УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.128

ПРИНЦИПИ РОБОТИ ZKP ТА ПРОТОКОЛ ІДЕНТИФІКАЦІЇ ШНОРРА

Наконечний В.В.
Науковий керівник – к.т.н, доц. каф. ІУС Сердюк Н.М.
Харківський національний університет радіоелектроніки,
м.Харків, Україна
e-mail: volodymyr.nakonechnyi@nure.ua

Zero-Knowledge Proof is a cryptographic method used in digital authentication to verify information without revealing sensitive data. This allows the parties to confirm the accuracy of the information without revealing the details. This approach is valuable to governments and organizations seeking to protect data privacy while simultaneously verifying information. Zero-knowledge verification is used in a variety of digital contexts, including identity verification, authentication, anti-spam, secure payments, account management, and more.

У різних сферах діяльності часто виникають ситуації, коли необхідно підтвердити виконання роботи, залишаючи деталі виконання конфіденційними. Один із типових прикладів - передача важливих відомостей, де потрібно підтвердити певні характеристики без розголошення додаткової інформації. Сюди входять аутентифікація користувача, онлайн платежі, електронні вибори, боротьба зі спамом, управління акаунтами, та збереження анонімності.

Розуміння суті доказу нульового знання можна проілюструвати за допомогою ігрової колоди карт. Одна сторона може передати іншій карту, стверджуючи, що вона має певний колір, але з об'єктивних причин не надає докладні деталі. У таких випадках сторона, що передає карту, може взяти колоду і відокремити всі картки певного кольору, показуючи тим самим, що вона дійсно складається з карт одного кольору. Це демонструє, що передана карта відповідає вказаному кольору без розголошення додаткових деталей.

Протокол Ідентифікації Шнорра (Schnorr Identification Protocol) та нульзнання (Zero-Knowledge Proofs, ZKP) є важливими концепціями в області криптографії та інформаційної безпеки.

Протокол Ідентифікації Шнорра широко використовується в області криптовалют. Наприклад, у покращеному біткойн-протоколі “Тапрут” (Taproot), який спрямований на підвищення приватності та ефективності трансакцій. Ще однією перевагою протоколу Шнорра є його стійкість до підслуховування. Навіть якщо зловмисник прослуховує певну кількість підписаних повідомлень, важко вивести закритий ключ. Іноді протокол Ідентифікації Шнорра поєднується з кільцевими підписами (Ring Signatures) для досягнення більшої анонімності.

ZKP використовуються для розв'язання різноманітних завдань, таких як доказ володіння конкретною інформацією, відтворення доказів без розкриття деталей тощо.

В області криптовалют ZKP використовуються для забезпечення конфіденційності та приватності транзакцій. Наприклад, протокол zk-SNARK використовується у Zcash. ZKP можуть служити для забезпечення безпеки мульти партійних виборів, де кожен голосуючий може підтверджувати свій вибір, не розкриваючи його. Постійно відбуваються дослідження та розробки нових протоколів нуль-знання, що розширюють можливості застосування цих концепцій.

Обидва ці принципи визначають сучасні стандарти конфіденційності та безпеки в різних сферах, від криптовалют до кібербезпеки. їх комбінування та застосування можуть сприяти створенню ефективних та безпечних інформаційних систем.

Подана вище ситуація є наочним прикладом застосування доказів нульового знання у реальному житті. Проте, подібні випадки можуть виникати і в цифровому просторі, коли особі необхідно підтвердити певні відомості чи коректність даних, не розкриваючи деталей про виконану роботу. Для ефективного використання алгоритмів доказів нульового знання у цифровому середовищі, необхідно дотримуватися певних принципів [2]:

1. чесність сторін. Якщо твердження коректне, то чесна сторона, яка його доводить, зможе це довести іншій чесній стороні отримувачу;
2. обгрунтованість наведених доказів. Якщо твердження не коректне, то сторона доведення не може задовольнити сторону отримувача;
3. суть доказу нульового знання полягає в тому, що при наданні доказів особі абсолютно не має бути відомо додаткової інформації про твердження, крім того, що воно є правильним.

Також розрізняють різні схеми підтвердження доказу, а саме інтерактивна і не інтерактивна відповідно [2]:

— інтерактивна схема вимагає того, аби існувала сторона, що проводить підтвердження того, що твердження є вірним – верифікатор;

— не інтерактивна схема – передбачає, що створення доказу базується на загальних параметрах і що доказ може бути перевірений ким завгодно.

Прикладом роботи інтерактивної схеми є верифікація особистості у мобільному додатку «Дія» за допомогою сервісу BANKID. Використовуючи банківський додаток для верифікації в «Дія», можна підтвердити свою особистість без передачі чутливих даних.

Проте із не інтерактивною схемою коли немає верифікатора найкраще підходить не інтерактивний протокол ідентифікації Шнорра [1]. Він передбачає собою підтвердження того, що одна людина знає те, що і інша.

Протокол ідентифікації Шнорра реалізується за таким алгоритмом [3]:

1. Визначимо просте число p і g, а також секретний ключ x.
2. Обчислимо значення X за наступною формулою:

$$X = g^x mod\ p$$

3. Сторона, яка доводить генерує випадкове число y і обчислює значення Y:

$$Y = g^y mod\ p$$

4. Сторона, яка доводить надсилає стороні верифікатору значення Y.
5. сторона верифікатор генерує випадкове число c і надсилає його стороні, що доводить.
6. Сторона, яка доводить отримує c і обчислює значення z за формулою:

$$z = y + c * x$$

7. Сторона доведення надсилає стороні верифікатора значення z.
8. Сторона верифікатор проводить наступні операції по верифікації отриманих значень, а саме обчислює дві змінні v1 і v2:

$$v1 = g^z mod\ p$$

$$v2 = (Y * X^c) mod\ p$$

9. Верифікатор обчислює змінні v1 і v2 та перевіряє їх на рівність. Якщо вони рівні, значення вважається правильним, в іншому випадку - неправильним.
10. У процесі верифікації, якщо значення v1 і v2 однакові, це свідчить про те, що і верифікатор, і сторона, що доводить, знають, що значення, яке має сторона, що доводить, ідентичне значенню сторони верифікації.

Реалізація роботи алгоритму ідентифікації Шнорра наведена за посиланням: https://colab.research.google.com/drive/1-BR95Wz-ip5tLvhSE0Zk8PBKI2AdrFjh?usp=sharing.

Список використаних джерел

1. 8235. RFC. Official edition. Newcastle upon Tyne, 2017. 12 p. 4.
2. Computerphile. Zero Knowledge Proofs - Computerphile, 2017. *YouTube*. URL: https://www.youtube.com/watch?v=HUs1bH85X9I (date of access: 29.02.2024).
3. Schnorr Identification Scheme - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/schnorr-identification-scheme/ (date of access: 29.02.2024).