УДК 004.056.55 **DOI:10.30837/rt.2025.3.222.05**

Р.І. МОРДВІНОВ, канд. техн. наук

ПРОТОКОЛИ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ: ТЕОРЕТИЧНІ ОСНОВИ ТА ЗАСТОСУВАННЯ В СУЧАСНІЙ КРИПТОГРАФІЇ

Вступ

У сучасному цифровому світі, де обмін інформацією відбувається постійно, забезпечення конфіденційності та цілісності даних є надзвичайно важливим. Криптографія відіграє ключову роль у захисті інформації, надаючи інструменти для шифрування, аутентифікації та забезпечення безпечного зв'язку. Протоколи з нульовим розголошенням (ZKP) є однією з найбільш інноваційних та перспективних концепцій у криптографії, що дозволяє одній стороні (доказувачу) переконати іншу сторону (верифікатора) у правдивості певної заяви, не розкриваючи при цьому жодної додаткової інформації, крім самого факту її істинності [1].

Поняття доказів з нульовим розголошенням сформувалося в середині 1980-х років завдяки піонерським роботам Ш. Гольдвассер, С. Мікалі та Ч. Ракова, які ввели концепцію «складності знання» в інтерактивних доказах [2]. На той час було показано, що за наявності односторонніх функцій будь-яка мова класу NP має інтерактивний доказ з нульовим знанням, тобто можна переконувати у твердженнях без розкриття секретної інформації. Класичними прикладами кінця 1980-х стали протоколи автентифікації, побудовані за схемою трьохходового обміну (так звані σ-протоколи). Зокрема, схема Фіата–Шаміра і протокол Шнорра дозволили переконливо доводити знання секретного ключа без його розголошення – ці роботи заклали основу поняття Zero-Knowledge у прикладних сценаріях. Важливим етапом розвитку стало усунення інтерактивності: 1988 р. М. Блум, П. Фельдман і С. Мікалі вперше запропонували концепцію неінтерактивних доказів з нульовим розголошенням, коли доведення здійснюється за допомогою спільного випадкового рядка без обміну запитами. Цей результат продемонстрував, що взаємодія не є обов’язковою для збереження нульового розголошення, і відкрив шлях до подальших удосконалень протоколів.

У 1990-х роках теорія ZKP стрімко розвивалася: було доведено повноту ZKP для всього класу NP, розроблялися багатоверифікаторні (multi-prover) системи і застосовувалися нові техніки, такі як докази з перевіркою за допомогою поліномів (ідеї PCP). Ці дослідження підготували ґрунт для появи стислих доказів знання. Починаючи з 2010-х фокус змістився на підвищення ефективності: з’явилися перші практичні реалізації NIZK-доказів для довільних обчислень. Зокрема, було запропоновано конструкції типу zk-SNARK, які дали можливість генерувати дуже короткі докази й перевіряти їх у часі, не залежному від складності твердження. Наприклад, до 2016 р. Й. Грот розробив перевірюваний за мілісекунди SNARK з постійного розміру доказом [5], що стало проривом для використання ZKP на практиці. У 2018 р. з’явилася альтернатива на основі лише геш-функцій – zk-STARK, що не потребує довіреної установки та є стійким до квантових атак [4]. Ці досягнення збіглися з вибухом інтересу до ZKP у контексті блокчейну: якщо перші концепції 1980-х були суто теоретичними, то з середини 2010-х докази з нульовим розголошенням впроваджуються у реальні системи. Яскравий приклад – криптовалюта Zcash, у якій технологія zk-SNARK забезпечила повну приватність транзакцій. Відправник, отримувач і сума платежу приховані, але достовірність транзакції можна перевірити публічно. На платформі Ethereum також з’явилися рішення, що використовують ZKP (проєкти Aztec, StarkWare та ін.) для підвищення конфіденційності і масштабованості смарт-контрактів. Таким чином, станом на зараз ZKP перетворилися з академічного концепту на ключову технологію у сфері криптовалют і розподілених систем.

Базове визначення протоколу з нульовим розголошенням включає три ключові властивості:

- повнота (Completeness). Якщо твердження є істинним, чесний доказувач зможе переконати чесного версифікатора;
- надійність (Soundness). Якщо твердження є хибним, жоден (навіть шахрайський) доказувач не зможе переконати чесного верифікатора (за винятком незначної ймовірності);
- нульове розголошення (Zero-Knowledge). У процесі доведення верифікатор не дізнається нічого, крім того, що твердження є істинним.

