дополнительной информации. Были исследованы кодовые схемы, построенные на основе следующих протоколов с нулевым разглашением: протокола Фиата-Шамира [2], протокола Шнорра [3] и схемы идентификации Штерна [4]. Все изученные протоколы можно рассматривать как доказательство знания для решения задачи синдромного декодирования некоторого конкретного кода, где в качестве открытой информации выступает синдром, а соответствующий ему вектор ошибки — неразглашаемой информацией.

Выводы. В ходе работы были рассмотрены протоколы с нулевым разглашением и проведено исследование применимости корректирующих кодов для их построения. Использование протоколов с нулевым разглашением на основе корректирующих кодов позволит сделать схемы аутентификации более устойчивыми к атакам квантового компьютера.

Список использованных источников:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.

2. Gueron S., Persichetti E., Santini P. Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup // Cryptography. — №6.5. —2022.

3. Baldi M., Chiaraluce F., Santini P. Code-based signatures without trapdoors through restricted vectors // Cryptology ePrint Archive, — Paper 2021/294, —2021.

4. Bellini E., Gaborit P. Enhancing Code Based Zero-Knowledge Proofs Using Rank Metric// Cryptology and Network Security, — CANS 2020. Lecture Notes in Computer Science, — 2020.

Калинина Е.А. (автор) Подпись
Давыдов В.В. (научный руководитель) Подпись