УДК 004.056.55 **DOI:10.30837/rt.2025.4.223.04**

Р.І. МОРДВІНОВ, канд. техн. наук

СИСТЕМАТИЗАЦІЯ МЕТОДІВ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Вступ

Приватність та безпека інформації є ключовими вимогами сучасних інформаційних систем. Докази з нульовим розголошенням (ZKP) – це криптографічні протоколи, що дають змогу одній стороні (доказуючому) довести іншій (верифікатору) істинність деякого твердження, не розкриваючи при цьому ніяких додаткових даних, окрім самого факту істинності [1]. Концепція ZKP була вперше сформульована в 1980-х роках у роботах Голдвассер, Мікалі та Ракова [1], де було введено поняття «складності знання» інтерактивних доказів. Відтоді теорія доказів з нульовим знанням інтенсивно розвивалася: було показано, що за наявності односторонніх функцій будь-яка належна до NP мова має доведення з нульовим знанням [6]. Класичними прикладами є протоколи ідентифікації, як-от схема Фіата–Шаміра [3] чи протокол Шнорра [5], що дозволяють довести знання секретного ключа без його розголошення.

Актуальність технологій ZKP стрімко зросла у 2010-х роках у зв'язку з потребою забезпечення конфіденційності в блокчейнах, фінансових транзакціях та інших сферах [7, 11]. Поява практичних реалізацій, зокрема стислих неінтерактивних доказів знання (zk-SNARK) [7] і масштабованих прозорих доказів (zk-STARK) [8], продемонструвала можливість використання ZKP в реальних застосунках – від анонімних криптовалютних платежів до перевірки правильності виконання обчислень на стороні. Це зумовило потребу у впорядкуванні знань про різні методи ZKP, їх класифікації та оцінці сильних і слабких сторін.

Методи доказу з нульовим розголошенням можна класифікувати за кількома ключовими ознаками [2, 11]. Однією з базових є тип взаємодії між доказуючим і верифікатором. За цим критерієм розрізняють інтерактивні протоколи ZKP та неінтерактивні. В інтерактивних протоколах потрібен багаторазовий обмін повідомленнями: верифікатор надсилає випадкові виклики (запити), на які доказуючий відповідає, і така процедура повторюється кілька раундів для досягнення високого рівня довіри [3, 4]. Натомість неінтерактивні докази дозволяють обмежитися одним повідомленням від доказуючого, яке верифікатор може перевірити самостійно без подальших запитань [7]. Перетворення інтерактивного протоколу на неінтерактивний можливе, наприклад, за допомогою геш-евристики Фіата–Шаміра [3, 23]. Неінтерактивні ZKP є особливо привабливими для практичних застосувань (наприклад, у блокчейнах), оскільки не потребують онлайн-взаємодії сторін.

Другим важливим критерієм є математична основа та структура протоколу. За цією ознакою в роботі пропонується виділити алгебраїчні та стохастичні методи доказу. Алгебраїчні методи ґрунтуються на використанні алгебраїчних структур та рівнянь над ними: наприклад, групи з обчислювально складними задачами (дискретний логарифм, факторизація тощо) або поліноміальні представлення обчислень [7, 8]. Такі протоколи часто будуються як σ-протоколи (Sigma-protocols) з трьохходовою схемою «зобов'язання-виклик-відповідь» і мають строгі алгебраїчні властивості (наприклад, лінійність відповідей), що спрощує доказ коректності та нульового розголошення [2, 5]. Натомість стохастичні методи спираються на випадковість та ймовірнісне переконання верифікатора. До них належать, наприклад, класичні протоколи Блума для NP-повних задач (графовий ізоморфізм, гамільтонів цикл тощо), де доказуючий приховує секрет випадковим чином і з певною ймовірністю проходить перевірку [4]. Характерною рисою стохастичних протоколів є наявність ненульової ймовірності обману, тому для надійності їх повторюють багаторазово, зменшуючи цю ймовірність до незначної величини (наприклад, 2^-20 або менше) [4]. Таким чином, алгебраїчні методи зазвичай дають детермінований результат за один раунд (спираючись на

складні алгебраїчні припущення), тоді як стохастичні потребують статистичного підходу з повторенням раундів.

