УДК 003.26:004.421:004.428
Кацюба М.В.[1], Неласа Г.В.[2]
[1] студ. гр. БК-710 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

РЕАЛІЗАЦІЯ НЕІНТЕРАКТИВНОГО ПРОТОКОЛУ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ В СХЕМАХ АВТЕНТИФІКАЦІЇ

Одним із сучасних методів автентифікації є автентифікація з використанням систем доказів з нульовим розголошенням.

Доказ із нульовим розголошенням — це криптографічний протокол, який дозволяє стороні, що доводить, підтвердити істинність твердження іншій стороні (верифікатору), при цьому не розкриваючи ніякої додаткової інформації про нього (ні змісту, ні джерела, з якого доказуючий дізнався про правдивість) [1].

Приклади проектів, що використовують докази з нульовим розголошенням в автентифікаційних схемах:

Proton Mail – сервіс веб-пошти із шифруванням. Для автентифікації використовує протокол парольної автентифікації SRP (Secure Remote Password), який дозволяє користувачеві доводити серверу, що знає пароль, не розкриваючи його. На етапі реєстрації клієнт обчислює та відправляє на сервер верифікатор. При генерації верифікатора використовується пароль, але пароль ніколи не потрапляє на сервер. Відновити пароль за допомогою верифікатора неможливо [2].

Iden3 – це рішення SSI (Self-Sovereign Identity), яке дозволяє користувачам використовувати свої вже існуючі перевірені ідентифікатори. Завдяки SSI вони можуть довести, що вони є тими, за кого себе видають, на основі доказів нульового знання.

Одним із прямих застосувань технології iden3 є дозвіл веб-додаткам використовувати ці ідентифікатори для автентифікації. Зокрема для систем автентифікації використовує принцип неінтерактивної взаємодії, тобто після запиту автентифікації від сервера клієнт самостійно генерує доказ і один раз відправляє його серверу (верифікатору) на перевірку.

Iden3 підтримує Groth16 для генерації та перевірки доказів [3].

Процес автентифікації, який реалізовано в iden3, можна поділити на кроки:

Крок 1. Сервер генерує запит на автентифікацію. Він може бути доставлений користувачеві через різні канали зв’язку: QR-код, електронну пошту, Deep Links тощо.

Крок 2. Клієнт аналізує запит, генерує доказ і надсилає відповідь на URL-адресу зворотного виклику.

Крок 3. Сервер перевіряє доказ і, в залежності від результату перевірки, приймає або відхиляє авторизацію.

Метою даної роботи є реалізація схеми автентифікації від iden3 з використанням одного із сучасних протоколів з нульовим розголошенням.

Для реалізації у якості протоколу з нульовим розголошенням для генерації та перевірки доказів було обрано сучасний протокол Plonky2 [4].

Його основні риси: використовує FRI [5] замість схем на еліптичних кривих; є рекурсивним протоколом: розбиває доказ на окремі докази, які обчислюються паралельно, і потім об'єднуються в один доказ; використовує основне просте поле Галуа за модулем $p = 2^{64} - 2^{32} + 1$, яке дозволяє оптимізувати обчислення на апаратному рівні.

Завдяки цим рисам Plonky2 є швидким протоколом, який можна використовувати у системах, де необхідна швидкодія.

У якості мови програмування була обрана мова програмування Rust. Він є сучасним аналогом C++, проте, на відміну від нього, реалізовує автоматичне керування пам'яттю, що захищає від проблем, які виникають через низькорівневу роботу з пам'яттю.

Також для Rust існує бібліотека plonky2, який дозволяє зручно вбудовувати цей протокол у проекті.

На даний момент розробляється практична реалізація даної системи автентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems. SIAM journal on computing. 1989. Т. 18, № 1. С. 186–208.

2. Butler B. Improved authentication for email encryption and security | Proton. Proton. URL: https://proton.me/blog/encrypted-email-authentication.

3. Login protocol - iden3 documentation. Iden3 Documentation. URL: https://docs.iden3.io/protocol/zklogin/.

4. GitHub - 0xPolygonZero/plonky2. GitHub. URL: https://github.com/0xPolygonZero/plonky2.

5. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. Electronic Colloquium on Computational Complexity. 2018. № 2. С. 12–19.