УДК 004.056

ВИКОРИСТАННЯ ZERO KNOWLEDGE PROOF ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ІДЕНТИФІКАЦІЇ ОСОБИ

Хотян М.О., Побіженко І.О.
e-mail: mykhailo.khotian@nure.ua
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна

This work focuses on the application of Zero Knowledge (ZK) protocols to enhance the security and privacy of user authentication and personal data verification. It explores how ZK proofs can be used to authenticate users without revealing sensitive personal information, such as passwords, and examines the potential of ZK protocols in verifying the validity of personal data while preserving privacy. The paper discusses various cryptographic methods, including Groth16 and PLONK, and highlights the advantages of using these protocols to prevent unauthorized access and reduce the risk of data leaks.

З кожним роком все гостріше постає проблема ідентифікації користувача – яку інформацію користувач має передати іншій стороні для доведення того, що він людина. Це може бути номер телефона або електронна пошта – інформація, яка майже не дає персональної інформації про користувача, проте кожна людина може мати безліч номерів телефонів або поштових адрес. Цей метод вже широко використовується, проте ризик використання цих даних іншою стороною вимагає захисту таких даних. Один з таких методів - використання Zero Knowledge протоколу (надалі – ZK).

Протоколи з нульовим розголошенням (вони ж ZK) є криптографічними методами, які дозволяють одній стороні (доказувачу) підтвердити іншій стороні (верифікатору) істинність певного твердження без розкриття будь-якої додаткової інформації, окрім факту істинності самого твердження. Будь-який протокол нульового розголошення має відповідати трьом основним вимогам:

1. Повнота (Completeness): Якщо твердження є істинним і доказувач слідує протоколу, то чесний верифікатор отримає підтвердження істинності з великою ймовірністю.
2. Звук (Soundness): Якщо твердження є хибним, то навіть обманний доказувач не зможе переконати чесного верифікатора у його істинності, за винятком малоймовірних випадків.
3. Нульове розголошення (Zero-Knowledge Property): Верифікатор не отримує жодної додаткової інформації, окрім факту, що твердження є істинним.

На сьогодні найпоширенішими верифікаторами для доказів з нульовим розголошенням є Groth16 та PLONK. Groth16 забезпечує високу ефективність та компактність доказів, однак вимагає довіреної початкової

установки (trusted setup) для кожного нового кола. PLONK, натомість, є більш універсальним і підтримує єдиний trusted setup для різних схем, що робить його більш привабливим для масштабованих застосувань та не вимагає довіри до проведеної ptau-церемонії для генерації trusted setup.

Для ілюстрації того, як протоколи з нульовим розголошенням (ZK) можуть підвищити рівень захисту персональної інформації, розглянемо проблему автентифікації користувачів. Більшість сучасних веб-сайтів не зберігають паролі у відкритому вигляді, а зберігають результати, отримані за допомогою односторонніх криптографічних функцій, таких як криптографічні хеш-функції. Це запобігає прямому витоку паролів у разі компрометації бази даних, оскільки обчислення преобразу для односторонньої функції є обчислювально складною задачею, пов’язаною, зокрема, з проблемою дискретного логарифмування. Однак, традиційна схема автентифікації все ще передбачає необхідність передачі пароля значення серверу для перевірки коректності введених даних. Такий підхід зберігає ризик компрометації пароля під час його передачі або у випадку атаки на сервер. Використання протоколів з нульовим розголошенням дозволяє усунути цю вразливість: клієнт може локально згенерувати zk-доказ знання правильного пароля без його розголошення та надіслати цей доказ серверу для перевірки. Це дозволяє реалізувати автентифікацію без необхідності передавання пароля чи його хешу, усуваючи потенційні вектори атак, пов’язані з компрометацією серверної інфраструктури.

Ще одним прикладом застосування протоколів з нульовим розголошенням є забезпечення анонімності під час голосування. Використання ZK-протоколів дозволяє зберегти конфіденційність виборця, одночасно підтверджуючи факт його участі в голосуванні. Зокрема, можна довести, що особа проголосувала за певний варіант, не розкриваючи її особисту інформацію, або ж просто підтвердити факт того, що вона брала участь у голосуванні, без розкриття її вибору. Це може бути використано для створення системи анонімних голосувань, що гарантують безпеку приватної інформації та унеможливить відстеження походження голосу. Така система може бути використана для надання можливості кожному користувачу робити анонимні опитування за будь-якою темою та гарантовувати анонімність та безпеку всіх опитуваних.

Список використаних джерел:

1.Goldreich, O., Micali, S., & Wigderson, A. (1986). Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. Journal of the ACM, 38(3), 691-729.

2. Jens Groth, "On the Size of Pairing-Based Non-Interactive Arguments," EUROCRYPT 2016. URL:https://eprint.iacr.org/2016/260 (дата звернення: 03.03.2025).