Наступний критерій – умови початкової довіри. Деякі сучасні протоколи потребують так званої довіреної установки (trusted setup): одноразової генерації загальних параметрів, які потім використовуються для побудови доказів [7]. Приклад – zk-SNARK, де на етапі ініціалізації генерується пара ключів (для доказуючого і верифікатора) з використанням випадкових секретних значень, що мають бути знищені після процедури. Якщо зловмисник отримає доступ до "токсичних" залишків цієї установки, він зможе підробляти докази [7]. Наявність довіреної установки вважається недоліком, адже вимагає абсолютної чесності учасників на початковому етапі. Альтернативою є прозорі (transparent) протоколи, які не потребують секретної установки – всі їх параметри генеруються відкрито, наприклад, з публічного випадкового "маяка" [8]. До прозорих належать zk-STARK та низка новітніх систем, що підвищує довіру до них, оскільки відпадає ризик компрометації прихованих параметрів.

Важливими класифікаційними характеристиками також є тип гарантії нульового знання (перфектне, статистичне чи обчислювальне нульове знання [2]) та вид доказової моделі (доказ знання проти доказу існування). Перфектне нульове розголошення означає, що верифікатор взагалі не може отримати інформацію про секрет (у сильному теоретичному сенсі рівності розподілів), статистичне допускає мізерну похибку, а обчислювальне – гарантує нульове знання лише за припущення обмеженості обчислювальних можливостей верифікатора [2]. Більшість практичних схем (наприклад, zk-SNARK) забезпечують обчислювальне нульове знання, оскільки спираються на криптографічні примітиви (хеш-функції, шифрування тощо) [7]. Щодо доказової моделі, то протоколи можуть доводити саме знання секрета (arguments of knowledge) або просто факт існування рішення без його розкриття. Докази знання потребують додаткової властивості – повноти по знанню, яка гарантує, що доказуючий не лише переконує в істинності твердження, а й володіє певною інформацією (наприклад, приватним ключем) [1, 2]. ZKP-протоколи за визначенням часто розглядаються як докази знання.

Також важливо зазначити і постквантові підходи для доказу з нульовим розголошенням. Незважаючи на успіхи zk-SNARK та zk-STARK, питання стійкості протоколів ZKP до атак квантових обчислювачів залишається відкритим. Прозорі хеш-базовані схеми на зразок zk-STARK уже володіють постквантовою стійкістю, проте мають великий розмір доказів (десятки чи сотні кілобайт). Альтернативним напрямом є використання решіткових криптосистем. Розроблено низку рішень на решітках, що теоретично забезпечують постквантове нульове розголошення. Наприклад, схема на основі задач SIS/LWE демонструє ZK-доказ знання з гарантією стійкості до квантових атак, однак ціна – дуже громіздкі докази (порядку сотень кілобайт) [13]. Це ускладнює практичне застосування таких схем. В останні роки запропоновано нові техніки оптимізації решіткових доказів. Зокрема, на CRYPTO 2023 представлено гібридну схему з «точними/релаксованими» доказами на решітках, що суттєво підвищує ефективність перевірки округлень і пов'язаних примітивів [14]. Подібні роботи спрямовані на скорочення розміру і часу перевірки решіткових ZK-доказів без втрати безпеки. Водночас ідеї квантових доказів з нульовим знанням поки що носять переважно академічний характер. Існують концепції «сліпих» квантових доказів, у яких обмін повідомленнями відбувається квантовими станами замість класичних бітів, або протоколи перевірки квантових обчислень із класичним верифікатором. Втім, такі квантові ZKP перебувають на ранніх стадіях досліджень і далекі від практичного застосування. Отже, досягнення постквантової стійкості ZKP наразі спираються на класичні криптосистеми (хеші, решітки тощо) та потребують подальшого вдосконалення для досягнення прийнятної продуктивності. Вирішення цих проблем є критично важливим, адже впровадження стійких до квантових атак ZKP дозволить зберегти безпечність блокчейн-систем і конфіденційність даних у прийдешню еру квантових обчислень.

