УДК 004.056.5:004.4

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ ДОКАЗІВ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Прядко В. С.
Науковий керівник – к.т.н., Голян Н. В.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна
e-mail: vladyslav.priadko@nure.ua

The article provides an overview of zero-knowledge proofs (ZKPs), emphasizing their role in ensuring privacy and data protection in technologies such as blockchain. It explains ZKP as a method that allows proving truth without revealing basic details, ensuring security in digital interactions. The text compares several ZKP protocols, including zk-SNARKs, zk-STARKs, Bulletproofs, and PLONK, highlighting their unique features, applications, and tradeoffs between efficiency, security, and privacy.The discussion reflects ZKP's ongoing development to overcome current limitations while offering a future in which privacy and verification are harmoniously integrated.

У сучасному світі, де конфіденційність та безпека даних стають все більш важливими, існує потреба в технологіях, які дозволяють перевіряти та взаємодіяти з приватними даними без їх розголошення. Традиційні методи криптографії часто вимагають повного розкриття інформації авторизованим сторонам, що може бути неприйнятним в багатьох випадках. Альтернативні рішення, такі як повністю гомоморфне шифрування та безпечні багатосторонні обчислення, мають значні обмеження щодо ефективності та масштабованості.

Проблема полягає в знаходженні оптимального протоколу та схеми для формування доказів прикладних задач з реального життя, які забезпечать баланс між конфіденційністю, безпекою та ефективністю. Протоколи доказів з нульовим розголошенням (ZKP) є перспективним рішенням, здатним задовольнити ці вимоги.

Докази з нульовим знанням (ZKP) – це сімейство криптографічних методів, які дозволяють доводити достовірність тверджень без розкриття інформації, що лежить в їх основі. Вони передбачають інтерактивний протокол між тим, хто доводить, що володіє секретними знаннями, і тим, хто перевіряє. Верифікатор переконує верифікатора через взаємодію "виклик-відповідь", яка розкриває достатньо інформації для встановлення достовірності, зберігаючи при цьому конфіденційність. ZKP задовольняють трьом властивостям: повнота (якщо твердження істинне, то верифікатор переконаний), достовірність (якщо твердження хибне, то верифікатор не може бути обманутий) і нульове знання (верифікатор не дізнається нічого, окрім істинності твердження).

Унікальність ZKP полягає в тому, що вони задовольняють ці властивості одночасно. Особливо примітною є властивість нульового знання, яка дає змогу дописувачу розкрити секрет, що охороняється, без його розголошення. ZKP мають практичне застосування в обчисленнях зі збереженням конфіденційності, безпечних багатосторонніх обчисленнях, технологіях блокчейн і перевірених аутсорсингових обчисленнях. В епоху, коли цінується конфіденційність і захист даних, ZKP уможливлюють безпечну співпрацю, транзакції та заяви, які можна перевірити, не ставлячи під загрозу конфіденційну інформацію. Крім застосувань в обчисленнях з конфіденційністю та масштабуванні блокчейнів, протоколи доказів із нульовим розголошенням також мають потенціал для підвищення ефективності та безпеки децентралізованих фінансових протоколів, таких як автоматизовані маркет-мейкери (AMM). AMM використовують математичні моделі для динамічного встановлення цін та забезпечення ліквідності для торгівлі криптоактивами [1]. Інтеграція ZKP в алгоритми пулів ліквідності AMM може дозволити конфіденційне відстеження резервів та забезпечити криптографічні докази правильності цінової динаміки без повного розкриття внутрішніх даних.

З розвитком технологій дослідники продовжують вивчати нові підходи і вдосконалювати існуючі протоколи для розробки більш ефективних, масштабованих і безпечних систем з нульовим рівнем розголошення знань, підживлювані бажанням розкрити весь їхній потенціал для майбутнього, в якому співіснують конфіденційність і можливість верифікації. У динамічній сфері доведень з нульовим знанням з'явився різноманітний набір протоколів, кожен з яких пропонує унікальні можливості і використовує окремі математичні основи. Першопрохідцями в цій галузі є zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge – стислий неінтерактивний аргумент знання з нульовим знанням), який привернув до себе велику увагу і отримав широке розповсюдження. Ці протоколи використовують можливості квадратичних арифметичних програм (QAP) [2], представляючи обчислення у вигляді складних поліноміальних рівнянь. Покладаючись на знання секретного оціночного ключа, згенерованого на етапі довіреного налаштування, zk-SNARK створюють стислі докази постійного розміру, які можна ефективно перевірити, що робить їх добре придатними для застосування в криптовалютах, що зберігають конфіденційність, таких як Zcash, а також для перевірених обчислень і безпечних сценаріїв аутсорсингових обчислень. Однак їхня залежність від криптографії еліптичних кривих, білінійних пар та поліноміальних схем зобов'язань також створює складнощі та потенційні вразливості [3].

Усуваючи деякі обмеження zk-SNARKs, протокол zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) пропонує альтернативний підхід. Побудований на основі інтерактивних доведень з

оракулом (IOP), алгебраїчних методів, таких як тестування низьких степенів, і поліноміальних зобов'язань, zk-STARKs має на меті забезпечити прозорі і масштабовані доведення з нульовим знанням без необхідності довірених налаштувань. Запозичені з таких областей, як теорія кодування, інтерактивні доведення та алгебраїчна геометрія, zk-STARKs знайшли застосування в рішеннях для масштабування блокчейну, верифікованих обчисленнях і машинному навчанні, що зберігає конфіденційність. Хоча їхні докази, як правило, більші, ніж у zk-SNARK, вони пропонують переваги пост-квантової безпеки і пом'якшують припущення про довіру, притаманні довіреним системам.

