ДОДАТОК А

Перелік джерел посилання за науковими напрямами керівника та науковців кафедри програмної інженерії

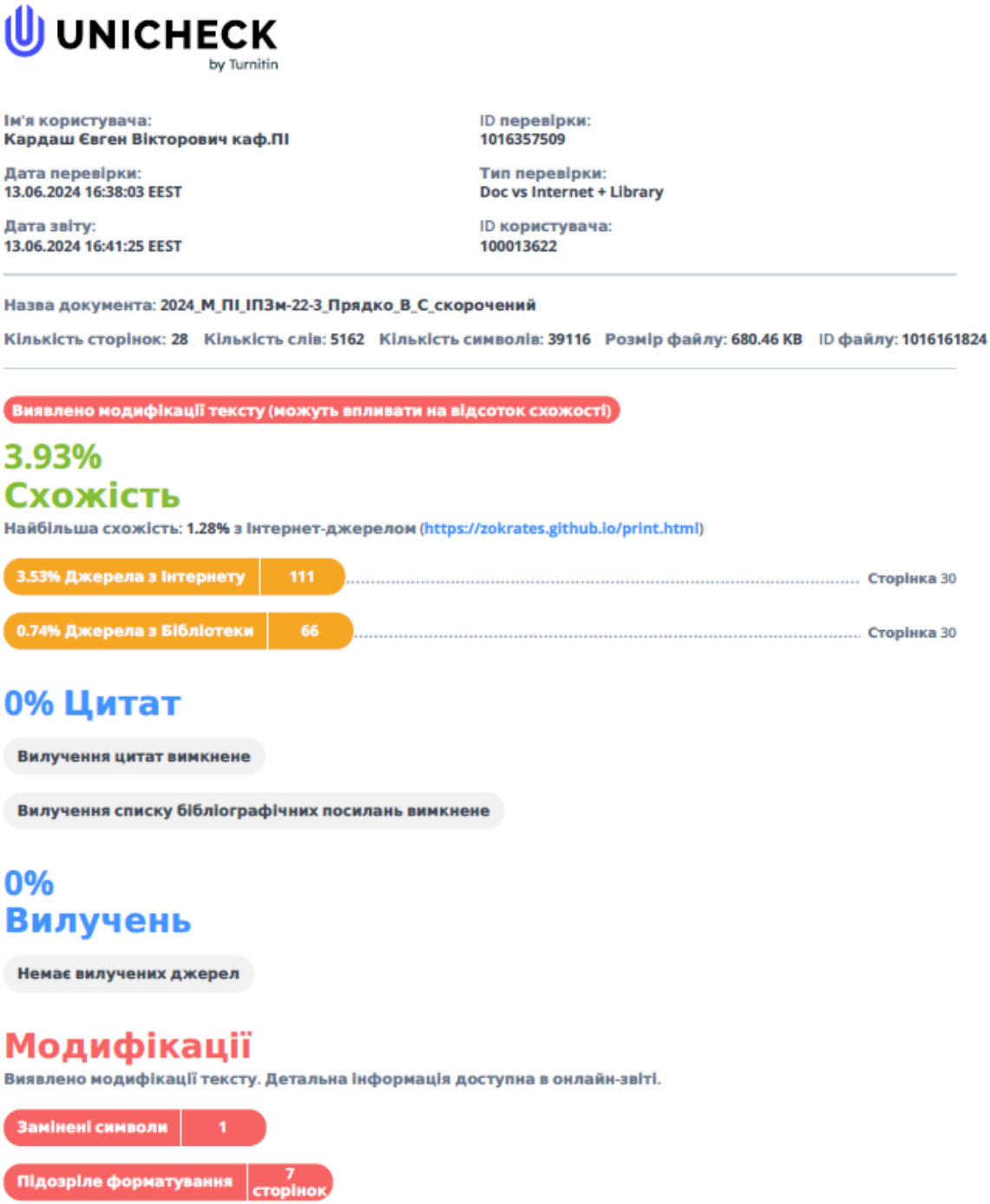
5. Качко О.Г., Мельникова О.А. Some methods for increasing the speed of operations on elliptic curves in the normal basis // 10-а науково-технічна конференція “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”. Науково-технічний збірник. – Вип. 11. – Київ, 2005.

6. Качко О.Г., Аулов І.Ф. Mechanisms for improving the performance of cryptographic libraries for end users in cloud technologies // Міжнародна наукова школа – семінар Питання оптимізації обчислень (ПОО-XLII) 21-25 вересня 2015. Україна, Закарпатська область, Мукачівський район, смт Чинадієво. – 21-25 вересня 2015 року.

17. Качко О.Г., Телевний Д.К. Study of applicability of SMT/SAT proofs in cryptanalysis of Keccak family hash functions // Журнал Радіотехніка. – 2017. – Вип. 189. – С. 75-80.

ДОДАТОК Б

Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ



UNICHECK
by Turnitin

Ім'я користувача:
Кардаш Євген Вікторович каф.ПІ

ID перевірки:
1016357509

Дата перевірки:
13.06.2024 16:38:03 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2024 16:41:25 EEST

ID користувача:
100013622

Назва документа: 2024_М_ПІ_ІПЗм-22-3_Прядко_В_С_скорочений

Кількість сторінок: 28 Кількість слів: 5162 Кількість символів: 39116 Розмір файлу: 680.46 KB ID файлу: 1016161824

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

3.93%
Схожість

Найбільша схожість: 1.28% з Інтернет-джерелом (https://zokrates.github.io/print.html)

