КІЛЬЦЕВІ ПІДПИСИ У БЛОКЧЕЙН СИСТЕМАХ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

Фроленко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних блокчейн системах питання забезпечення анонімності, цілісності та стійкості до квантових атак є одним з ключових напрямів розвитку криптографії. Традиційні методи цифрових підписів ґрунтуються на комутативних групах (RSA, ECDSA), які можуть бути вразливими до квантових алгоритмів. Одним із перспективних підходів є використання кільцевих підписів на основі некомутативних груп [1, 2], що відкриває нові можливості для реалізації постквантової безпеки у блокчейн-технологіях.

Метою доповіді є теоретичне обґрунтування моделі кільцевого підпису для блокчейн систем на основі некомутативних груп, що забезпечує анонімність підписанта та стійкість до квантових атак.

У зв'язку з інтенсивним розвитком квантових обчислень, виникає потреба у нових криптографічних механізмах, здатних протистояти квантовим атакам. На відміну від традиційних схем кільцевого підпису, що базуються на задачах дискретного логарифма або факторизації (у комутативних групах), дана модель використовує некомутативні структури, серед яких: групи кіс (braid groups), групи матриць над кільцями з невзаємозамінними елементами, або групи перетворень із некомутативними операціями. Кожна з них характеризується високим ступенем обчислювальної складності при виконанні операцій знаходження зворотного елементу, що є основою для побудови стійких криптографічних примітивів. Застосування цих структур у схемах кільцевого підпису забезпечує формування криптографічних систем нового покоління, здатних забезпечити постквантову стійкість, анонімність учасників і захист від криптоаналітичного розкриття навіть у разі появи потужних квантових обчислювальних засобів [3].

Основна ідея схеми полягає у забезпеченні можливості одному з учасників групи підписати повідомлення таким чином, щоб інші могли перевірити його достовірність, але не могли визначити, хто саме з учасників створив підпис. У запропонованій моделі, побудованій на некомутативних групах, кожен учасник володіє відкритим ключем, що формується на основі його секретного ключа та фіксованого елемента групи. Сукупність усіх відкритих ключів утворює «кільце» потенційних підписантів.

Учасник, що здійснює підписання, використовуючи свій секретний ключ, генерує підпис за допомогою комбінацій некомутативних операцій над елементами групи.

Перевірка підпису здійснюється через спільну перевірку групових співвідношень, без розкриття інформації про те, який саме ключ було використано [3]. Такий підхід гарантує анонімність підписанта, цілісність

повідомлення та незаперечність факту підпису від імені будь-якого члена кільця. На відміну від еліптичних кривих або RSA, задачі на некомутативних групах (зокрема спряження чи декомпозиції) не мають відомих ефективних квантових алгоритмів для їх розв'язання. Це робить модель перспективною в умовах появи квантових обчислень.

Через властивість некомутативності операцій результати навіть близьких ключів у групі виглядають статистично незалежними. Це знижує ризик атак деанонімізації у блокчейн-мережах. Модель може бути вбудована в механізми анонімних транзакцій або доказів знань без розкриття.

Використання некомутативних структур забезпечує високий рівень криптографічної ентропії та захист від квантового криптоаналізу, що робить таку модель придатною для інтеграції у децентралізовані блокчейн-мережі.

Реалізація кільцевих підписів на некомутативних групах може бути використана для побудови анонімних транзакцій, приватних голосувань або конфіденційних смартконтрактів у децентралізованих мережах.

Запропонована модель кільцевого підпису на основі некомутативних груп розглядається як перспективний напрям розвитку постквантової блокчейн-криптографії [4, 5]. Її доцільність полягає у здатності забезпечувати квантову стійкість криптографічних механізмів, підвищувати рівень анонімності транзакцій, зменшувати ризик криптоаналітичного розкриття підписів, а також у можливості інтеграції в сучасні блокчейн-платформи без необхідності суттєвих структурних змін.

Список літератури

5. Kotukh, Y., Khalimov, G., & Dzhura, I. (2025). Cryptographic competitiveness of cryptosystems based on noncommutative groups. Radiotekhnika, (221), 72–82. https://doi.org/10.30837/rt.2025.2.221.10

6. Kotukh, E., Severinov, O., Vlasov, A., Kozina, L., Tenytska, A., & Zarudna , E. (2021). Methods of construction and properties of logariphmic signatures. Radiotekhnika, 2(205), 94–99. https://doi.org/10.30837/rt.2021.2.205.09

7. Easttom, C. (2022). Quantum computing and cryptography. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 397-407). Cham: Springer International Publishing.

8. Поддубний В.О., Гвоздьов Р.Ю., Сєвєрінов О.В. Методи електронного підпису на основі некомутативних груп // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: 12-та міжнародна науково-технічна конференція, 27-28 квітня 2022 р. – Баку – Харків – Жиліна, 2022. - Т. 1, С. 149.

9. G.Khalimov, Y.Kotukh, S.Khalimova, O.Sievierinov, A.Vlasov. "Towards advance encryption based on a Generalized Suzuki 2-groups". International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) 2021.

10. G.Khalimov, Y.Kotukh, I.Didmanidze, O.Sievierinov. "Towards three-parameter group encryption scheme for MST3 cryptosystem improvement". Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) 2021.