УДК 004

ЗАСТОСУВАННЯ ГІБРИДНИХ МЕТОДІВ ШИФРУВАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРЕДАВАННЯ ДАНИХ У БЛОКЧЕЙН-МЕРЕЖАХ

Скорін Юрій, Лактіонов Артем

Харківський національний економічний університет ім. Семена Кузнеця

Технічні проблеми з безпекою даних та ризики вразливості:

Перша та найважливіша технічна проблема — це вразливість даних під час їхнього передавання, хоча часто використовуються захищені канали з TLS, це не впливає на атаки типу «людина посередині» (Man-in-the-Middle, MITM) на рівні застосунку або при перехопленні трафіку між внутрішніми вузлами мережі.

Друга проблема — це безпечне обмін ключами шифрування. Для швидкого шифрування великих обсягів даних добре підходять симетричні алгоритми (наприклад, AES), однак їхній головний недолік — складність забезпечення безпечної передачі секретного ключа між відправником та одержувачем у відкритій або децентралізованій мережі.

Третя проблема — надмірна висока складність обчислень при використанні асиметричного шифрування. Асиметричні алгоритми, наприклад, RSA або ECC, розв'язують проблему обміну ключами, але вони значно повільніші за симетричні. Використовувати їх для шифрування кожного повідомлення або великих файлів нераціонально, оскільки це призводить до великого навантаження на потужності процесора клієнта та сервера.

Четверта проблема — прозорість та незмінність блокчейну.

Будь-які конфіденційні дані, такі як особиста інформація, фінансові деталі або комерційна таємниця, що потрапляють у блокчейн, не можуть бути видалені або змінені. Це створює постійний ризик утечки даних, оскільки будь-хто, у кого є доступ до реєстру, може прочитати цю

інформацію. Стандартні механізми блокчейну не забезпечують конфіденційності даних.

П’ята проблема – необхідність захисту off-chain даних, у багатьох сучасних DApps (децентралізованих застосунках) лише хеш або підтвердження транзакції зберігається в блокчейні, тоді як основний масив даних (наприклад, документи, зображення, JSON-об'єкти) зберігається поза мережею (off-chain), необхідно забезпечити, щоб ці дані також були надійно зашифровані, а доступ до них мали лише авторизовані сторони.

Шоста проблема – відсутність гнучкого та уніфікованого рішення, розробники часто змушені або покладатися на складні, монолітні криптографічні бібліотеки, або реалізовувати власні схеми, що призводить до помилок, на об'єкті управління бракує стандартизованого, легкого модуля, який би реалізовував перевірену гібридну схему (поєднуючи швидкість AES для даних та безпеку ECC для ключів.

Метою дослідження є теоретичне обґрунтування, практична розробка та аналіз ефективності гібридної криптографічної схеми, адаптованої для підвищення безпеки передавання даних у блокчейн-мережах. *Кінцевим завданням* є створення моделі, що забезпечує високий рівень конфіденційності, цілісності та автентичності інформації, долаючи притаманні блокчейну обмеження прозорості. *Актуальність дослідження* зумовлена стрімким впровадженням блокчейн-технологій у сфери, що вимагають не лише цілісності, але й суворої конфіденційності даних. Виникла фундаментальна суперечність, яку можна назвати «парадоксом безпеки блокчейну». З одного боку, технологія блокчейн за своєю суттю є безпечною, оскільки криптографічно гарантує цілісність (захист від зміни даних) та незмінність (impenetrability) записів у розподіленому реєстрі. З іншого боку, класичні публічні блокчейни (як Bitcoin або Ethereum) є прозорими за дизайном. Будь-який учасник мережі може переглянути вміст транзакцій, що унеможливлює роботу з чутливою або комерційною інформацією. Таким чином, блокчейн сам по собі не забезпечує повноцінної

конфіденційності. Це створює низку критичних вразливостей, які дослідження має вирішити:

– вразливість каналів передачі, дані, що передаються між вузлами мережі або між користувачем та вузлом (наприклад, при надсиланні транзакції), можуть бути перехоплені;
– атаки типу «людина посередині» (MITM), зловмисник може втрутитися у передавання даних, прочитати або навіть модифікувати їх до моменту включення у блок;
– загрози для Off-Chain даних, у багатьох сучасних децентралізованих застосунках (DApps) лише хеш або підтвердження зберігається в блокчейні (on-chain), тоді як основний обсяг даних (документи, метадані) зберігається поза мережею (off-chain), наприклад, в IPFS або інших сховищах, ці дані також потребують надійного шифрування;
– перехоплення приватної інформації, конфіденційні дані можуть бути перехоплені у процесі створення, підписання чи передачі транзакцій.