3.53% Джерела з Інтернету 111 ..... Сторінка 30

0.74% Джерела з Бібліотеки 66 ..... Сторінка 30

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 1

Підозріле форматування 7 сторінок

ДОДАТОК В

Слайди презентації

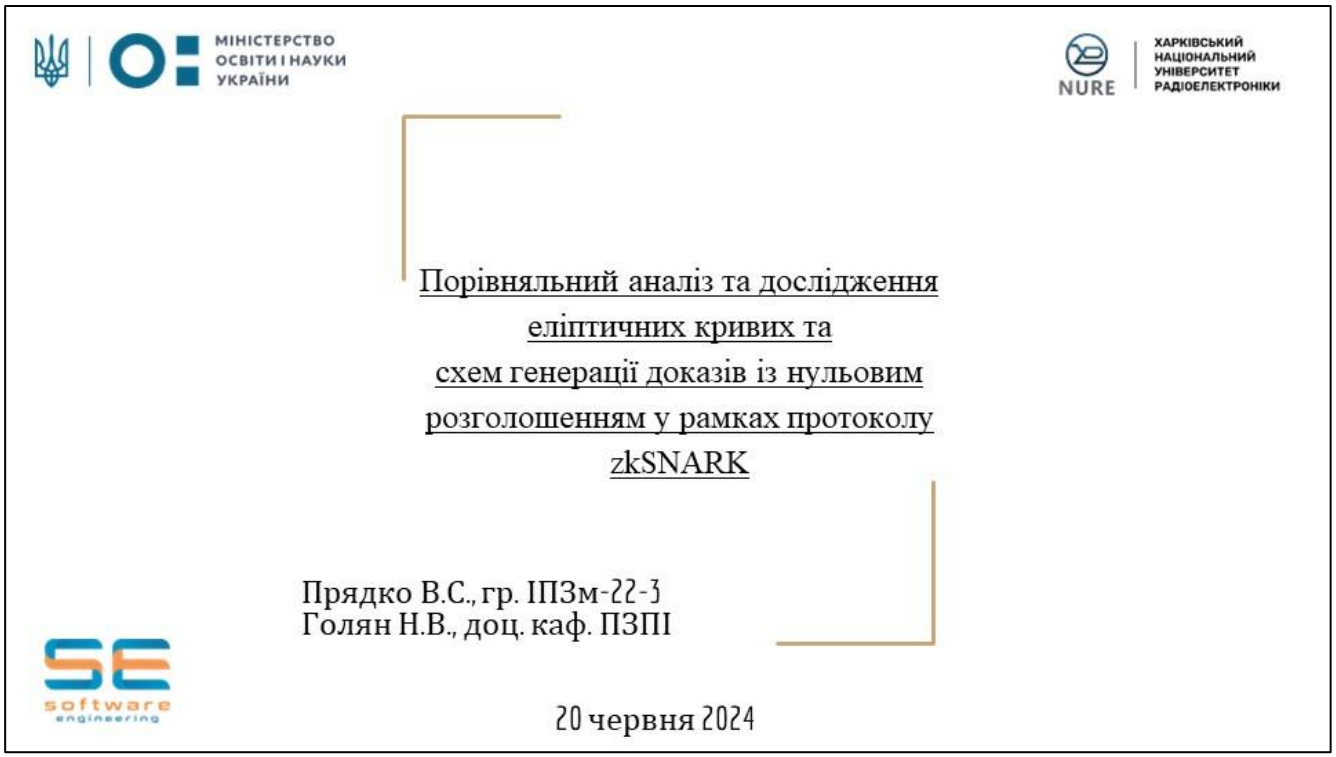


Рисунок В.1 – Слайд 1

Рисунок В.2 – Слайд 2

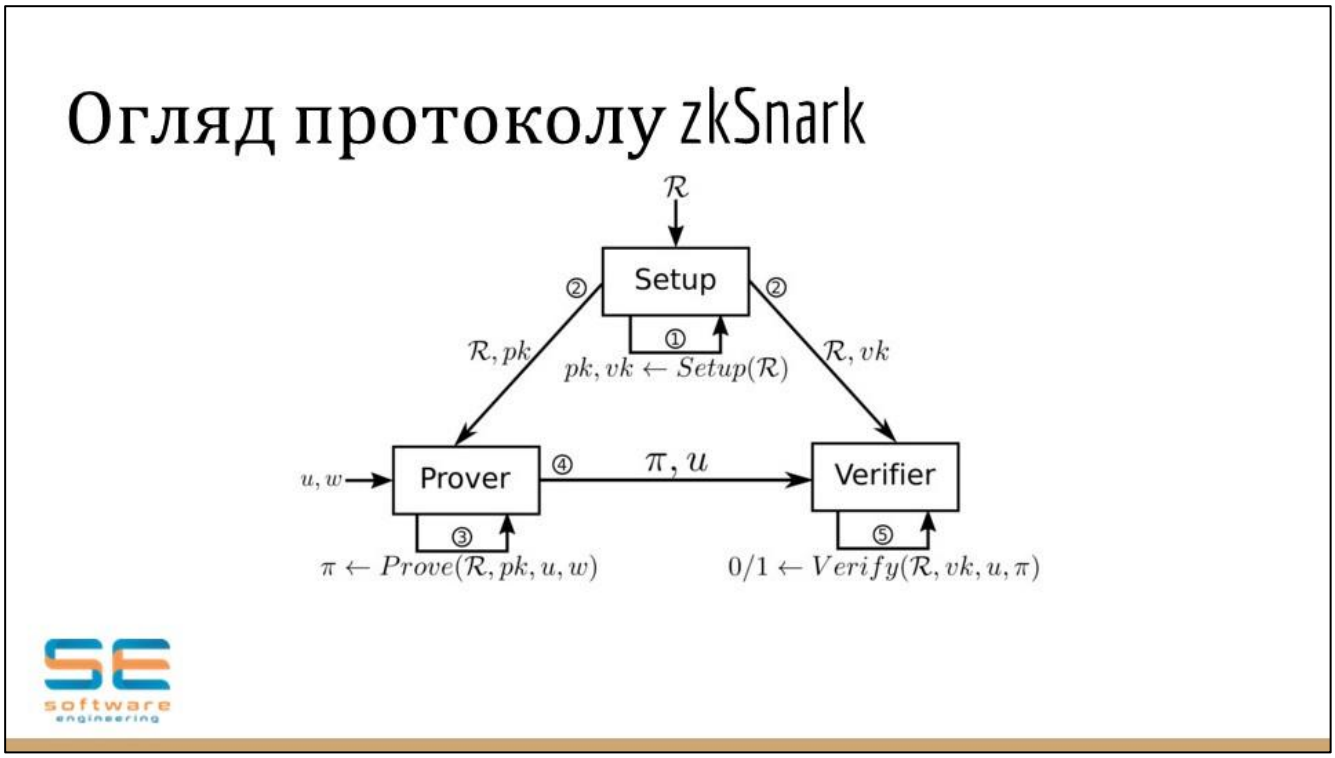


Рисунок В.3 – Слайд 3

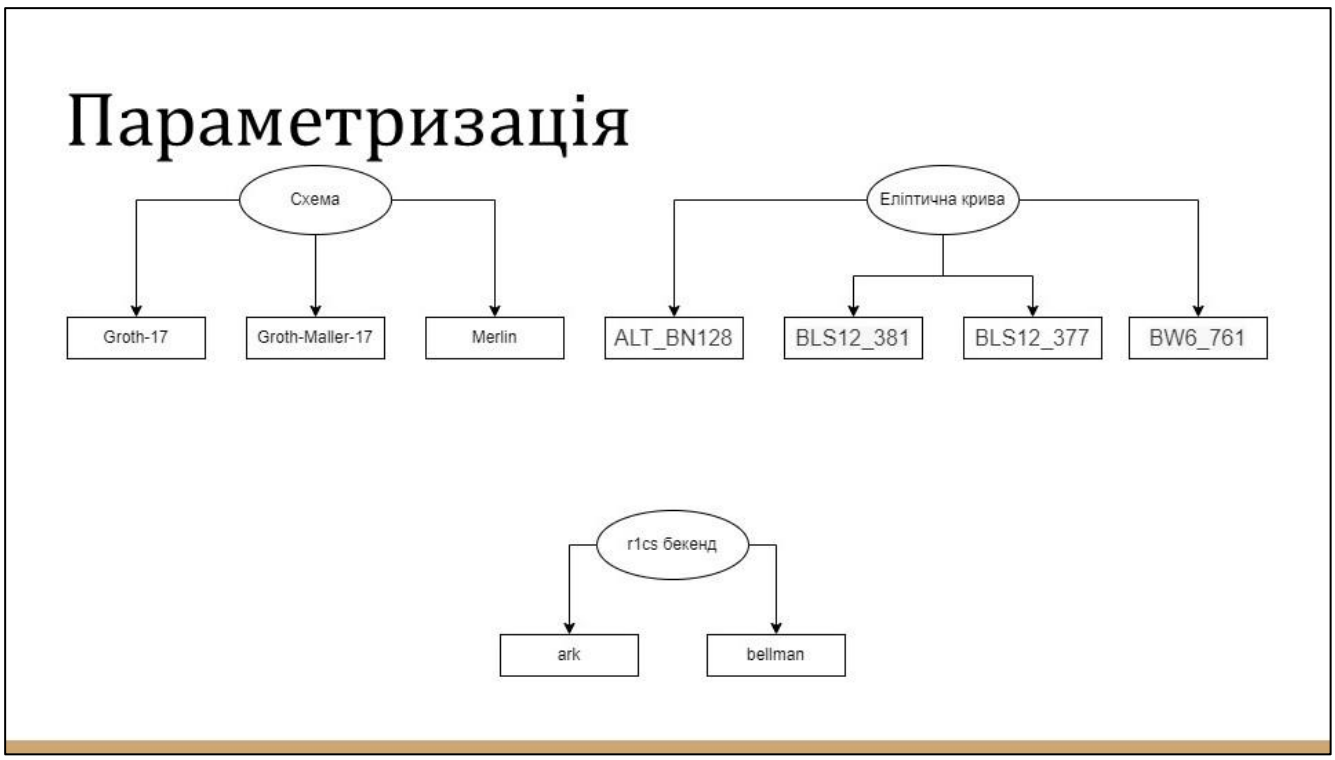


Рисунок В.4 – Слайд 4

Мета дослідження

	EVM-comp	Universal setup	Replay attack resistant	Backend		Z*
G16	1.000	0	0	2		0.140
GM17	1.500	0	1	2		0.290
Marlin	1.500	1	1	1		0.570
β	0.4	0.3	0.2	0.1		
α	0.25	1	0.5	0.2		

$$Z = \max_{i=1,m} \sum_{j=1}^{n} \alpha_j \beta_j a_{ij}$$

Рисунок В.5 – Слайд 5

Методологія дослідження

1. Визначення та імплементація класів задач
2. Створення синтетичних даних
3. Визначення методів вимірювання основних метрик
4. Створення стенду для ітеративного тестування
5. Комбінування параметрів, відсіювання нежиттєздатних
6. Фактичне тестування
7. Очистка, фільтрація та нормалізація отриманих значень
8. Візуалізація даних
9. Аналіз та висновки з отриманих знань

