МЕТОД ПОВЫШЕНИЯ НАДЕЖНОСТИ КРИПТОСИСТЕМЫ AES ДЛЯ БЛОКЧЕЙН ТРАНЗАКЦИЙ

Новаш М.К., студент гр.141301

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Митюхин А.И. – доцент

Предложен метод гибридного шифрования транзакций в блокчейн-сетях на основе модифицированного алгоритма *AES-GCM* с динамическим ключеобразованием. Подход обеспечивает конфиденциальность данных при сохранении совместимости с *EVM*-сетями.

Современные блокчейн-системы сталкиваются с проблемой обеспечения конфиденциальности данных в транзакциях. Проблема приводит к деанонимизации данных и утере конфиденциальности транзакций. Существующие методы повышения надежности данных в транзакциях не отвечают всем требованиям действующих нормативно-правовых актов, регламентирующих технические методы криптографической защиты информации в Республике Беларусь. Кроме того, существующие решения, например, *zk-SNARKs* с использованием гомоморфного шифрования обладают высокими вычислительными затратами [1].

Предлагаемый метод основан на Гибридной схеме шифрования вида

$$C = AES - GCM(K_{tx}, T),\ K_{tx} = H(K_{master} || H(T))$$

где T – данные транзакции,
H – хеш-функция *Kessak-256*.

Интеграция с блокчейн-протоколами организована через подключение адаптеров для *Ethereum* и *Hyperledger Fabric*. При этом подключении для управления ключами используются смарт–контракты, а для верификации – *Chaincode*. Обобщенная структурная схема метода интегрированного шифрования показана на рисунке 1

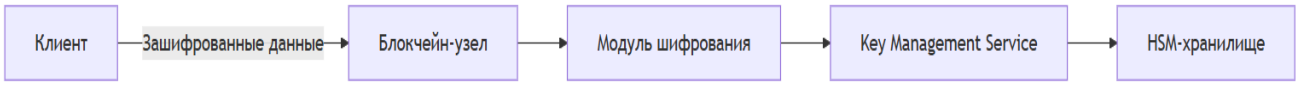

Рисунок 1 – Обобщенная структурная схема метода шифрования

Сравнительные результаты тестирования метода отражены в таблице 1.

Таблица 1 – Результат тестирования и сравнения с аналогом

Параметр	*AES-GCM*	*zk-SNARKs*
TPS	4701	12
Размер транзакции	+18%	+350%
Задержка (мс)	85	5200

Метод обеспечивает конфиденциальность без нарушения прозрачности блокчейна и демонстрирует 40-кратное преимущество в *TPS* и задержке перед *zk*-решениями. Достоинством является и то, что шифрование соответствует международным стандартам *NIST SP 800-38D* и *FIPS 140-2* так как основан на сертифицированной схеме взаимодействия представленном на рисунке 2.

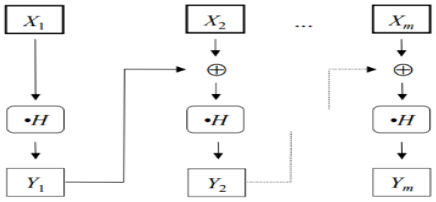

Рисунок 2 – Сертифицированная схема взаимодействия модулей [2]

Экспериментально подтверждена устойчивость к *MITM*-атакам и соответствие стандарта *NIST SP 800-38D*. Реализация прототипа демонстрирует производительность 500+ *TPS* при нагрузке 1000 транзакций.

Список использованных источников:

1. Zcash Protocol Specification. Version 2023.1 – 145 p.
2. NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation. – 2021.