Дослідження в галузі протоколів з нульовим розголошенням є досить широким і включає значну кількість наукових праць. Крім фундаментальної роботи Гольдвассер, Мікалі та Ракоффа [2], важливими є праці, що досліджують різні типи ZKP та їхні застосування. Огляд різних конструкцій ZKP можна знайти в роботі [3]. Питання практичної реалізації та ефективності ZKP, особливо в контексті блокчейн-технологій, активно досліджуються в роботі [4]. Останні досягнення в області неінтерактивних доказів з нульовим розголошенням (NIZK), таких як zk-SNARKs та zk-STARKS, детально розглядаються в [5]. Також існують роботи, присвячені вивченню потенційних загроз та обмежень ZKP, включаючи питання масштабованості та стійкості до квантових атак [6, 7].

Протоколи з нульовим розголошенням можуть бути класифіковані на кілька типів залежно від їхніх характеристик.

Інтерактивні та неінтерактивні докази

У інтерактивних протоколах верифікатор та доказувач обмінюються серією повідомлень для підтвердження істинності твердження. Класичним прикладом є протокол Фіата–Шаміра, що використовується для аутентифікації [8]. У такому протоколі верифікатор надсилає випадкові запитання доказувачу, і той має надати правильні відповіді, не розкриваючи секретної інформації.

Неінтерактивні протоколи (Non-Interactive Zero-Knowledge, NIZK) дозволяють доказувачу створити доказ, який може бути перевірений будь-ким без необхідності взаємодії з доказувачем. Перевага NIZK полягає в їхній зручності для практичного застосування, оскільки вони не вимагають постійної присутності обох сторін.

zk-SNARK та zk-STARK

Серед неінтерактивних протоколів особливе місце займають zk-SNARK (Zero-Knowledge Succinct Non-Interactive ARgument of Knowledge) та zk-STARK (Zero-Knowledge Scalable Transparent ARgument of Knowledge).

zk-SNARK є одним з найбільш використовуваних типів NIZK. "Succinct" означає, що розмір доказу є малим і час його перевірки також невеликий, незалежно від складності твердження. "ARgument of Knowledge" вказує на те, що доказувач не просто стверджує, що знає певну інформацію, а й надає криптографічний доказ цього знання. Для створення zk-SNARK часто потрібен початковий етап довіреної установки (Trusted Setup), в якому генеруються спільні параметри для доказувача та верифікатора. Недоліком цього етапу є потенційний ризик, якщо інформація, використана під час установки, потрапить до зловмисників.

zk-STARK є альтернативою zk-SNARK, яка не потребує довіреної установки, що робить їх більш прозорими та безпечними з точки зору криптографічних припущень. "Scalable" вказує на те, що час генерації та перевірки доказів зростає полілогарифмічно зі зростанням складності твердження, що робить їх більш придатними для великомасштабних застосувань. Однак розмір доказів zk-STARK часто більший, ніж у zk-SNARK.

Основні математичні засади

В основі протоколів з нульовим розголошенням лежать різні криптографічні примітиви та математичні концепції.

- Доведення знання дискретного логарифма. Це один з базових прикладів ZKP, де доказувач може переконати верифікатора, що йому відоме значення x таке, що

y = g^x mod p (де g є генератором групи, а p є простим числом), не розкриваючи при цьому самого значення x.

- Гомоморфне шифрування. Деякі протоколи ZKP використовують властивості гомоморфного шифрування, яке дозволяє виконувати певні операції над зашифрованими даними, не розшифровуючи їх. Результат такої операції при розшифруванні відповідає результату тієї ж операції, виконаної над відкритими даними.
- Поліноміальні зобов'язання (Polynomial Commitments). У zk-SNARK та zk-STARK часто використовуються поліноміальні зобов'язання, які дозволяють доказувачу зафіксувати поліном і потім надавати докази щодо значень цього полінома в певних точках, не розкриваючи сам поліном.
- Гешування. Криптографічні хеш-функції використовуються для створення стислих і незворотних представлень даних, що є важливим для забезпечення надійності протоколів.
- Еліптичні криві. У багатьох сучасних криптографічних системах, включаючи ZKP, використовуються еліптичні криві завдяки їхнім високим рівням безпеки при відносно невеликих розмірах ключів.

Приклади практичного застосування

Протоколи з нульовим розголошенням знаходять широке застосування в різних сферах, де потрібна конфіденційність та верифікація даних.

