ФИЛИАЛ МГУ имени М. В. ЛОМОНОСОВА в городе БАКУ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ

Курсовая работа

на тему:

Шифрование и защита информации в блокчейн-системах в условиях квантовых вычислений

студента III курса группы № 222
Садыгов Алим Хамой оглу

Научный руководитель:
м.н.с. Сиротич Богдан Михайлович

Содержание

1 Введение

В работе рассматриваются вопросы шифрования и защиты информации в блокчейн-системах. Криптографические методы, такие как **RSA**, становятся уязвимыми с развитием квантовых вычислений, что требует перехода к постквантовым алгоритмам.

1.1 Определения

Блокчейн последовательная цепочка блоков, содержащих данные и связанных криптографически.

Блок в блокчейне структурированная запись в блокчейне, содержащая заголовок (включая хеш предыдущего блока), транзакции и служебную информацию.

Цифровая подпись криптографический механизм, подтверждающий подлинность данных.

Шифрование преобразование данных с целью их защиты от несанкционированного доступа.

Асимметричное шифрование метод, использующий два ключа: открытый для шифрования и закрытый для расшифровывания.

Открытый ключ криптографический ключ, предназначенный для шифрования данных или проверки цифровой подписи. Может быть доступен всем пользователям системы.

Закрытый ключ криптографический ключ, используемый для расшифровывания данных или создания цифровой подписи.

RSA криптографический алгоритм, основанный на факторизации больших чисел.

ECDSA (Elliptic Curve Digital Signature Algorithm) криптографический алгоритм цифровой подписи, использующий свойства эллиптических кривых.

Алгоритм Шора алгоритм разложения числа на множители.

SNDL (Store Now, Decrypt Later) стратегия сбора данных для их последующей расшифровки.

Криптографическая стойкость устойчивость алгоритма к расшифровке без ключа.

Хеш-функция криптографический алгоритм, необратимо преобразующий входные данные в фиксированную строку символов.

Хеш результат хеш-функции, имеющий фиксированную длину и изменяющийся при изменении входных данных.

2 Актуальность задачи

SNDL — основная угроза. Блокчейн-системы используют криптографические алгоритмы, такие как **RSA** и **ECDSA**, для защиты данных и цифровой подписи транзакций. Однако стратегия **SNDL** делает их уязвимыми.

Уязвимость RSA, ECDSA. Алгоритм Шора.

RSA основан на сложности факторизации больших чисел, а **ECDSA** — на вычислительной сложности дискретного логарифмирования на эллиптических кривых. **Алгоритм Шора** ускоряет разложение числа на множители и решает задачу дискретного логарифма на квантовом компьютере, что делает **RSA** и **ECDSA** уязвимыми в условиях квантовых атак.

Основные последствия:

- **Кража приватных ключей** — квантовый компьютер сможет восстановить закрытый ключ, что приведёт к подделке подписей транзакций.
- **Компрометация данных** — зашифрованные в прошлом транзакции и контракты будут вскрыты в будущем.
- **Нарушение целостности блокчейна** — возможность подделки подписей ставит под угрозу неизменность записей.

Вывод.

1. SNDL-атаки делают текущие зашифрованные данные уязвимыми в будущем.
2. RSA и ECDSA становятся незащищёнными в условиях квантовых вычислений.

3 Проблематика задачи

Цифровая подпись — основной механизм обеспечения подлинности транзакций и блоков в блокчейн-системах. Её безопасность напрямую зависит от стойкости используемого криптографического алгоритма. Алгоритмы, основанные на факторизации или дискретном логарифмировании, такие как **RSA** и **ECDSA**, уязвимы перед квантовыми атаками, в частности — перед **алгоритмом Шора**.

Цифровые подписи, созданные до появления квантовых компьютеров, сохраняются в блокчейне и могут быть подделаны в будущем. Даже при переходе на постквантовые алгоритмы, ранее подписанные данные остаются уязвимыми, так как невозможно их изменение без нарушения неизменности цепочки блоков.

Одним из распространённых методов повышения стойкости является увеличение длины криптографического ключа. Однако это приводит к росту вычислительной нагрузки, снижению скорости генерации и проверки подписей, а также увеличению объёма данных в блоках. В условиях блокчейна, где каждая подпись обрабатывается и хранится множеством узлов, это может привести к деградации производительности сети.

то что ниже мне я переделаю, как только выберу блокчейн, так как идей вообще нет

В рамках данной работы в качестве примера рассматривается блокчейн-система **Monero**, использующая протокол **CryptoNote** и механизм кольцевых подписей. Несмотря на то, что **RSA** в Monero напрямую не применяется, его можно рассматривать как обобщённую модель асимметричного шифрования для анализа зависимости между длиной ключа, уровнем криптостойкости и скоростью вычислений.

Проблема заключается в необходимости нахождения баланса между безопасностью и эффективностью. Стремление обеспечить максимальную стойкость может привести к непрактичным задержкам в работе сети. Цель данного исследования — определить оптимальную длину ключа, обеспечивающую достаточный уровень безопасности без существенного ущерба производительности в условиях современных вычислительных возможностей.

Таким образом, вопрос безопасности блокчейна в условиях квантовых вычислений остается нерешенным, что требует разработки и внедрения устойчивых криптографических механизмов.

Список литературы