Інший відомий протокол, Bulletproofs, використовує новий підхід до доказів з нульовим рівнем знання, зосереджуючись на менших розмірах доказів, зберігаючи при цьому ефективну перевірку. Заснований на евристиці Фіата-Шаміра для перетворення інтерактивних протоколів в неінтерактивні аргументи, Bulletproofs використовує криптографію на основі дискретного логарифму, зобов'язання Педерсена та векторні зобов'язання. Ця унікальна комбінація призвела до їх застосування в криптовалютах, що зберігають конфіденційність, таких як Monero, і смарт-контрактах, що зберігають конфіденційність, де компактні розміри доказів є вкрай бажаними. З нещодавніх розробок, протокол PLONK [4] став багатообіцяючим претендентом, пропонуючи стислі та ефективні докази без необхідності довіреної церемонії налаштування. Використовуючи нову схему поліноміальних зобов'язань, засновану на базисах Лагранжа і тензорних добутках, PLONK забезпечує універсальні і оновлювані доведення з нульовим знанням. Спираючись на концепції схем поліноміальних зобов'язань, базисів Лагранжа, тензорних добутків і таких методів, як перестановка аргументів і лінійні арифметичні схеми, PLONK набув популярності в блокчейн-додатках, обчисленнях із збереженням конфіденційності та сценаріях обчислень, що піддаються перевірці.

Окрім цих відомих протоколів, сфера доведень з нульовим знанням продовжує розвиватися, дослідники вивчають нові підходи та вирішують конкретні проблеми. Протокол zk-PIRGs (Zero-Knowledge Proofs for Iterated Rational Geometric Series) фокусується на ефективній перевірці обчислень на великих наборах даних, знаходячи застосування у верифікованих аутсорсингових обчисленнях і машинному навчанні, що зберігає конфіденційність. Sonic (Zero-Knowledge by Certifying Completeness), з іншого боку, має на меті забезпечити прозорі та масштабовані докази без довірених налаштувань, використовуючи інтерактивні оракулові докази та алгебраїчні методи. Ligero, оптимізований для доведення і перевірки правильності обчислень в оперативній пам'яті, має потенційне застосування в безпечних аутсорсингових обчисленнях і рішеннях для масштабування блокчейну. ZKBoo, з його акцентом на ефективні докази задовільності булевих схем,

знаходить застосування в смарт-контрактах, що зберігають конфіденційність, і обчисленнях, які можна верифікувати. Крім того, протоколи доказу з нульовим знанням, засновані на решітковій криптографії, такі як ZKP над решітками, пропонують потенційні переваги пост-квантової безпеки, в той час як підходи, що використовують методи безпечних багатосторонніх обчислень, такі як ZKP від Secure Multiparty Computation, ставлять на перше місце практичну ефективність.

Ця різноманітна сфера протоколів доказу з нульовим розголошенням знань демонструє швидкий темп інновацій і невпинний пошук рішень, пристосованих до конкретних випадків використання, причому кожен протокол пропонує унікальні переваги і компроміси з точки зору розміру доказу, часу перевірки, надійних припущень про налаштування і міркувань пост-квантової безпеки.

Докази з нульовим знанням зробили революцію в галузі криптографії, уможлививши широкий спектр додатків, що зберігають конфіденційність, зберігаючи при цьому можливість перевірки. Різноманітні розглянуті протоколи, кожен з яких має свої унікальні переваги та компроміси, ілюструють постійні дослідження та інновації в цій галузі. Оскільки з'являються нові виклики і випадки використання, розробка більш ефективних, безпечних і універсальних протоколів з нульовим доказом буде продовжувати залишатися важливою сферою досліджень, прокладаючи шлях до майбутнього, в якому конфіденційність і верифікованість гармонійно співіснують.

У висновку, знаходження оптимального протоколу та схеми доказів з нульовим розголошенням для прикладних задач реального життя вимагає ретельного аналізу вимог до конфіденційності, безпеки та продуктивності. Жоден з наявних протоколів не є ідеальним для всіх сценаріїв, тому необхідно оцінити компроміси між розміром доказів, припущеннями довіри, стійкістю до квантових загроз та іншими факторами. Подальші дослідження та інновації у сфері ZKP матимуть вирішальне значення для розробки більш ефективних, масштабованих і гнучких рішень, що відповідають різноманітним потребам конфіденційності та верифікації в майбутньому цифровому середовищі.

Список використаних джерел

1. Comparative Analysis Of Automated Market Makers Liquidity Pools Algorithms / Pryadko V., Golian N. // Ways of Science Development in Modern Crisis Conditions – 2022.

2. Quadratic Arithmetic Programs: from Zero to Hero URL: https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649 (date of access: 08.03.2024).

3. Zk-SNARKs: Under the Hood – https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6 (date of access: 08.03.2024).

4. Thaler J. Proofs, Arguments, and Zero-Knowledge/ J. Thaler // Foundations and Trends in Privacy and Security – 2022. – Vol. 4: No. 2–4, P. 455.