Технічні науки

УДК 004.051

Середа Дар'я Антонівна

студентка

Харківського національного університету радіоелектроніки

Sereda Daria

Student of the

Kharkiv National University of Radio Electronics

Науковий керівник:

Шубін Ігор Юрійович

кандидат технічних наук, доцент,

професор кафедри програмної інженерії

Харківський національний університет радіоелектроніки

ПОСТ-КВАНТОВА КРИПТОГРАФІЯ ТА БЛОКЧЕЙН
POST-QUANTUM CRYPTOGRAPHY AND BLOCKCHAIN

Анотація. *Досліджено теоретичні питання щодо необхідності використання пост-квантової криптографії у блокчейні.*

Ключові слова: *квантовый, пост-квантова, криптографія, блокчейн, хеш, решітки.*

Summary. *Theoretical questions regarding the necessity of using post-quantum cryptography in the blockchain have been studied.*

Key words: *quantum, post-quantum, cryptography, blockchain, hash, lattice.*

Квантові обчислення матимуть великий вплив на наше життя: розробка ліків, оптимізація трафіку, штучний інтелект або прогноз погоди виграють від збільшення потужності, яку принесе з собою квантовий

комп'ютер; але з великою потужністю приходить велика відповідальність, і вплив квантових обчислень на кібербезпеку може бути катастрофічним, якщо не просувати вперед поточні криптографічні методи.

Квантові обчислення були активною дослідницькою сферою з моменту їх першої появи у 80-х роках. З розвитком квантових обчислень були створені алгоритми Шора та Гровера [1].

Вплив алгоритму Шора особливо важливий у технології блокчейн, оскільки він може бути використаний для зламу алгоритму цифрового підпису ECDSA, який використовується серед інших Bitcoin, Ethereum або Zcash.

Основним наслідком алгоритму Гровера є можливість створювати квантові алгоритми, здатні знаходити прообрази хеш-функцій, що є ще однією обчислювально складною проблемою для класичного комп'ютера. Алгоритм Гровера становить загрозу, оскільки його можна використовувати проти хеш-функцій, таких як SHA256, Keccak або RIPEMD160, і це призводить до серйозних уразливостей у Bitcoin, Ethereum, Litecoin або Zcash [2]. Крім того, алгоритм можна використовувати для пошуку хеш-колізій, що дозволяє замінювати блоки в блокчейні.

Ключовим фактором, який змушує класичний комп'ютер прогавати у деяких ситуаціях у порівнянні з квантовим комп'ютером, є суперпозиція, яка, по суті, є здатністю квантової системи перебувати в кількох станах (вгорі та внизу, всередині та зовні тощо) під час той же час. Наприклад, для заданої функції f квантовий комп'ютер дозволяє нам обчислити f(x) для суперпозиції всіх значень x одночасно. Потенційні квантові атаки на блокчейн можуть вплинути або на етап PoW, або на цифрові підписи.

У першому випадку алгоритм Гровера може бути використаний для виконання хеш-кешу PoW, який використовується, наприклад, у біткойнах, із квадратично меншою кількістю хешів, ніж вимагає класичний комп'ютер. Цей факт означає, що зловмисник з квантовим комп'ютером може змінити

блок і відтворити блокчейн набагато швидше, відходячи від «нового блоку». Це має кілька наслідків: з одного боку, зловмисні майнери отримають більше винагород, ніж чесні майнери, а з іншого — зловмисні майнери зможуть набагато швидше взяти під контроль блокчейн, оскільки здатність створювати нові блоки збільшується.

У другому випадку алгоритм Шора може бути використаний проти алгоритму цифрового підпису ECDSA. Квантовий зловмисник міг би отримати приватний ключ користувача, маючи його відкритий ключ. Хоча ця атака не впливає на структуру блокчейну з точки зору зв'язаних хешів, вона дійсно відкриває двері для підробки вмісту в блоці: включення необробленої транзакції в блок після її трансляції не відбувається негайно; якщо квантовий комп'ютер може отримати секретний ключ, зловмисник може використати його для створення нової транзакції, перенаправляючи платіж на його адресу.

Щоб подолати атаки, описані вище, і бути готовими до майбутніх квантових атак, важливо знайти нові математичні інструменти, які ведуть до більш ефективних криптографічних алгоритмів. В цій новій системі теорії чисел уже недостатньо, і потрібна більш складна математична структура, так і з'являється поява нової галузі досліджень: постквантової криптографії.

Основними методами, дослідженими для визначення нових квантово-стійких криптографічних алгоритмів, є решітки, ізогенії суперсингулярних еліптичних кривих, коди, багатовимірні поліноми та хеш-функції [3].

Решітка – це повторюване розташування точок у просторі. Їх застосування в криптографії охоплює всі примітиви: шифрування/дешифрування, цифрові підписи і обмін ключами.

Безпека цих методів залежить від кількох задач (проблем). Нехай Zq позначає цілі числа за модулем простого q:

1. Проблема про найближчий вектор: у цій задачі за заданим вектором потрібно знайти найближчий нетривіальний вектор у решітці. На рисунку 1 синьою точкою позначено найкоротший вектор.

2. Проблема найкоротшого вектора: тут потрібно знайти найкоротший нетривіальний вектор у решітці.

