УДК 004.8

ВИКОРИСТАННЯ ПРОТОКОЛІВ ZKP ТА ІДЕНТИФІКАЦІЇ ШНОРРА

Наконечний В. В.
Науковий керівник – к.т.н, доц. каф. ІУС Сердюк Н. М.
Харківський національний університет радіоелектроніки, каф. ІУС,
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, боротьба зі спамом та управління акаунтами тощо. Оскільки витік чутливих даних може спричинити суттєві репутаційні, фінансові та навіть привести до проблем із законом із-за неналежного захисту даних під час проведення операцій із ними.

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

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, що відображає всю суть протоколу доказу нульового-знання.

Протокол ідентифікації Шнорра широко використовується в області криптовалют. Наприклад, у покращеному біткойн-протоколі «Тапрут» (Taproot), який спрямований на підвищення приватності та ефективності транзакцій. 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. Оскільки під час транзакцій у протоколі «Тапрут» використовується саме протокол ідентифікації Шнорра це дозволяє зберегти спільний секрет обох сторін не розголошуючи деталей про нього, що відповідно підвищує безпеку транзакцій.

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

Наведена ситуація із колодою карт 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 додаткових деталей. Для ефективного використання протоколів доказу 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.

Проте із неінтерактивною схемою коли немає верифікатора найкраще підходить неінтерактивний протокол ідентифікації Шнорра [1]. Він передбачає собою підтвердження того, що одна сторона знає те, що і інша.

Протокол ідентифікації Шнорра реалізується за наступним 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 *v*1 і *v*2:

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

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

9. Верифікатор обчислює змінні *v*1 і *v*2 та перевіряє їх на рівність. Якщо вони рівні, значення вважається правильним, в іншому випадку – неправильним.
10. У процесі верифікації, якщо значення *v*1 і *v*2 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 алгоритму Шнорра мовою програмування python наведена за посиланням [4].

Таким чином, базуючись лише на тому, що дві сторони володіють одним спільним секретом, використовуючи протокол ідентифікації Шнорра можна ефективно та безпечно підвердити вірність твердження.

Список використаних джерел:

1. 8235. RFC. Official edition. Newcastle upon Tyne, 2017. 12 p.
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).
4. Наконечний В. В. Google Colaboratory. Google Colab. URL: https://colab.research.google.com/drive/1-BR95Wz-ip5tLvhSE0Zk8PBKI2AdrFjh?usp=sharing. (date of access: 23.03.2024).