Для вирішення цих проблем необхідні додаткові криптографічні засоби. Проте існуючі стандартні підходи мають суттєві обмеження в контексті децентралізованих систем: симетричне шифрування (напр., AES); асиметричне шифрування (напр., RSA, ECC). *Постановка задачі дослідження* полягає у розробці та аналізі гібридної криптографічної моделі. Така модель поєднує переваги обох підходів. Основний обсяг даних (повідомлення, файл) шифрується за допомогою швидкого симетричного алгоритму (AES) з унікальним, випадково згенерованим сесійним ключем. Сам сесійний ключ AES шифрується за допомогою повільного, але надійного асиметричного алгоритму (ECC), використовуючи публічний ключ одержувача. Зашифровані дані та зашифрований сесійний ключ безпечно передаються одержувачу. Такий підхід дозволяє досягти як високої продуктивності, так і безпечного обміну ключами у децентралізованому середовищі. Для досягнення поставленої мети дослідження було поділено на

три основні етапи, що охоплюють теоретичний аналіз, практичне моделювання та експериментальну оцінку.

1. Теоретичний аналіз предметної області (обсяг 1): огляд стану безпеки; порівняльний аналіз алгоритмів; детальний порівняльний аналіз основних криптографічних методів; проаналізовано його переваги та режими роботи; досліджено класичний асиметричний підхід та його недоліки (великі ключі, низька продуктивність); виявлено переваги ECC над RSA, зокрема значно менший розмір ключів при еквівалентному рівні безпеки (напр., 256-біт ECC ≈ 3072-біт RSA); досліджено актуальні задачі та напрямки розвитку гібридної криптографії, включаючи інтеграцію з постквантовими алгоритмами (PQC) та вбудовування криптографії у смарт-контракти.

2. Практичне моделювання та обґрунтування вибору (обсяг 2): на основі аналізу загроз визначено детальні функціональні та нефункціональні вимоги до захищеної системи, включаючи конфіденційність, цілісність, захищений обмін ключами, високу продуктивність та сумісність з блокчейн-архітектурою; обґрунтування вибору алгоритмів: для реалізації гібридної моделі було обґрунтовано вибір конкретних стандартів; обґрунтування вибору інструментів: для програмної реалізації та моделювання було обрано бібліотеку PyCryptodome для мови Python.

3. Розробка та експериментальна оцінка (обсяг 3): розроблено загальну архітектуру гібридної криптографічної системи; проведено аналіз інтеграції з блокчейн; досліджено практичні сценарії інтеграції розробленої моделі з блокчейн-середовищем; обґрунтовано доцільність моделі захисту "off-chain" даних; проведено експериментальне тестування продуктивності розробленого прототипу; результати підтвердили, що симетричні операції (шифрування/дешифрування даних) є надзвичайно швидкими (близько 1.1-1.2 мс), тоді як асиметричні (генерація ключів) є більш тривалими (4.3 мс), це доводить, що гібридна модель є високоефективною, оскільки «важкі» асиметричні операції виконуються рідко, а «швидкі» симетричні – для основного обсягу даних.

У ході роботи було проведено комплексне дослідження гібридних методів шифрування та їх застосування для забезпечення захисту інформації у блокчейн-середовищах. На основі теоретичного аналізу встановлено, що поширена думка про "повну" безпеку блокчейну є хибною: технологія гарантує цілісність та незмінність, але не конфіденційність даних. Підтверджено, що гібридна криптографія, яка поєднує сильні сторони обох підходів — високу швидкодію симетричних алгоритмів (зокрема AES) та безпечну передачу ключів асиметричних алгоритмів (зокрема ECC) – є оптимальним рішенням для досягнення балансу між продуктивністю та безпекою в децентралізованих мережах. У практичній частині проаналізовано інструментальні засоби реалізації. Змодельовано сценарії шифрування, обміну ключами та перевірки цілісності повідомлень. Результати кількісних тестів показали, що обрана криптографічна модель дуже ефективна. Вимірювали час виконання різних операцій, і виявилося, що найбільш трудомісткі асиметричні операції (наприклад, генерація ключів ECC або обчислення секрету ECDH) виконуються не часто, тоді як основні операції шифрування та дешифрування даних за допомогою AES-GCM виявилися дуже швидкими (близько 1,1–1,2 мс). Це означає, що запропонована гібридна модель не впливає сильно на швидкість і підходить для великих систем та DApps. Сформовано практичні способи інтеграції моделі з блокчейн-архітектурою. Отримані результати можуть бути основою для розробки реальних модулів та рішень у сфері безпечного передавання даних у системах Web3.

Література:

1. ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. Київ : ДП УкрНДНЦ, 2015. 28 с.
2. ДСТУ 3582:2013. Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила (ISO 4:1984, NEQ; ISO 832:1994, NEQ) / Нац. стандарт України. Київ : Мінекономрозвитку України, 2014. 18 с.