ОБЧИСЛЮВАЛЬНА ТА КОМУНІКАЦІЙНА СКЛАДНІСТЬ ПРОТОКОЛУ РОЗПОДІЛЕНОГО ШИФРУВАННЯ НА ОСНОВІ ШИФРУ ЕЛЬ-ГАМАЛЯ

Доценко М.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Шифр Ель-Гамаля є відомим алгоритмом гомоморфного шифрування, який широко застосовується в протоколах безпечних багатосторонніх обчислень (SMPC), наприклад, у протоколах розподіленого електронного голосування [1-3]. Для забезпечення децентралізації та усунення єдиного центру довіри у фінальних стадіях таких протоколів використовується протокол розподіленого розшифрування [2], який забезпечує розшифрування шифртекстів Ель-Гамаля лише за умови участі визначеної кількості довірених учасників, що володіють своїми частковими секретними ключами. Такий підхід підвищує стійкість системи до компрометації окремих вузлів і гарантує безпеку колективного розкриття даних.

Метою доповіді є експериментальне дослідження обчислювальної та комунікаційної складності протоколу розподіленого розшифрування Ель-Гамаля, реалізованого в криптосистемах еліптичних кривих secp256k1, secp384r1 та secp512r1, що належать до стандартів SECG SEC2 та NIST SP 800-186 [4].

В доповіді наводяться результати експериментального вимірювання часових та комунікаційних характеристик протоколу розподіленого розшифрування Ель-Гамаля на еліптичних кривих secp256k1, secp384r1 та secp521r1. Отримані дані демонструють лінійну залежність як обчислювальної, так і комунікаційної складності протоколу від кількості його учасників. Реалізація на еліптичній кривій secp256k1 виявилася найефективнішою за швидкодією та обсягом переданих даних, тоді як дві інші розглянуті криві більшого порядку забезпечують вищий рівень криптографічної стійкості ціною пропорційного зростання часових і комунікаційних витрат.

Список літератури

1. Zhang, J., Zhang, B., Nastenko, A., Balogun, H., Oliynykov, R. Privacy-Preserving Decision-Making over Blockchain. DOI: https://doi.org/10.1109/TDSC.2022.3231237

2. Felix Brandt. Efficient Cryptographic Protocol Design Based on Distributed El Gamal Encryption. DOI: https://doi.org/10.4018/IJITSA.304810

3. 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.

4. SEC 2: Recommended Elliptic Curve Domain Parameters. URL: https://www.secg.org/sec2-v2.pdf