Рисунок В.6 – Слайд 6

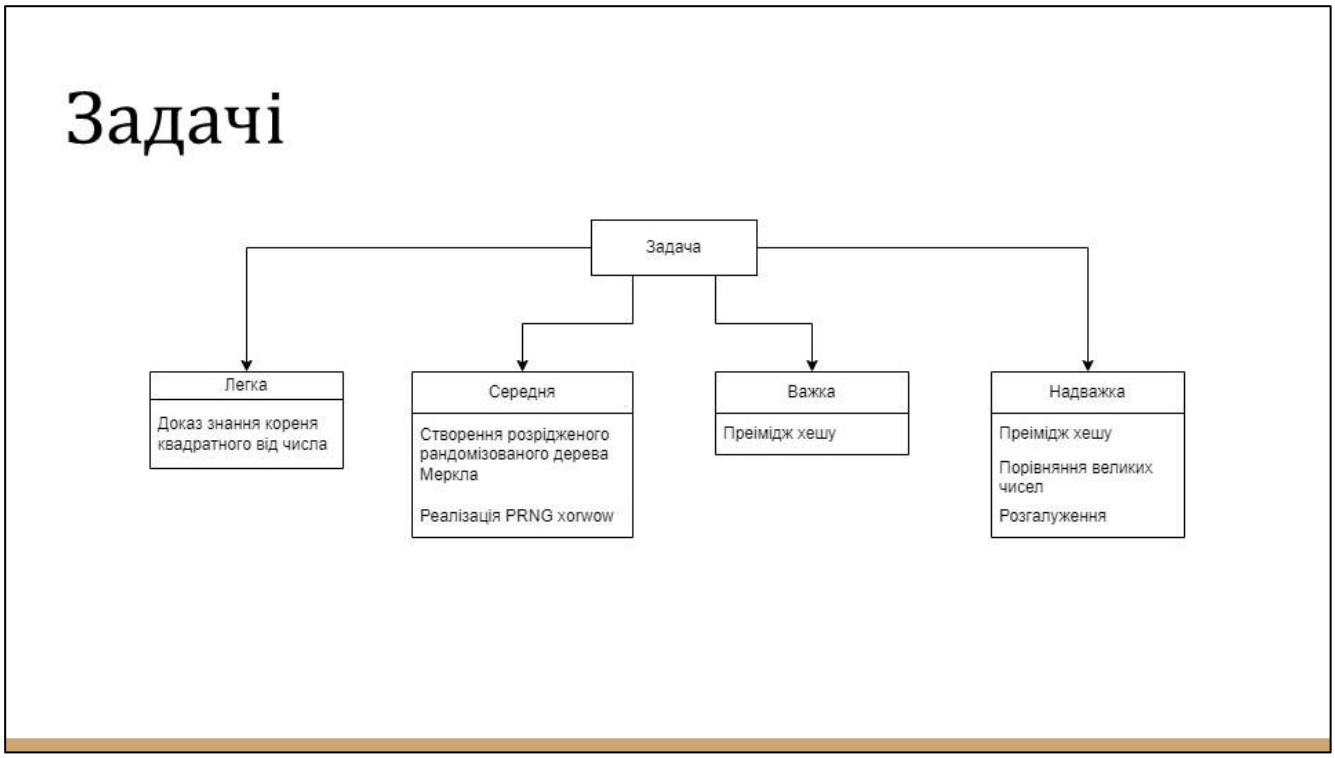


Рисунок В.7 – Слайд 7

Рисунок В.8 – Слайд 8

Програмне забезпечення та технічні рішення

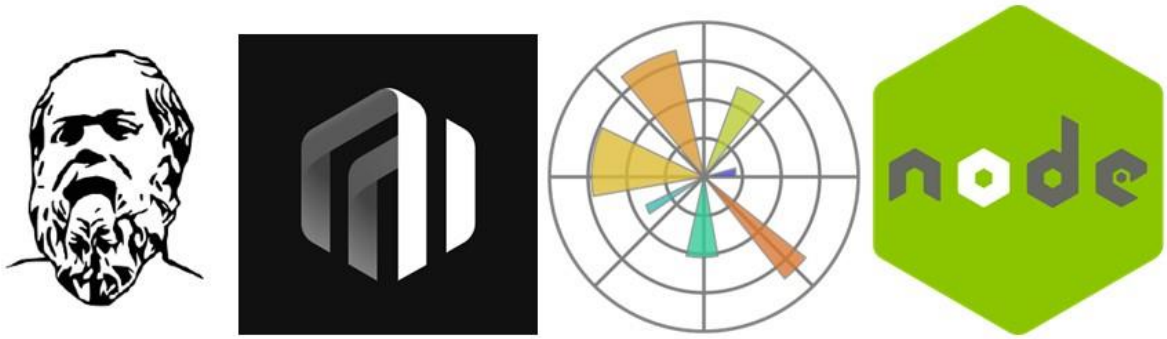


Рисунок В.9 – Слайд 9

Умови проведеного експерименту

Операційна система Windows 10
Процесор Intel Core i3-8130U 2.20GHz
4 задачі, реалізовані в .zok
10 ітерацій, 6 годин

Вагові коефіцієнти ранжування:

```
export const taskWeights: { [key: string]: number } = {
  simple: 1,
  middle: 2,
  complex: 3,
  advanced: 4,
};

export const metricWeights: { [key: string]: number } = {
  computationTime: 2.0,
  computationMemory: 0.5,
  computationVolume: 0.5,
  proofGenerationTime: 2.0,
  proofGenerationMemory: 1.0,
  proofGenerationVolume: 0.5,
  verificationTime: 3.0,
  verificationMemory: 2.5,
  verificationVolume: 1.0,
};
```

