УДК 004.056

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ ПОСТКВАНТОВЫХ ПРИМИТИВОВ В КРИПТОВАЛЮТЕ ETHEREUM

Леевик А.Г. (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»)

В данной работе рассмотрены криптографические примитивы, используемые в криптовалюте Ethereum, определены уязвимые к квантовому компьютеру компоненты системы. Проведено тестирование с использованием постквантовых криптографических примитивов, посчитаны время работы алгоритмов, количество использованной памяти и размеры подписей сообщений и проведено сравнение с теми же показателями непостквантовых алгоритмов.

Криптовалюты с каждым годом становятся все популярнее, это подтверждает высокая капитализация криптовалюты, которая составила 2,58 трлн долларов на конец ноября 2021 года. Криптовалюта Ethereum является одной из популярных на рынке криптовалют, ее доля на рынке составляет примерно 23,8%. В связи с появлением квантового компьютера и квантовых алгоритмов, позволяющих взломать существующие криптографические схемы, некоторые алгоритмы, используемые в криптовалюте Ethereum, могут быть взломаны в будущем с помощью мощных квантовых компьютеров. Для устранения такой возможности предлагается использовать постквантовые криптографические алгоритмы, устойчивые к атакам с помощью квантового компьютера.

В криптовалюте Ethereum главным компонентом, уязвимым к квантовому компьютеру является электронная подпись. В оригинальной системе в качестве алгоритма электронной подписи используется алгоритм ECDSA, основанный на эллиптических кривых. В работе предлагается заменить данный алгоритм на алгоритм электронной подписи на решетках и исследовать изменение работы системы.

В работе представлен обзор и анализ криптографических примитивов криптовалюты Ethereum, определены уязвимые алгоритмы и построена система с использованием постквантовых алгоритмов. Обе системы протестированы и сравнены показатели времени работы алгоритмов, количества использованной памяти и размеров получившихся подписей. В дальнейшем, на основе полученных значений, планируется усовершенствование алгоритмов и, как следствие, улучшение показателей работы системы.

Леевик А.Г. (автор)

Давыдов В.В. (научный руководитель)