ПОРІВНЯЛЬНИЙ АНАЛІЗ КОМУТАТИВНИХ І НЕКОМУТАТИВНИХ КРИПТОГРАФІЧНИХ МОДЕЛЕЙ

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

Безпека цифрових даних та транзакцій є ключовою умовою розвитку сучасних інформаційних технологій. Традиційні криптографічні методи засновані на комутативних групах і довели свою ефективність, проте розвиток квантових обчислень ставить під сумнів їхню довгострокову стійкість. За таких умов зростає значення некомутативних криптографічних моделей, які пропонують нові можливості для анонімності та постквантової безпеки.

Метою доповіді є порівняльний аналіз комутативних і некомутативних криптографічних моделей та оцінка їх доцільності для сучасних і постквантових цифрових систем.

Комутативні криптографічні моделі ґрунтуються на структурах, де порядок виконання операцій не впливає на результат. Вони включають модульну арифметику, що використовується у RSA та ElGamal, і еліптичні криві, застосовані в ECDSA та EdDSA. Основною перевагою таких моделей є швидкодія, відносно невеликий розмір ключів і простота реалізації алгоритмів перевірки. Ці характеристики роблять комутативні моделі оптимальними для масового використання у сучасних системах. Водночас розвиток квантових алгоритмів, таких як алгоритм Шора, ставить під загрозу їхню стійкість, оскільки ці алгоритми здатні ефективно розв’язувати задачі дискретного логарифма та факторизації великих чисел, на яких базується безпека комутативних схем [1, 2]. Таким чином, хоча комутативні моделі залишаються швидкими та практичними, їхня криптографічна надійність у перспективі може знижуватися.

Некомутаційні моделі базуються на структурах, де порядок виконання операцій критично важливий, що створює додатковий рівень обчислювальної складності [3, 4]. До таких структур належать групи кіс, матричні групи над некомутативними кільцями та групи перетворень із некомутативними операціями. Складність вирішення пов’язаних задач, таких як задача спряження або декомпозиції, забезпечує високий рівень стійкості до атак, включаючи потенційні квантові. Некомутативні моделі дозволяють реалізовувати анонімні цифрові підписи, що важливо для захисту приватності користувачів у блокчейн-мережах та системах електронного голосування.

Перевага некомутативних моделей полягає не лише у стійкості до квантових атак, але й у здатності забезпечити анонімність підписантів у схемах кільцевих або групових підписів. Така анонімність стає критичною у фінансових системах і децентралізованих платформах, де конфіденційність користувачів є ключовою вимогою. Водночас недоліком таких моделей є

більша обчислювальна складність, що може обмежувати швидкодію та збільшувати витрати на формування і перевірку підписів. Для практичного застосування важливо оптимізувати алгоритми обчислення групових операцій і зменшити обсяг даних, що передаються, без втрати криптографічної стійкості.

Порівняння показує, що комутативні моделі залишаються ефективними для задач, де пріоритетом є швидкодія та простота реалізації, тоді як некомутативні моделі забезпечують вищий рівень безпеки та анонімності. У сучасних блокчейн-системах доцільно застосовувати некомутативні підходи, особливо у тих випадках, коли важлива захищеність даних від майбутніх квантових обчислень та конфіденційність користувачів.

Подальший розвиток полягає у пошуку ефективних представлень груп і оптимізації обчислювальних алгоритмів, що дозволить інтегрувати некомутативні моделі у великі децентралізовані мережі без значних втрат у продуктивності [5].

Порівняльний аналіз комутативних і некомутативних криптографічних моделей показує, що обидва підходи мають свої переваги та обмеження. Комутативні моделі залишаються швидкими та простими у реалізації, але їхня довгострокова безпека під питанням через розвиток квантових обчислень. Некомутативні моделі забезпечують підвищену стійкість і анонімність, що робить їх перспективними для постквантових систем і блокчейн-платформ. Оптимізація алгоритмів і гібридні підходи дозволять поєднувати ефективність та безпеку, формуючи основу для нового покоління криптографічних механізмів у цифрових інфраструктурах.

Список літератури

1. Khalimov, G., Sievierinov, O., Khalimova, S., Kotukh, Y., Chang, S. Y., & Balytskyi, Y. (2021, October). Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 465-469). IEEE.

2. 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.

3. Поддубний В. О. Методи електронного підпису на основі некомутативних груп / В. О. Поддубний, Р. Ю. Гвоздьов, О. В. Сєвєрінов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : матеріали дванадцятої міжнар. НПК, 27-28 квітня 2022 р. – Баку – Харків – Жиліна, 2022. – С. 149.

4. Гвоздьов, Р.Ю., Сєвєрінов, О.В. (2022). Метод шифрування на основі багатопараметричних груп // Проблеми інформатизації: десята міжнародна науково-технічна конференція, 24 – 25 листопада 2022 року, Том 1. - Черкаси – Баку – Бельсько-Бяла – Харків – 2022.

5. 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 – Харків : НТУ "ХПІ", 2025. – С. 54-55.