Рисунок В.10 – Слайд 10

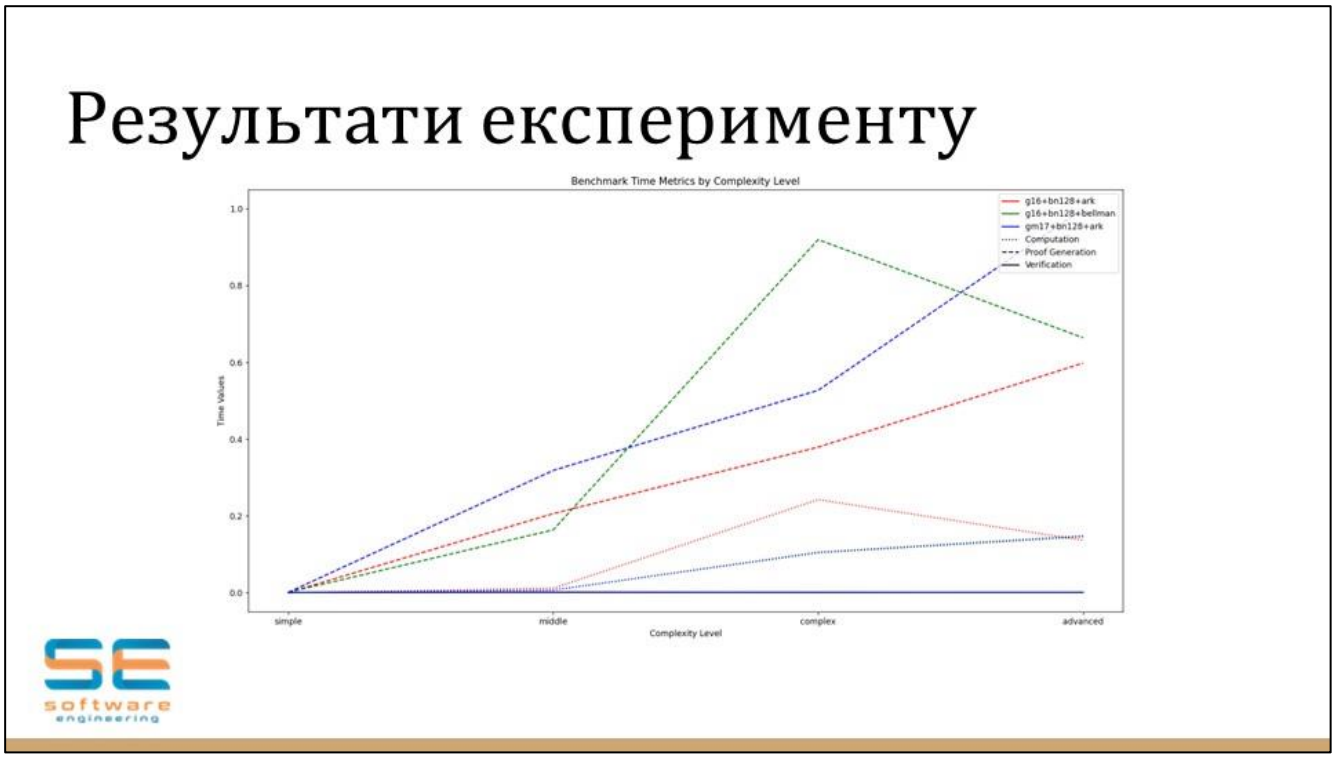


Рисунок В.11 – Слайд 11

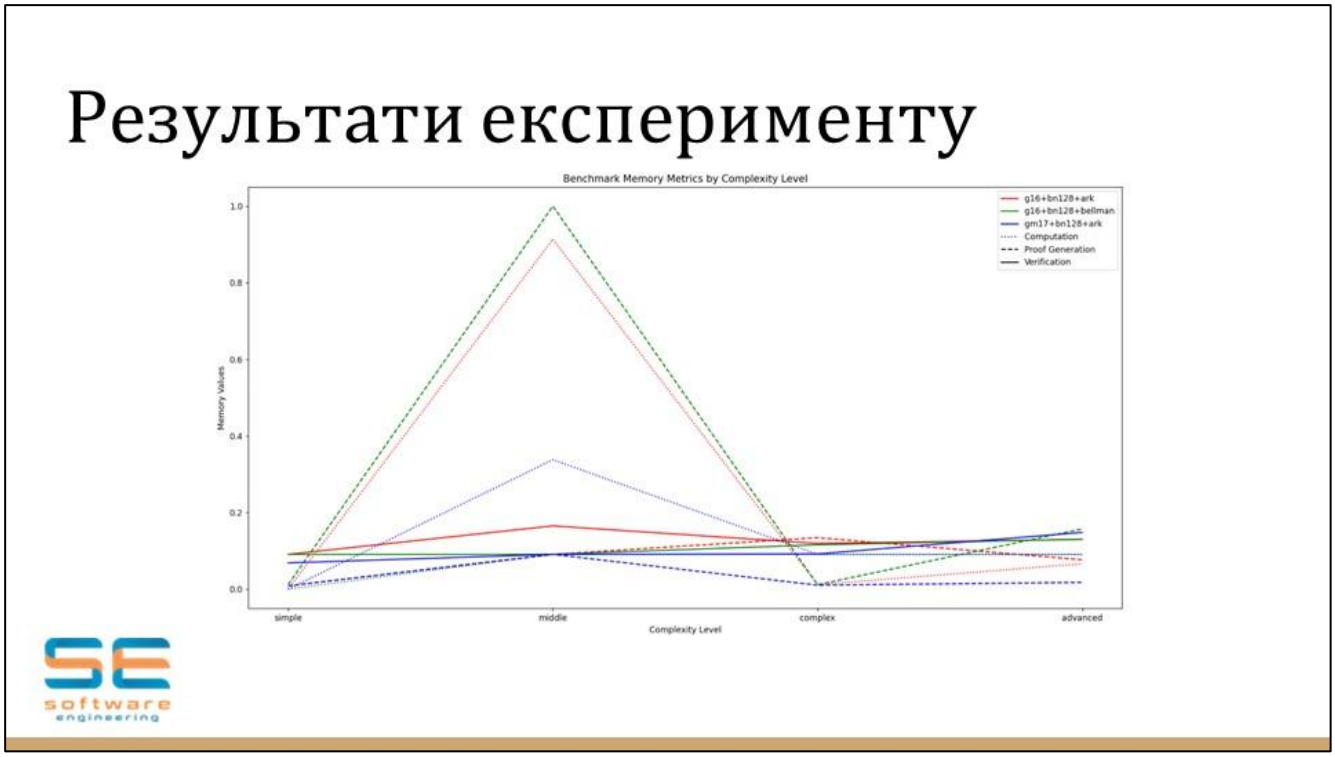


Рисунок В.12 – Слайд 12

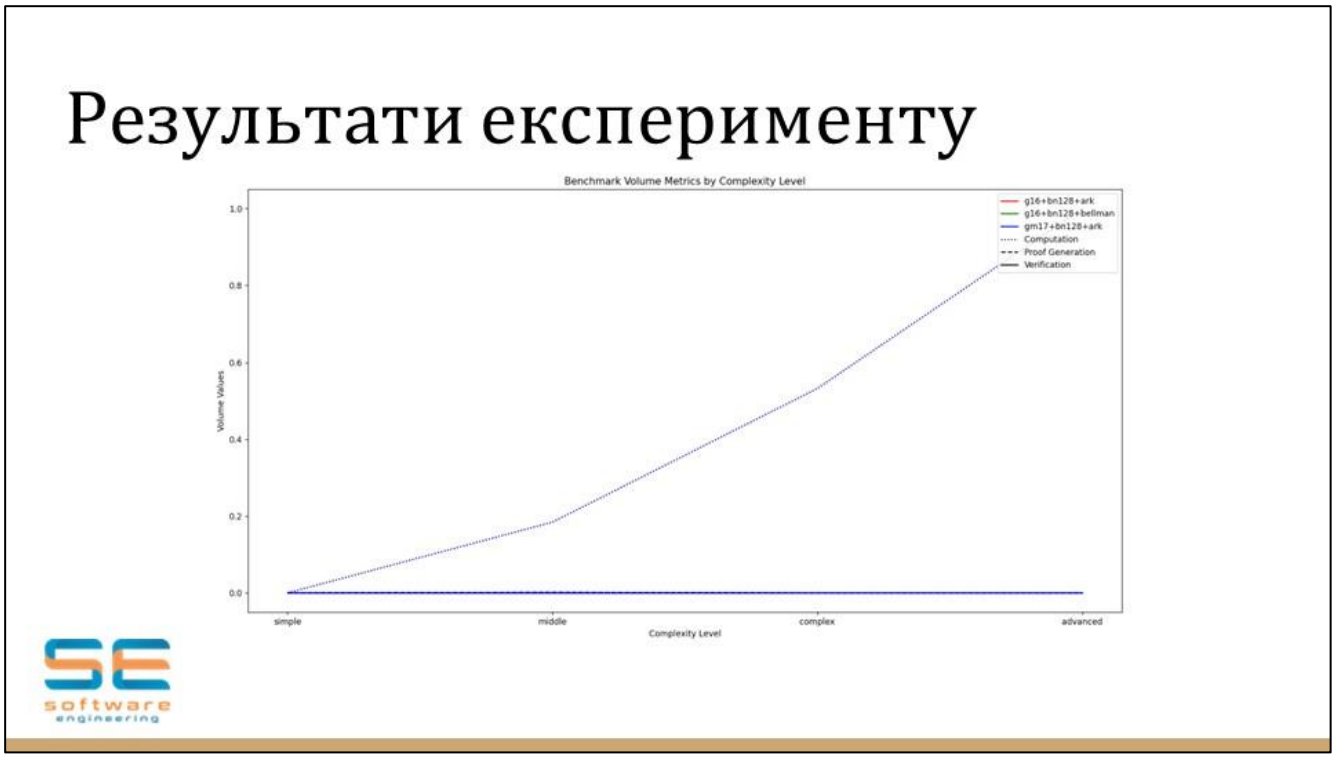


Рисунок В.13 – Слайд 13

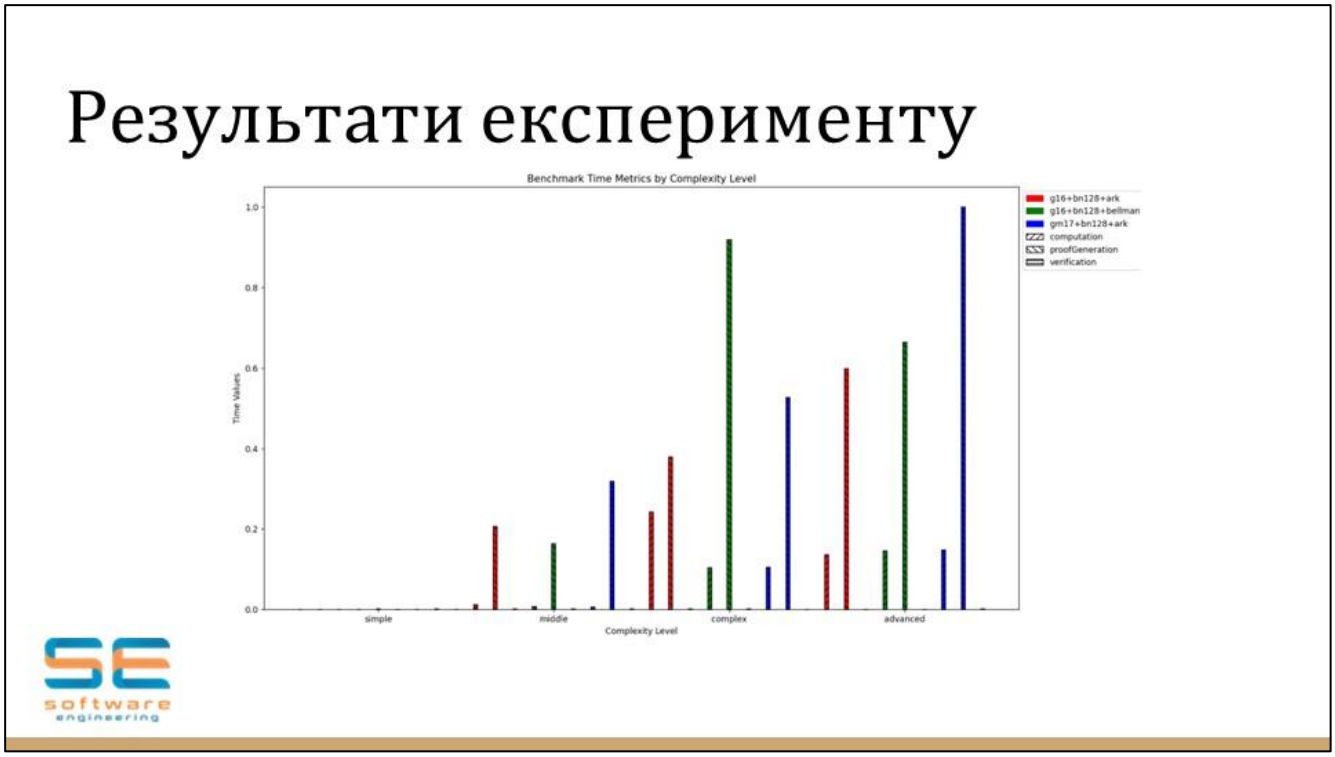


Рисунок В.14 – Слайд 14

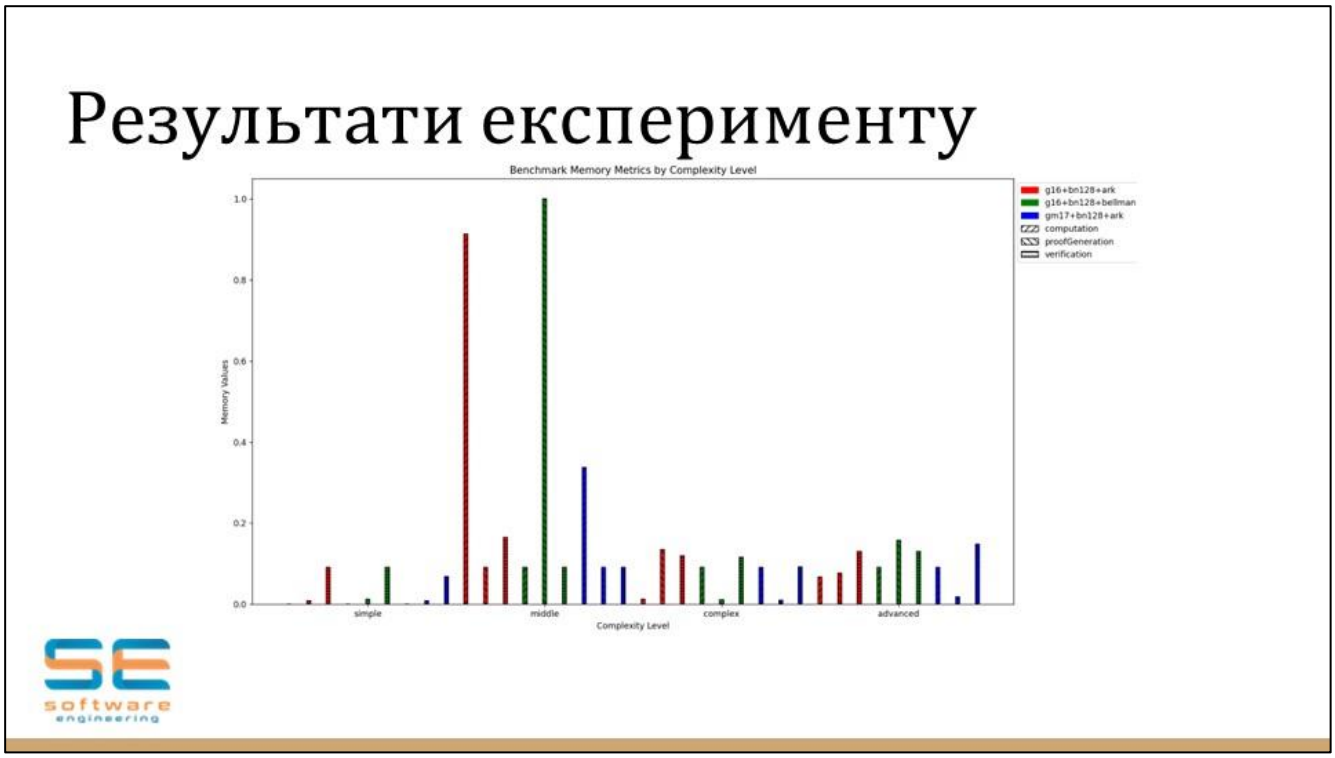


Рисунок В.15 – Слайд 15

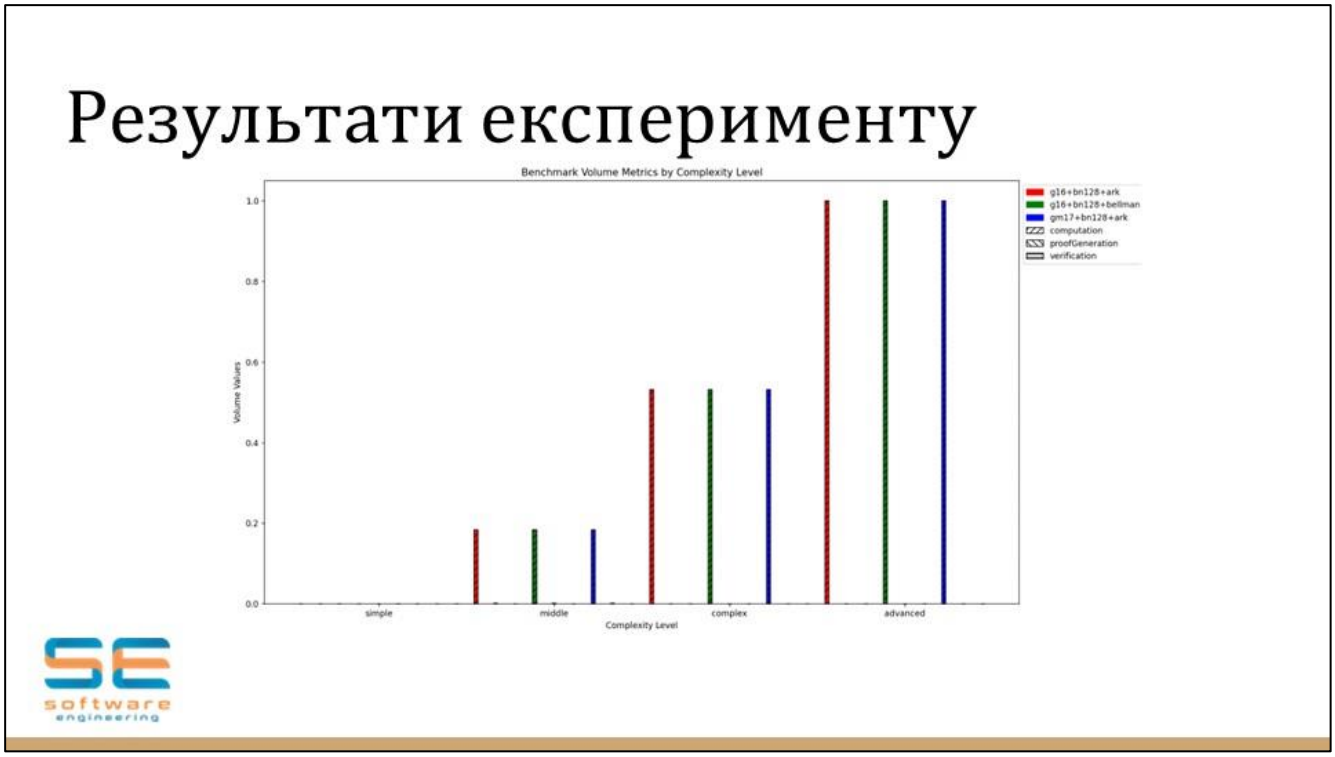


Рисунок В.16 – Слайд 16

Аналіз та ранжування


```
{
  scheme: 'g16',
  curve: 'bn128',
  backend: 'ark',
  weightedComputation: {
    timeMetric: 0.1297140266454953,
    memoryMetric: 0.21276961767519365,
    volumeMetric: 0.5964861858551802