- Криптовалюти. Одним з найбільш відомих прикладів є криптовалюта Zcash, яка використовує технологію zk-SNARK для забезпечення повністю приватних транзакцій. Користувачі можуть здійснювати перекази, приховуючи інформацію про відправника, одержувача та суму транзакції, при цьому зберігаючи можливість перевірити легітимність транзакції. Проєкти на базі Ethereum, такі як Aztec та StarkWare, також активно використовують zk-SNARK та zk-STARK для підвищення приватності та масштабованості транзакцій [4].
- Автентифікація. ZKP можуть бути використані для створення безпечних та приватних систем автентифікації. Користувач може довести, що він володіє певним секретом (наприклад, паролем або біометричними даними), не розкриваючи сам секрет верифікатору. Це може бути використано для покращення безпеки онлайн-акаунтів та інших систем доступу.
- Цифрові ID. Концепція цифрових ідентифікаторів, що зберігають персональну інформацію користувачів, може значно виграти від використання ZKP. Користувач зможе надавати лише ту інформацію, яка необхідна для конкретної ситуації, не розкриваючи зайвих персональних даних. Наприклад, при оренді автомобіля можна підтвердити наявність водійського посвідчення та достатній вік, не показуючи повну копію документа.
- Голосування. Протоколи з нульовим розголошенням можуть бути використані для створення анонімних та верифікованих систем електронного голосування. Виборець може довести, що він має право голосувати, не розкриваючи свій вибір до завершення голосування.
- Доведення володіння секретами. ZKP можуть бути використані для доведення володіння певним секретом, наприклад приватним ключем у криптовалютній системі, без його розкриття.

Сучасні напрями досліджень

Постквантові докази з нульовим розголошенням. Одним з актуальних напрямів є розробка квантостійких ZKP-протоколів. Більшість класичних схем (наприклад, на основі дискретного логарифма чи факторизації) потенційно вразливі перед квантовими алгоритмами. Сучасні дослідження зосереджені на альтернативах, стійких до квантових атак, зокрема на протоколах, що покладаються лише на геш-функції або на складні задачі теорії ґраток. Прикладом є поява прозорих протоколів zk-STARK, які використовують лише криптографічні хеші і вважаються витривалими до квантових обчислень. Інший підхід – ґраткові ZKP: використовуються математичні задачі на ґратках, схожі до тих, що лягли в основу постквантових

підписів. Нещодавно було запропоновано нові методи побудови доказів знання на ґратках, що значно зменшують розмір і покращують продуктивність таких доказів [9]. Хоча поки що ґраткові ZKP поступаються класичним за ефективністю, прогрес у цій галузі триває – вже створено прототипи квантобезпечних схем, придатних для реалізації в протоколах приватності. Постквантовий напрям є критично важливим, адже забезпечить довгострокову безпеку ZKP в умовах появи квантових комп'ютерів.

Zero-Knowledge і машинне навчання (ZKML). Інша передова сфера – поєднання доказів з нульовим розголошенням з методами машинного навчання. ZKML – це новітня технологія, що дозволяє перевіряти результати виконання ML-моделей або певні властивості даних без розкриття самих моделей чи даних. Фактично, ZKP надають інструмент для доведення правильності роботи алгоритму штучного інтелекту, зберігаючи в таємниці і сам алгоритм, і використані для навчання дані. Це відкриває можливості для приватного та верифікованого AI: наприклад, вузол мережі може довести, що виконав Inference нейронної мережі без і закладених «бекдорів», не показуючи модель цілком. Останні дослідження демонструють значний прогрес у цій галузі – розробляються спеціальні фреймворки і бібліотеки, що оптимізують генерацію SNARK-доказів для моделей глибокого. Вже показано, що за допомогою таблиць пошуку й інших прийомів можна прискорити докази для нелінійних функцій (наприклад, ReLU, softmax та ін.) на порядки без втрати точності. Хоча ZKML все ще перебуває на ранніх етапах, він розглядається як ключовий компонент майбутніх *довірених AI*-систем, де користувачі зможуть перевіряти чесність моделей штучного інтелекту, не отримуючи доступу до їх внутрішніх параметрів.

Конфіденційність у Web3 та децентралізованих додатках. Zero-knowledge протоколи відіграють дедалі більшу роль у забезпеченні приватності та безпеки в екосистемі Web3. По-перше, вони лежать в основі самої ідеї *децентралізованої ідентичності* (Self-Sovereign Identity): користувач може мати цифровий ID і доводити окремі атрибути (вік, громадянство, наявність ліцензій тощо) без розкриття повного профілю. Це дозволяє будувати селективне розкриття даних – наприклад, підтвердити право доступу чи виконання регуляторних вимог, не передаючи особистої інформації контрагенту. По-друге, ZKP активно досліджуються для приватності смарт-контрактів і децентралізованих фінансових протоколів. Існують концепції «приватних DeFi», де транзакції та стан контрактів шифруються, а їхня коректність доводиться нульовим розголошенням. Таким чином, можна створювати біржі, кредитні платформи чи аукціони, що зберігають таємницю комерційних даних (балансів, заявок тощо), але залишаються перевіряльними. По-третє, ZKP пропонуються як рішення для регуляторних задач у блокчейні. Зокрема, концепція *zkKYC* передбачає, що користувач проходить перевірку KYC/AML у довіреного провайдера і отримує криптографічне доказ цього, яке може пред'являти в смарт-контрактах. При цьому самі персональні дані (ім'я, документи) не розкриваються блокчейну, але контракт упевнений, що користувач дотримується вимог законодавства. Подібні рішення покликані знайти баланс між анонімністю Web3 та необхідністю відповідати нормативним правилам. Загалом, напрям приватності у Web3 охоплює широкий спектр досліджень – від анонімних облікових записів і соціальних мереж до захищеного обміну даними між організаціями на блокчейні – і Zero-Knowledge докази є ключовою технологією для втілення бачення «приватного децентралізованого Інтернету».