3. Проблема короткого цілого розв'язку: у цій задачі задано m векторів (розмірності n) з елементами в Zq, розташованих у вигляді стовпців матриці A, потрібно знайти досить малий розв'язок для $A \cdot z = 0 \pmod q$.

4. Навчання з помилками: розглянемо секретний n-вимірний вектор S з елементами в Zq, відкриту (m,n)-матрицю A з елементами в Zq і шумовий m-вимірний вектор E з елементами в Zq. Дано $B = A \cdot S + E$, завдання полягає в тому, щоб знайти S.

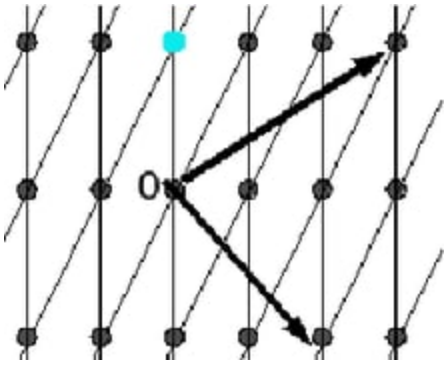

Рис. 1. Знаходження найкоротшого вектора за допомогою решітки

Хоча алгоритми на основі решітки потребують покращення з точки зору розмірів ключів, вони є дуже перспективним рішенням у постквантовій криптографії. Останні дослідження показують, що деякі пропозиції є швидкими та навіть порівнянними з поточними асиметричними алгоритмами, такими як RSA, під час тестування на класичних комп'ютерах. Це показує, що алгоритми на основі решітки можуть бути придатними для технології блокчейн. Що стосується цифрових підписів, такі пропозиції, як Dilithium і qTesla, є одними з найшвидших алгоритмів.

Хеш-функція виводить дайджест фіксованої довжини незалежно від довжини вхідних даних. Він повинен задовольняти дві властивості:

1. Бути стійким до зіткнень, це означає, що за наявності двох різних входів обчислювально неможливо знайти спільний вихід.

2. Бути стійким до прообразів, це означає, що з огляду на вихід хеш-функції, обчислювально неможливо знайти дійсний вхід.

Безпека схем на основі хешування залежить від безпеки основної хеш-функції, а не на складності базової математичної проблеми (як це відбувається з алгоритмами на основі решітки). Важливо мати на увазі, що більшість хеш-функцій, задіяних у технології блокчейну, таких як SHA256 у випадках Bitcoin та Ethereum, вважаються квантово стійкими, оскільки алгоритм Гровера просто зменшує кількість пошуків з 2^256. до 2^128.

Рішення для цифрового підпису на основі хешу мають покращитися з точки зору загальної продуктивності, щоб бути придатними для блокчейну.

Можна виділити кілька методів щодо квантового опору у блокчейні.

Підходи, які вимагають PoW, що вимагає великої кількості пам'яті, наприклад, цикли зозулі, засновані на пошуку підграфів постійного розміру у випадкових графах.

Використання розширеної схеми підпису Merkle (XMSS) у поєднанні з одноразовими підписами.

Використання алгоритмів на основі хешу для експериментування з SPHINCS.

Алгоритми, засновані на решітках, щоб забезпечити приховування одержувача, походження та значення. Можливість заміни цифрового підпису біткойна такими алгоритмами, як TESLA#, який спирається на поліноміальну версію проблеми навчання з помилками.

Таким чином, можна прийти до висновку, що для того, щоб бути повністю застосовною у середовищі блокчейну, постквантова стійка криптографія має враховувати наступні аспекти: блокчейн повинен

використовувати маленькі пари ключів, щоб зменшити необхідний простір для зберігання, крім того, малі ключі потребують менш складних обчислювальних операцій під час керування ними, постквантові схеми мають бути максимально швидкими та менш вимогливими до обчислень, щоб дозволити блокчейну обробляти велику кількість транзакцій за секунду, невеликий підпис і довжина хешу, якщо довжина підпису або хешу збільшується, розмір блокчейну також збільшиться.

Також ефективним є застосування кількох методів в налаштуванні блокчейну: сукупні підписи дозволяють генерувати комбінований підпис, отриманий з кількох із них; групові підписи дають члену групи дозвіл анонімно підписуватись від імені своєї групи; кільцеві підписи дозволяють вказати набір можливих підписантів, не розкриваючи, хто з них створив підпис. Крім того, решітки, окрім надання цікавих потенційних рішень для блокчейну, також відкривають двері для включення гомоморфного шифрування в блокчейн, що дозволить третім сторонам обробляти зашифровані транзакції без розкриття секретних даних.

Література

1. Quantum Threat to Blockchains: Shor's and Grover's Algorithms // codeburst: [Веб-сайт]. URL: https://codeburst.io/quantum-threat-to-blockchains-shors-and-grover-s-algorithms-9b01941bed01 (дата звернення: 10.01.2023).
2. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities // Science Direct: [Веб-сайт]. URL: https://www.sciencedirect.com/science/article/pii/S131915782100207X (дата звернення: 11.01.2023).
3. A Guide to Post-Quantum Cryptography // Medium: [Веб-сайт]. URL: https://medium.com/hackernoon/a-guide-to-post-quantum-cryptography-d785a70ea04b (дата звернення: 11.01.2023).