  },
  weightedProofGeneration: {
    timeMetric: 0.3942473561421038,
    memoryMetric: 0.08991498750270004,
    volumeMetric: 0.000292197079398013 1
  },
  weightedVerification: {
    timeMetric: 0.0008435785054146761,
    memoryMetric: 0.12978986021538558,
    volumeMetric: 0
  }
},
```

```
{
  scheme: 'gm17',
  curve: 'bn128',
  backend: 'ark',
  weightedComputation: {
    timeMetric: 0.0923504219885946,
    memoryMetric: 0.13106967630450211,
    volumeMetric: 0.5964861858551802
  },
  weightedProofGeneration: {
    timeMetric: 0.6219791810784944,
    memoryMetric: 0.029124880427068227,
    volumeMetric: 0.000292233100636135 1
  },
  weightedVerification: {
    timeMetric: 0.0009799851515713321,
    memoryMetric: 0.1117706051161786,
    volumeMetric: 0
  }
},
```

```
{
  scheme: 'g16',
  curve: 'bn128',
  backend: 'bellman',
  weightedComputation: {
    timeMetric: 0.09058710249603963,
    memoryMetric: 0.0816436263770173,
    volumeMetric: 0.5964861858551802
  },
  weightedProofGeneration: {
    timeMetric: 0.5743135327336661,
    memoryMetric: 0.267506248649983,
    volumeMetric: 0.000292197079398013 1
  },
  weightedVerification: {
    timeMetric: 0.0009213521572554587,
    memoryMetric: 0.11413274909741725,
    volumeMetric: 0
  }
}
```


