МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

АЛГОРИТМЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Рахлина Анна Евгеньевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент кафедры ММАД
Мальцев Михаил Владимирович

Минск, 2022

РЭФЕРАТ

Дыпломная праца, 69 старонак, 18 малюнкаў, 26 крыніц, 1 дадатак.

Ключавыя словы: ПОСТКВАНТАВАЯ КРЫПТАГРАФІЯ, БЛАКЧЭЙН, ЭЛЕКТРОННЫ ЛІЧБАВЫ ПОДПІС, ХЭШ-ФУНКЦЫІ.

Аб`ект даследавання – прымяненне постквантавых алгарытмаў у тэхналогіі блакчэйн.

Мэта працы - вывучэнне магчымасцяў выкарыстання постквантавых крыптасістэм у якасці шыфравання ў блокчейне, распрацоўка рэалізацыі.

Метады даследавання - тэарэтычные: даследаванне крыніц, якія змяшчаюць інфармацыю аб постквантавай крыптаграфіі і блакчэйне; вывучэнне характарыстык постквантавых крыптасістэм; вывучэнне будовы блакчэйна; практычныя: параўнанне постквантавых крыптасістэм па характарыстыках, якія вызначаюць магчымасць выкарыстання ў блакчэйне; распрацоўка мадэлі блакчэйна з выкарыстаннем постквантавых крыптасістэм.

Вынік працы – выяўлены ўразлівасці блокчэйна; прааналізаваны постквантавыя крыптасістэмы; прапанаваны магчымыя варыянты крыптасістэм для выкарыстання ў блокчейне; рэалізавана мадэль блокчейна з выкарыстаннем постквантавай крыптасістэмы.

Вобласць ужывання – забеспячэнне бяспекі пры выкарыстанні прыкладанняў на аснове тэхналогіі блакчэйн.

ABSTRACT

Graduate work, 69 pages, 18 figures, 26 sources, 1 attachment.

Keywords: POST-QUANTUM CRYPTOGRAPHY, BLOCKCHAIN, DIGITAL SIGNATURES, HASH FUNCTIONS.

Object of research – application of post-quantum algorithms in blockchain technology.

Purpose of work – exploring the use of post-quantum cryptosystems as encryption in blockchain, solution development.

Research methods – theoretical: study of sources containing information about post-quantum cryptography and blockchain; study of the characteristics of post-quantum cryptosystems; study of the structure of the blockchain; practical: comparison of post-quantum cryptosystems according to the characteristics that determine the possibility of their use in the blockchain; development of a blockchain model using post-quantum cryptosystems.

Result – definition of blockchain vulnerabilities; comparison of post-quantum cryptosystems; proposal of possible options of cryptosystems for use in the blockchain; a blockchain model using a post-quantum cryptosystem.

Scope – security ensurance of blockchain based applications.

РЕФЕРАТ

Дипломная работа, 60 стр., 9 рис., 11 источников, 1 приложение.

Ключевые слова: ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ, БЛОКЧЕЙН, ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, ХЭШ-ФУНКЦИИ.

Объект исследования – применение постквантовых алгоритмов в технологии блокчейн.

Цель работы – изучение возможностей использования постквантовых криптосистем в качестве шифрования в блокчейне, разработка решения.

Методы исследования – теоретические: изучение источников, содержащих информацию про постквантовую криптографию и блокчейн; изучение характеристик постквантовых криптосистем; изучения строения блокчейна; практические: сравнение постквантовых криптосистем по характеристикам, определяющим возможность их использования в блокчейне; разработка модели блокчейна с использованием постквантовых криптосистем.

Результат работы – выявлены уязвимости блокчейна; проанализированы постквантовые криптосистемы; предложены возможные варианты криптосистем для использования в блокчейне; реализована модель блокчейна с использованием постквантовой криптосистемы.

Область применения – обеспечение безопасности при использовании приложений на основе технологии блокчейн.

Введение

Квантовые вычисления, одно из последних направлений, объединяющих физику и компьютерную науку, - это научная и инженерная область, ориентированная на разработку устройств и алгоритмов обработки информации на основе квантовой механики. В настоящее время квантовые вычисления - это уже сформировавшаяся область исследований с солидными теоретическими и экспериментальными результатами которую все чаще стараются внедрить на высокотехнологичных предприятиях различных отраслей.

Однако в связи с развитием квантовых вычислений возникает масштабная проблема для криптографических алгоритмов. В основу многих используемых сейчас криптографических систем положена предполагаемая вычислительная сложность одной из математических задач: факторизации произведения больших простых чисел и вычисления дискретного логарифма. Считается, что решить ни одну из этих задач на классическом компьютере невозможно - это занимает слишком большое количество времени и ресурсов. В случае использования квантовых алгоритмов для вычислений, время выполнения этих операций значительно сокращается. По прогнозам ученых, уже в 2039 году может быть создан квантовый компьютер, который сможет взламывать современные криптосистемы основанные на данных проблемах, поэтому в скором времени может возникнуть необходимость в использовании постквантовых алгоритмов взамен текущих.

Проблема развития квантовых технологий является проблемой не только для криптографических систем, но и для связанных с ними технологий, одной из которых является блокчейн. Блокчейн и другие технологии распределенного реестра (DLT) значительно развились за последние годы, и их использование было предложено для многочисленных приложений благодаря их способности обеспечивать прозрачность, избыточность и контролируемость. Быстрый прогресс квантовых вычислений открыл возможность проведения атак с использованием квантовых алгоритмов в ближайшем будущем, заставляя задуматься о возможностях перепроектировки блокчейна, используя криптосистемы, устойчивые к квантовым атакам, создавая, таким образом, постквантовый блокчейн.

Вопрос о перепроектировке блокчейна говорит об актуальности данной темы в будущем. В основе данной работы лежит задача исследования безопасности блокчейна и постквантовых алгоритмов. В соответствии с ней были поставлены следующие цели:

1. Проанализировать безопасность криптографических алгоритмов в технологии блокчейн.
2. Изучить постквантовые алгоритмы и их возможности использования в блокчейне.

3. Разработать программную реализацию блокчейна с использованием постквантовых алгоритмов.