УДК 004.056.5:004.75:512.56

Фроленко В. О.

РОЗВИТОК МОДЕЛЕЙ КІЛЬЦЕВИХ ПІДПИСІВ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП У ПОСТКВАНТОВИХ БЛОКЧЕЙН-СИСТЕМАХ

Традиційні криптографічні механізми, що використовуються у більшості блокчейн-платформ, базуються на задачах дискретного логарифма або факторизації великих чисел. Однак розвиток квантових обчислень створює потенційну загрозу для таких систем, оскільки алгоритми, подібні до алгоритму Шора, теоретично здатні ефективно розв’язувати ці задачі. У зв’язку з цим особливого значення набувають дослідження у сфері постквантової криптографії. Одним із перспективних напрямів є використання некомутативних алгебраїчних структур для побудови криптографічних примітивів [1]. Зокрема, кільцеві підписи на основі некомутативних груп можуть забезпечити одночасно високий рівень анонімності та стійкість до потенційних квантових атак. Такі підписи дозволяють одному з учасників певної групи підписати повідомлення від імені

всієї групи, не розкриваючи своєї особи, що робить їх особливо актуальними для застосування у блокчейн-технологіях.

Метою даної роботи є наукове обґрунтування розвитку моделей кільцевих підписів на основі некомутативних груп, а також аналіз їх ефективності, масштабованості та криптографічної стійкості при використанні у блокчейн-системах з урахуванням вимог постквантової безпеки.

Кільцевий підпис (ring signature) є криптографічним механізмом, що забезпечує анонімність підписанта серед множини потенційних учасників. У класичних реалізаціях такі схеми ґрунтуються на комутативних групах, зокрема на еліптичних кривих або модульній арифметиці. Однак у контексті постквантової криптографії дедалі більший інтерес викликають моделі, що базуються на некомутативних групах.

Некомутаційні алгебраїчні структури, такі як групи кіс (braid groups), матричні групи над некомутативними кільцями або групи перетворень із некомутативними операціями, характеризуються високою обчислювальною складністю задач, що лежать в основі криптографічних протоколів. До таких задач належать задача спряження (conjugacy problem), задача декомпозиції та інші складні алгебраїчні проблеми, для яких на сьогодні не існує ефективних квантових алгоритмів розв’язання.

У моделі кільцевого підпису на основі некомутативних груп кожен учасник системи володіє секретним ключем, що належить до певної алгебраїчної структури, та відповідним відкритим ключем, сформованим через операції групи. Сукупність відкритих ключів формує так зване «кільце» підписантів. Учасник, який створює підпис, генерує криптографічну конструкцію, що включає результати некомутативних операцій над елементами групи, таким чином формуючи ланцюг перевірних співвідношень [2, 3].

Перевірка підпису здійснюється через перевірку коректності цих співвідношень для всіх елементів кільця. При цьому неможливо визначити, який саме учасник використав свій секретний ключ для створення підпису. Завдяки цьому забезпечується властивість анонімності підписанта, що є ключовою для багатьох застосувань у блокчейн-системах.

Одним із важливих напрямів подальших досліджень є аналіз ефективності таких схем. Оскільки операції у некомутативних групах можуть бути обчислювально складнішими, ніж у традиційних криптографічних системах, необхідно оптимізувати алгоритми обчислення групових операцій, зменшувати розмір підписів та скорочувати час перевірки. Для цього можуть застосовуватися методи агрегування підписів, оптимізації структури кільця або використання спеціалізованих алгебраїчних представлень груп.

Ще одним важливим аспектом є масштабованість системи. У реальних блокчейн-мережах кількість потенційних підписантів може бути значною, тому важливо забезпечити стабільність параметрів системи при збільшенні кількості учасників. Оптимізація алгоритмів формування та перевірки підписів дозволить забезпечити ефективну інтеграцію таких схем у децентралізовані платформи. Значну увагу необхідно приділити криптоаналітичному аналізу запропонованих моделей. Це передбачає дослідження можливих атак, пов’язаних зі структурними властивостями використовуваних груп, аналіз статистичних характеристик підписів, а також оцінку стійкості до нових типів атак, що можуть виникнути з розвитком квантових обчислювальних технологій.

Проведений аналіз показує, що використання некомутативних груп для побудови схем кільцевих підписів є перспективним напрямом розвитку постквантової криптографії. Такі моделі дозволяють забезпечити високий рівень анонімності підписантів, зберігаючи при цьому криптографічну стійкість навіть в умовах появи квантових обчислень. Подальший розвиток даного підходу пов’язаний із дослідженням

ефективності алгоритмів, оптимізацією параметрів системи та проведенням комплексного криптоаналізу. Отримані результати можуть стати основою для створення нових протоколів анонімних транзакцій, систем електронного голосування та конфіденційних смартконтрактів у децентралізованих мережах.

Таким чином, моделі кільцевих підписів на основі некомутативних груп мають значний потенціал для формування нового покоління криптографічних механізмів, здатних забезпечити надійний захист інформації у сучасних цифрових інфраструктурах та майбутніх постквантових системах безпеки.

Список використаних джерел

1. Фроленко В. О. Кільцеві підписи у блокчейн системах на основі некомутативних груп / В. О. Фроленко // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла: [у 4 т.]. Т. 2: секції 3, 7 / Ін-т систем управління МНО Азербайджанської республіки, Національний технічний університет "Харківський політехнічний інститут", Харківський національний університет радіоелектроніки [та ін.] – Харків : НТУ "ХПІ", 2025. – С. 54-55.

2. 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

3. Kotukh, E. V., Severinov, O. V., Vlasov, A. V., Kozina, L. S., Tenytska, A. O., & Zarudna, E. O. (2021). Методи побудови та властивості логарифмічних підписів. Radiotekhnika, (205), 94-99.