Winner:
g16+bn128+ark

Рисунок В.17 – Слайд 17

Апробація роботи

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

Рисунок В.18 – Слайд 18

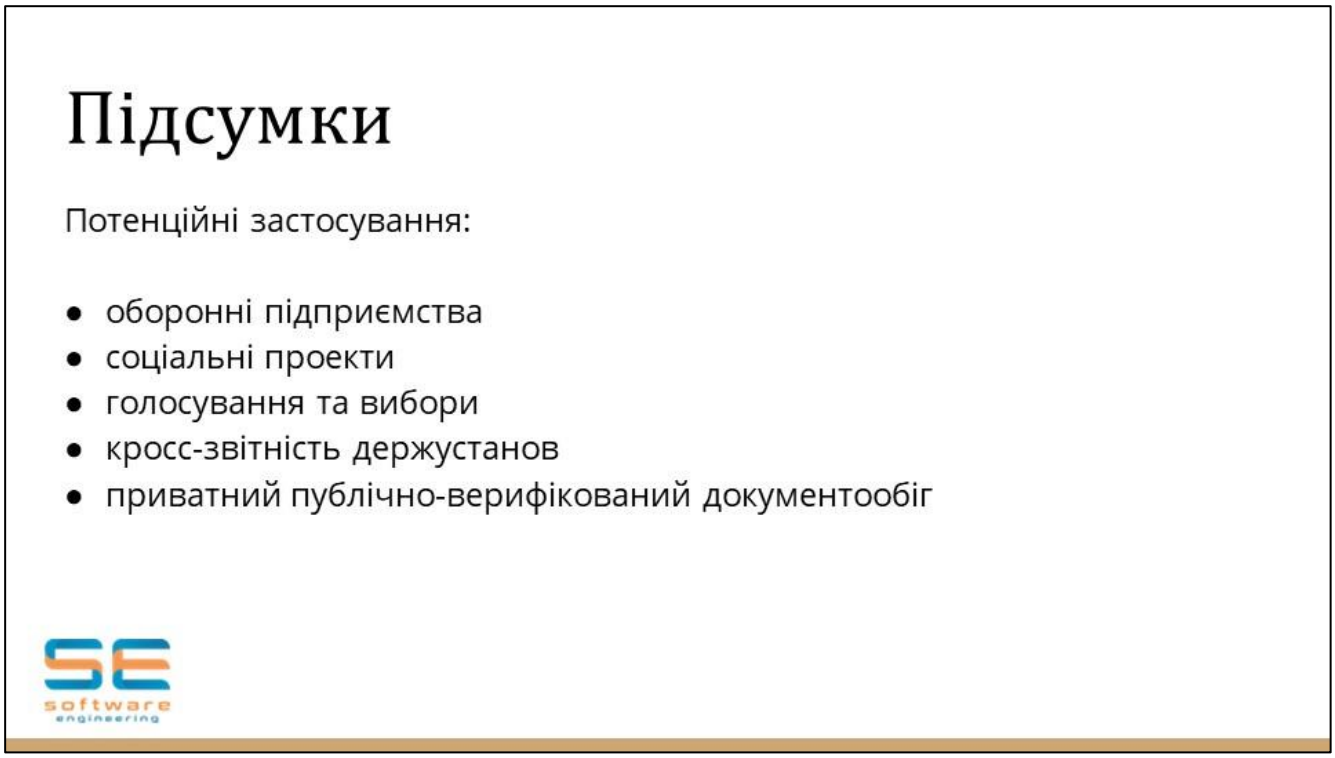


Рисунок В.19 – Слайд 19

ДОДАТОК Г

Апробація результатів роботи

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.

ДОДАТОК Д

Експертний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008: 2015

1

Експертний висновок результатів перевірки кваліфікаційної роботи

студент (посада) | програмної інженерії (кафедра) | ІПЗм-22-3 (група)

Прядко В.С.
(прізвище, ім'я, по батькові)

Зауваження

Пункт ДСТУ 3008-2015	Зміст пункту	Сторінка кваліфікаційної роботи
1	2	3
	7.1 Загальні положення	
	7.3 Нумерація сторінок звіту	
	7.4 Нумерація розділів, підрозділів, пунктів, підпунктів	
	7.5 Рисунки	
	7.6 Таблиці	
	7.7 Переліки	
	7.8 Примітки	
	7.10 Формули та рівняння	
	7.15 Додатки	
Методичні вказівки до виконання кваліфікаційної роботи магістра… **ЗАТВЕРДЖЕНО** кафедрою ПІ протокол № 5 від 13.11.2023р. 3.2 Оформлення пояснювальної записки згідно з ДСТУ 3008:2015 Звіти у сфері науки і техніки. Структура та правила оформлювання. **Шаблон** затверджений засіданням кафедри №3 від 16.10.2023.	Рисунок повинен розміщуватися одразу після його згадування у тексті, або на наступній сторінці. Під рисунком повинен бути підпис із словом Рисунок, порядковим номером цього рисунку, через тире з великої літери – назва рисунку та **в круглих дужках вказується джерело з якого взятий цей рисунок, або то, що його виконано самостійно.**	12, далі за текстом
Методичні вказівки до виконання кваліфікаційної роботи магістра… **ЗАТВЕРДЖЕНО** кафедрою ПІ протокол № 5 від 13.11.2023р. 3.2 Оформлення пояснювальної записки згідно з ДСТУ 3008:2015 Звіти у сфері науки і техніки. Структура та правила оформлювання. **Шаблон** затверджений засіданням кафедри №3 від 16.10.2023.	Назву таблиці друкують з великої літери і розміщують над таблицею з абзацного відступу та **в круглих дужках вказується джерело з якого взята ця таблиця, або то, що вона виконана самостійно. ПРИКЛАД: шаблон, стор.15**	11, далі за текстом

Експерт _____ (підпис) Вадим НЕЧВОЛОД (прізвище, ініціали)

13.06.2024