МОДЕЛЬ КІЛЬЦЕВОГО ПІДПИСУ З КОНТРОЛЬОВАНОЮ ЗВ'ЯЗУВАНІСТЮ ТРАНЗАКЦІЙ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

Фроленко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

Забезпечення анонімності учасників блокчейн-систем за одночасного збереження можливості перевірки достовірності транзакцій є актуальним завданням сучасної криптографії. Кільцевий підпис дозволяє підтверджувати належність підписанта до множини учасників без розкриття його особи. Попередні дослідження обґрунтували перспективність використання некомутативних груп для побудови таких механізмів та визначили необхідність оцінювання їх криптографічної стійкості й обчислювальної ефективності [1-3].

Водночас звичайний кільцевий підпис не передбачає виявлення повторного застосування одного секретного ключа. Для блокчейн-протоколів, зокрема механізмів протидії подвійному витрачанню активів, потрібна додаткова властивість зв'язуваності підписів. При цьому встановлення зв'язку між операціями не повинно автоматично розкривати особу підписанта.

Метою доповіді є обґрунтування структурно-функціональної моделі кільцевого підпису на основі некомутативних груп із контрольованою зв'язуваністю транзакцій у визначеному контексті блокчейн-системи.

Пропонується доповнити базову модель кільцевого підпису контекстно-залежним криптографічним ідентифікатором. Модель передбачає чотири основні процедури: генерування параметрів і ключових пар учасників, формування кільця відкритих ключів, створення та перевірку підпису, визначення зв'язуваності підписів у межах установленої області застосування. Контекст може включати ідентифікатор мережі, клас операції або область використання протоколу.

Нехай G - вибрана некомутативна група, а L - упорядкована множина відкритих ключів потенційних підписантів. Алгоритм підписання приймає повідомлення m, множину L, секретний ключ одного учасника та контекст c і формує пару (σ, τ), де σ - кільцевий підпис, τ - контекстно-залежний ідентифікатор зв'язуваності. Перевірка встановлює коректність σ відносно m, L та c; окрема процедура порівнює ідентифікатори τ для виявлення повторного використання ключа в одному контексті. Це є функціональною специфікацією моделі, а не завершеною криптографічною конструкцією.

Вибір групи G необхідно здійснювати за критеріями обчислювальної складності відповідної алгебраїчної задачі, ефективності операцій множення та інверсії, компактності кодування елементів і стійкості до відомих структурних атак. Потенційними кандидатами є групи кіс, матричні групи та

скінченні некомутативні групи [1, 4]. Некомутативність сама по собі не доводить постквантової безпеки; для конкретної конструкції потрібні формалізовані припущення та окремий аналіз класичних і квантових атак.

До вимог безпеки моделі належать коректність перевірки, стійкість до підроблення, анонімність підписанта, неможливість формування різних ідентифікаторів для одного ключа в межах того самого контексту та обмеження зв'язуваності між різними контекстами. Особливу увагу слід приділити атакам із підміною відкритих ключів, навмисним вибором складу кільця та використанням алгебраїчних особливостей групи.

Новизна запропонованого підходу полягає у структурно-функціональному поєднанні механізму анонімного підтвердження належності підписанта до множини учасників із механізмом контекстно-залежного виявлення повторного використання секретного ключа. Передбачається, що зв'язування операцій здійснюється лише в межах визначеного контексту, тоді як використання ключа в різних контекстах не повинно автоматично розкривати особу підписанта або створювати можливість зіставлення його дій. Такий підхід потребує формального визначення умов зв'язуваності, анонімності та стійкості до підроблення для конкретної криптографічної конструкції. Для подальшого експериментального дослідження доцільно оцінювати час генерування й перевірки підпису, обсяг підпису, розмір ключових даних і кількість групових операцій залежно від кількості учасників кільця. Порівняння різних представлень груп дозволить визначити практичні обмеження застосування моделі в блокчейн-системах.

Таким чином, сформульовано модель розвитку кільцевого підпису на основі некомутативних груп шляхом введення контрольованої зв'язуваності транзакцій. Її відмінність від базового підходу полягає в розділенні анонімної перевірки належності підписанта до кільця та виявлення повторного використання ключа в заданому контексті. Подальше дослідження передбачає побудову конкретних алгоритмів, формальне обґрунтування властивостей безпеки, реалізацію та експериментальну перевірку ефективності.

Список літератури

1. Фроленко В. О. Кільцеві підписи у блокчейн системах на основі некомутативних груп. Проблеми інформатизації : тези доп. тринадцятої міжнар. наук.-техн. конф., 27–28 листопада 2025 р. Харків : НТУ «ХПІ», 2025. Т. 2. С. 54–55.

2. Kotukh Y., Khalimov G., Dzhura I. Cryptographic competitiveness of cryptosystems based on noncommutative groups. Radiotekhnika. 2025. No. 221. P. 72–82. DOI: 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

4. 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 : матеріали дванадцятої міжнар. наук.-техн. конф., 27–28 квітня 2022 р. 2022. Т. 1. С. 149.