Одним із проривів останніх років стало впровадження рекурсивних доказів – техніки, що дозволяє вкладати один ZK-доказ у інший, утворюючи ланцюжок доказів. Це означає, що можна породити короткий доказ правильності одразу серії тверджень, де кожне наступне твердження підтверджує коректність попереднього. Рекурсія фактично реалізує ідею інкрементально верифікованих обчислень (IVC). Сучасні системи, такі як Halo 2 та Nova, демонструють практичність цього підходу – вони дозволяють доводити коректність довготривалих обчислювальних процесів, розбиваючи їх на кроки і перевіряючи кожен крок рекурсивно. Nova, зокрема, є одним із найпростіших і найшвидших рекурсивних доказових механізмів: вона потребує лише сталого обсягу обчислень для верифікації незалежно від числа кроків, а її доказувач працює дуже ефективно. Ключова ідея Nova – використання схем складання (folding schemes), що зводять перевірку двох тверджень NP до перевірки одного, з меншим навантаженням. SuperNova розвиває ці ідеї далі, дозволяючи доводити правильність виконання довільних програм без побудови універсальних схем (тобто без «універсальних» кіл) [16]. Рекурсивні докази відкривають шлях до масштабування блокчейн-систем: з їх допомогою тисячі транзакцій можуть бути «згорнуті» в один стислий доказ, придатний для публікації в основному ланцюжку (т.зв. zk-Rollup). Це дуже підвищує пропускну здатність мережі та знижує витрати, адже навантаження на основний блокчейн мінімізується [17]. Дійсно, у системах StarkNet, zkSync, Polygon та ін. вже реалізовано таку масштабованість: L2-ланцюжки генерують ZK-докази правильності великих пакетів транзакцій, і мережа L1 валідує лише цей доказ замість усіх транзакцій. Іншим напрямом оптимізації є агрегація доказів, що дозволяє об’єднувати кілька незалежних ZK-доказів у один. Агрегування спрощує масову верифікацію: наприклад, метод SnarkPack дає змогу звести 8192 окремих SNARK-доказів в один пакет за 8,7 с, який перевіряється за 163 мс. Такий підхід експоненційно прискорює перевірку порівняно з поодинокими доказами [15]. Комбінація рекурсії та агрегування забезпечує значне підвищення ефективності: рекурсія скорочує загальний обсяг даних (шляхом вкладення доказів), а агрегування зменшує витрати на їх перевірку. Завдяки цьому сучасні протоколи можуть гарантувати як скейлінг, так і збереження приватності: блокчейн-операції, складні обчислення чи навіть цілі програми можуть бути доказані з нульовим розголошенням настільки ефективно, що це придатно для практичного використання у реальних системах.

Отже, для систематизації методів ZKP доцільно використовувати такі ключові критерії: інтерактивність (наявність багаторазового обміну vs. одноразундові схеми), необхідність довіреної установки (наявність vs. відсутність), алгебраїчна чи стохастична природа протоколу, тип нульового розголошення (перфектне/статистичне/обчислювальне), криптографічні припущення (на яких завданнях ґрунтується безпека) та ефективність (обсяг переданих даних і обчислювальні витрати). На основі цих ознак буде здійснюється класифікація основних підходів до побудови доказів з нульовим знанням.

Перші практичні реалізації ZKP для доказу знання секрета у групах із складною задачею дискретного логарифма (DL) ґрунтуються на трьохходових σ-протоколах – схемі Фіата–Шаміра, Шнорра та їх численних узагальненнях [3]. Сучасні варіанти активно застосовують:

- Σ-протоколи над еліптичними кривими – в основі протоколів ідентифікації й e-cash;
- Σ-протоколи для знання факторизації (e.g., Okamoto-Uchiyama) – у системах e-vote;
- Σ-протоколи з агрегуванням – забезпечують паралельне об’єднання доказів і зменшують розмір повідомлень.

Починаючи з роботи Pinocchio (2013) й особливо статті Ben-Sasson та ін. [4] неінтерактивні докази стали практичними для великих обчислень. Характерні риси:

- довірена токсична установка (trusted setup);
- лінійна (O(n)) генерація доказу, але логарифмічна верифікація;
- розмір доказу < 1 кБ;
- обчислювальна модель Rank-1 Constraint System (R1CS).

До сучасних представників належать Groth16 [5], PLONK [9], Halo 2 [10], які оптимізують розмір ключів та підтримують рекурсивне об'єднання доказів.

zk-STARK [6] усуває потребу у довіреній установці, спираючись лише на довільні хеш-функції та коди Ріда–Соломона. Властивості:

- прозорість: всі параметри одержують із публічного випадкового джерела;
- постквантова стійкість;
- докази десятки/сотні КБ, але непотрібні токсичні залишки;
- складність перевірки – quasi-linear у розмірі трасування обчислення.

STARK-технології вже застосовуються у L2-мережах Ethereum (StarkNet).

