

УДК 003.26:004.421:004.428

Кацюба М.В.¹, Кацюба В.В.¹, Неласа Г.В.²

¹ студ. групи РТ-710, НУ «Запорізька політехніка»

² канд. техн. наук, доцент кафедри ЗІ, НУ «Запорізька політехніка»

АНАЛІЗ НЕІНТЕРАКТИВНИХ СИСТЕМ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ ZKSNARK ТА ZKSTARK

В криптографії існують системи, які дозволяють в умовах взаємної недовіри одній з взаємодіючих сторін переконатися в достовірності будь-якого твердження, не маючи при цьому жодної інформації відносно самого твердження, а використовуючи тільки короткий доказ, сформований заздалегідь.

Такі системи називають доказом з нульовим розголошенням [1, 2].

Докази з нульовим розголошенням за визначенням повинні відповідати таким основним вимогам:

- повнота (completeness). Для істинних тверджень сторона, що доводить (prover), завжди може переконати перевіряючого (verifier);

- обґрунтованість (soundness). У випадку неправдивих тверджень доказуючий не може переконати перевіряючого (навіть якщо він обманює та відхиляється від протоколу);

- нульове знання (zero knowledge). Перевіряючий не дізнається від взаємодії нічого, крім того факту, що твердження істинне. Система доказів відповідає цій вимозі, якщо існує третій алгоритм - симулятор (simulator), за допомогою якого можна генерувати доказ, який неможливо відрізнити від доказу чесного доказуючого.

Системи доказу також можуть містити екстрактор (extractor), тобто окремий алгоритм вилучення, за допомогою якого можна отримати секретну інформацію (witness).

Системи доказів поділяються на інтерактивні та не інтерактивні. В інтерактивних системах доказу обидві сторони обмінюються інформацією у безпосередній комунікації.

В неінтерактивних системах доказ складається лише з одного повідомлення, яке той, хто доводить, надсилає тому, хто перевіряє. Сучасними реалізаціями неінтерактивних систем є протоколи zkSNARK [3] та zkSTARK [4]. Метою доповіді є їх порівняльний аналіз.

zkSNARK (з англ. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge - стислий неінтерактивний аргумент знань із нульовим знанням) – це протокол з нульовим розголошенням, який не потребує взаємодії між тим, хто доводить, та тим, хто перевіряє.

Характеристика «стислий» означає, що докази нульового знання в цьому протоколі можна перевірити протягом декількох мілісекунд, а довжина такого доказу - лише кілька сотень байт, навіть для досить великого розміру вихідного твердження. Характеристика «неінтерактивний» означає, що доказ складається з одного повідомлення, надісланого тим, хто доводить, тому, хто перевіряє. У наш час є багато реалізацій zkSNARK, найвідомішими з яких є Pinocchio, Halo, Plonk, та Groth16 [5].

zkSTARK (з англ. Zero-Knowledge Scalable Transparent Argument of Knowledge — «масштабований прозорий аргумент знання з нульовим розголошенням») є також протоколом з нульовим розголошенням, але на відміну від zkSNARK, є:

- масштабованим (системи з використанням zkSTARK легко масштабуються в термінах швидкості обчислень та розміру пам'яті на завдання з великою кількістю обчислень);

- прозорим (не вимагає попереднього налаштування).

В zkSNARK присутня попередня фаза довірчого налаштування (Trusted setup). Якщо нечесний доказувач буде знати довірчі параметри, то він може

робити неправдиві докази. zkSTARK позбавлений цього недоліку. Крім того, zkSNARK не є стійким до квантових атак. Навпаки ж, zkSTARK використовує постквантову криптографію, тобто є стійким до квантових атак. Але досить сильною перевагою zkSNARK перед zkSTARK є розмір доказу: для першого він є набагато меншим, ніж для останнього.

У наш час системи доказу з нульовим розголошенням досить широко використовуються, зокрема у деяких блокчейнах і криптовалютах (наприклад, Zcash, ZEN, Ethereum).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. O. Goldreich, S. Micali, A. Wigderson, Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems // Journal of the ACM –1991. – (3), Volume 38. – P. 691 – 729.
2. Федюкович В.Є. Интерактивные системы с ничтожной ошибкой // Федюкович В.Є. / Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VI Міжн. наук.-практ. конф., 19-21 вересня 2012 р. : тези доповідей.– Запоріжжя, 2012. – С.242-244.
3. What are zk-SNARKs? [Електронний ресурс] – Режим доступу: <https://z.cash/technology/zksnarks/>
4. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev Scalable, transparent, and post-quantum secure computational integrity // Cryptology ePrint Archive: Report 2018/046. – Режим доступу: <https://eprint.iacr.org/2018/046.pdf>
5. Groth J. On the Size of Pairing-based Non-interactive Arguments [Електронний ресурс].– Режим доступу: <https://eprint.iacr.org/2016/260.pdf>.