Переваги й виклики

Використання протоколів з нульовим розголошенням має значні переваги, але також пов'язане з певними викликами.

Переваги:

- Підвищення приватності. Основною перевагою ZKP є можливість довести істинність твердження, не розкриваючи жодної зайвої інформації. Це є критично важливим для багатьох застосувань, де конфіденційність даних є пріоритетом.

• Зниження потреби в довірі. У деяких випадках ZKP можуть зменшити або усунути потребу в довірених посередниках. Верифікатор може бути впевнений у правдивості твердження лише на основі наданого доказу.

• Покращення безпеки. Завдяки можливості підтверджувати володіння секретами без їхнього розкриття, ZKP можуть підвищити безпеку різних систем автентифікації та контролю доступу.

Виклики:

• Масштабованість. Генерація та перевірка доказів з нульовим розголошенням може бути обчислювально інтенсивною, особливо для складних тверджень. Покращення масштабованості є однією з ключових проблем у цій галузі.

• Складність реалізації. Розробка та впровадження протоколів з нульовим розголошенням є складним завданням, що вимагає глибоких знань в області криптографії та математики.

• Довірена установка (для zk-SNARK). Необхідність довіреної установки в zk-SNARK створює потенційну вразливість, якщо параметри установки будуть скомпрометовані. Розробка альтернатив, таких як zk-STARK, спрямована на вирішення цієї проблеми.

• Постквантові аспекти. Як і багато сучасних криптографічних систем, деякі ZKP можуть бути вразливі до атак з використанням квантових комп'ютерів. Розробка квантовостійких протоколів з нульовим розголошенням є важливим напрямком досліджень.

Висновки

Протоколи з нульовим розголошенням є потужним інструментом у сучасній криптографії, що відкриває нові можливості для забезпечення приватності, безпеки та достовірності інформації в цифровому світі. Від забезпечення анонімності транзакцій у криптовалютах до створення безпечних систем цифрової ідентифікації, ZKP демонструють свій значний потенціал у різних галузях. Незважаючи на існуючі виклики, такі як питання масштабованості та складності реалізації, активні дослідження та розробки в цій області продовжують просувати технологію вперед. З появою більш ефективних та безпечних протоколів, таких як zk-STARK, можна очікувати ще ширшого застосування протоколів з нульовим розголошенням у майбутніх криптографічних системах.

Список літератури:

1. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM Journal on Computing. 1989. Vol. 18, No. 1. P. 186–208.
2. Goldwasser S., Micali S., Wigderson A. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design // 27th Annual Symposium on Foundations of Computer Science. IEEE, 1986. P. 174–187.
3. Camenisch J., Stadler M. Proof systems for general statements in discrete logarithms. ETH Zurich, 2003. [Електронний ресурс]. Режим доступу: https://crypto.ethz.ch/publications/files/CamSta97b.pdf
4. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // IACR Cryptology ePrint Archive. 2018. No. 046. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/2018/046.pdf
5. Groth J. Short pairing-based non-interactive zero-knowledge arguments // Advances in Cryptology – ASIACRYPT 2010. Lecture Notes in Computer Science, Vol. 6477. Springer, 2010. P. 321–340. [Електронний ресурс]. Режим доступу: https://www.iacr.org/archive/asiacrypt2010/6477323/6477323.pdf
6. Yu R., Liu J. K. A survey of zero-knowledge proof systems // Journal of Computer Science and Technology. 2021. Vol. 36, No. 4. P. 705–727.
7. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. 2018. Vol. 16. P. 38–41.
8. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // Advances in Cryptology – CRYPTO'86. Lecture Notes in Computer Science. Vol. 263. Springer, 1987. P. 186–194. [Електронний ресурс]. Режим доступу: https://mit6875.github.io/PAPERS/Fiat-Shamir.pdf
9. Zero knowledge proofs IBM research project [Електронний ресурс]. Режим доступу: https://research.ibm.com/projects/zero-knowledge-proofs

Надійшла до редколегії 20.05.2025

Відомості про автора:
Мордвінов Руслан Ігорович – кандидат технічних наук, Україна; email: rmordvinov@gmail.com; ORCID: https://orcid.org/0000-0003-1229-2840