Протоколи Блума–Фельдмана, Goldreich–Micali–Wigderson та ін. доводять NP-твердження зі статистичним нульовим знанням, використовуючи багаторазові випадкові commit-challenge-response-раунди [2]. Вони універсальні (існують для будь-якої NP-мови), проте потребують багатьох раундів і значного обсягу передачі ($\approx O(n \cdot k)$, де k – кількість повторів для зниження ймовірності шахрайства).

Lattice-based ZKP для задач NTRU або SIS/LWE надають постквантову стійкість, але поки мають великі розміри доказу (сотні кілобайт) [11].

Сліпий квантовий доказ (QZKP) пропонує передавати квантові стани замість класичних повідомлень.

Zero-Knowledge Machine Learning Proofs: доведення коректності inferencing-моделі без розкриття параметрів (дослідження 2023 – 2025 рр.) [12].

У табл. 1 наведено порівняння описаних вище підходів.

Таблиця 1

Порівняльний аналіз підходів

Підхід	Trusted Setup	Розмір доказу	Час генерації	Час перевірки	Безпека	Типові застосунки
Σ-протокол (DL) [18]	Ні	64-128Б	$O(1/\epsilon)$	$O(1/\epsilon)$	Обчисл. ZK, EUF-CMA	Ідентифікація, e-cash
zk-SNARK (Groth16) [19, 20]	Так	128-192Б	O(n log n)	O(1)	Обчисл. ZK, DL	Приватні платежі (Zcash)
zk-SNARK (PLONK) [19, 20]	Так	624-2400Б	O(n log n)	O(n log n)	Обчисл. ZK, DL	L2 Rollups
zk-STARK [6, 7, 21]	Ні	50-200КБ	O(n log n)	O(n log n)	Постквант., ш.хеш	Масштабований CI
Bulletproofs [7]	Ні	O(log n) ≅ (3-6КБ)	O(n log n)	O(n)	Обчисл. ZK, DL	Конфіденц. транзакції (Monero)
Lattice ZKP [22]	Ні	13-400 КБ	O(n log n)	O(n log n)	Постквант. SIS	e-ID, PKE

П р и м і т к а : n – розмір вхідних даних/схеми; CI – computational integrity.

Перспективи та відкриті проблеми:

1. Постквантова стійкість. Хеш-базовані STARK є перспективою, однак потрібно зменшити розмір доказу та час перевірки [6].

2. Рекурсивні та агреговані докази. Halo 2, Nova та SuperNova дозволяють вкладати докази у докази, що критично для масштабованості блокчейн-L2 [10].

3. Захист метаданих. Навіть за ZK-доказів бокові канали (розмір, час, мережеві патерни) можуть розкривати приватність; потрібні протоколи укриття трафіку.

4. Zero-Knowledge ML. Перевірка коректності виконання НН-моделей із приватними вагами залишається відкритою задачею за обмежень продуктивності [12].

Висновки

У статті систематизовано сучасні методи доказу з нульовим розголошенням за ознаками інтерактивності, математичної природи, потреби у довіреній установці та типу гарантій нульового знання. Алгебраїчні zk-SNARK і прозорі zk-STARK довели практичність ZKP для широкого спектра прикладних задач – від конфіденційних платежів до захищених хмарних обчислень. Порівняльний аналіз показав компроміси між ефективністю та безпекою: SNARKи забезпечують мінімальний розмір доказу, але вимагають trusted setup; STARKи ж прозорі й постквантові, однак громіздкі. Подальші дослідження зосереджено на рекурсивних схемах, постквантових конструкціях, стандартизації та інтеграції у високорівневі застосунки, зокрема машинне навчання й Інтернет речей. Розв'язання цих проблем забезпечить нові можливості для безпечних та приватних інформаційних технологій.

Список літератури:

1. Meiklejohn S., Mercer R. ZKProof Community Reference. ZKProof Community Docs. 2022. Режим доступу: http://docs.zkproof.org/reference.pdf
2. Lindell Y. How To Simulate It – A Tutorial on the Simulation Proof Technique // IACR Cryptology ePrint Archive. 2016. No. 046. Режим доступу: https://eprint.iacr.org/2016/046.pdf
3. Boneh D., Shoup V. A Graduate Course in Applied Cryptography. 2020. Ch. 19, 23. Режим доступу: https://crypto.stanford.edu/~dabo/cryptobook/
4. Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture // IACR Cryptology ePrint Archive. 2013. No. 879. Режим доступу: https://eprint.iacr.org/2013/879.pdf
5. Groth J. On the Size of Pairing-Based Non-interactive Arguments // IACR Cryptology ePrint Archive. 2016. No. 260. Режим доступу: https://eprint.iacr.org/2016/260.pdf
6. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // IACR Cryptology ePrint Archive. 2018. No. 046. Режим доступу: https://eprint.iacr.org/2018/046.pdf
7. Bünz B., Bootle J., Boneh D., et al. Bulletproofs: Short Proofs for Confidential Transactions and More // IACR Cryptology ePrint Archive. 2017. No. 1066. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/2017/1066.pdf
8. Ben-Sasson E., Chiesa A., Spooner N. Interactive Oracle Proofs // Theory of Cryptography Conference (TCC 2016-B). Lecture Notes in Computer Science. Vol. 9985. Springer, 2016. P. 163–190.
9. Gabizon A., Williamson Z., Ciobotaru O. PLONK: Permutations over Lagrange-Bases for Oecumenical Non-interactive Arguments of Knowledge // IACR Cryptology ePrint Archive. 2019. No. 953. Режим доступу: https://eprint.iacr.org/2019/953.pdf
10. Bowe S., Gabizon A., Green M., et al. Halo 2: Recursive Proof Composition without a Trusted Setup // IACR Cryptology ePrint Archive. 2019. No. 1021. Режим доступу: https://eprint.iacr.org/2019/1021.pdf
11. Lyubashevsky V., Seiler G. Zero-Knowledge Proofs from Lattices: New Techniques // Advances in Cryptology – CRYPTO 2022. Lecture Notes in Computer Science. Vol. 13508. Springer, 2022. P. 66–92. DOI: 10.1007/978-3-031-15979-4_3
12. Hao M., Chen H., et al. zk-ML: Scalable Zero-knowledge Proofs for Non-linear Functions in Machine Learning // IACR Cryptology ePrint Archive. 2025. No. 507. Режим доступу: https://eprint.iacr.org/2025/507.pdf
13. Rafaël Del Pino: Efficient lattice-based zero-knowledge proofs and applications p. 49. Режим доступу: https://theses.hal.science/tel-02445482v1/document
14. Muhammed F. Esgin, Ron Steinfeld, Dongxi Liu, Sushmita Ruj: Efficient Hybrid Exact/Relaxed Lattice Proofs and Applications to Rounding and VRFs. Режим доступу: https://eprint.iacr.org/2022/141.pdf
15. Nicolas Gailly, Mary Maller, Anca Nitulescu: SnarkPack: Practical SNARK Aggregation. Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2-6, 2022, Revised Selected Papers P. 203–229
16. Roy Lu: Moore's Law for Zero Knowledge Proofs. Stanford Blockchain Review Volume 3, Article No. 2. Режим доступу: https://review.stanfordblockchain.xyz/ p/22-moores-law-for-zero-knowledge
17. Shashidhara R. Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions. Security and Privacy 8(1) September 2024. Режим доступу: https://www.researchgate.net/publication/ 384056745_Promise_of_Zero-Knowledge_Proofs_ZKPs_for_Blockchain_Privacy_and_Security_ Opportunities_Challenges_and_Future_Directions#:~:text=other%20zk,processes%20transac
18. Ivan Damgard: On Σ-protocols. CPT 2010, v.2. Режим доступу: https://www.cs.au.dk/~ivan/Sigma.pdf
19. Garg S. et al. zkSaaS: Zero-Knowledge SNARKs as a Service (USENIX Security 2023). Режим доступу: https://eprint.iacr.org/2023/905.pdf

20. Arka Rai Choudhuri, Sanjam Garg, Aarushi Goel, Sruthi Sekar, Rohit Sinha: SublonK: Sublinear Prover PLONK // Proceedings on Privacy Enhancing Technologies. 2024. No 3. P. 314–335. Режим доступу: https://petsymposium.org/popets/2024/popets-2024-0080.pdf

21. Kimi Wu: Revealing The All Mysterious zk-STARKs. Режим доступу: https://medium.com/coinmonks/reveal-mysterious-zk-starks-42d00679c05b

22. Ngoc Khanh Nguyen, George O'Rourke: More Efficient Lattice-Based Zero-Knowledge Proofs with Straight-Line Extractability. APKC '25 // Proceedings of the 12th ACM ASIA Public-Key Cryptography Workshop. Режим доступу: https://dl.acm.org/doi/10.1145/3709015.3728673

Надійшла до редколегії 12.10.2025

Відомості про автора:

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